kaspersky

Kaspersky Endpoint Security 10 Service Pack 2 for Windows

Spis treści

Informacje o Kaspersky Endpoint Security 10 Service Pack 2 for Windows

Ta sekcja opisuje funkcje, składniki i pakiet dystrybucyjny Kaspersky Endpoint Security oraz zawiera listę wymagań sprzętowych i programowych Kaspersky Endpoint Security.

Nowości

Program Kaspersky Endpoint Security 10 Service Pack 2 for Windows oferuje następujące funkcje i ulepszenia:

1. Kontrola uruchamiania aplikacji:
   - Obsługuje serwerowe systemy operacyjne.
   - Kontroluje pobieranie sterowników i modułów DLL.
   - Zarządza listą obiektów zadania inwentaryzacji (moduły DLL i pliki skryptu).
   - Kontroluje obiekty w oparciu o nowe kryteria - według atrybutów certyfikatów elektronicznych i podpisów cyfrowych.
   - Generuje raport z testowego uruchamiania zablokowanych aplikacji.
   - Obsługuje dwa tryby działania: "Czarna lista" i "Biała lista".
   - Używa sumy kontrolnej SHA256 do kontroli i inwentaryzacji obiektów.
   - Kontroluje uruchamianie skryptów z interpretera PowerShell.
   - Używa magazynu zaufanych certyfikatów systemowych.
2. Microsoft BitLocker Administration umożliwia szyfrowanie dysków twardych przy pomocy technologii BitLocker firmy Microsoft:
   - Zarządzaj zdalnie szyfrowaniem.
   - Monitoruj zaszyfrowane urządzenia.
   - Twórz raporty z szyfrowania urządzeń.
   - Przywróć dostęp do zaszyfrowanych urządzeń.
3. Kaspersky Disk Encryption:
   - Obsługa wprowadzania danych uwierzytelniających w środowisku wykonawczym przed uruchomieniem systemu dla Agenta autoryzacji z użyciem klawiatury wirtualnej.
   - Obsługa trybu szyfrowania do szyfrowania tylko zajętego obszaru urządzenia.
   - Obsługa szyfrowania na tabletach (MS Surface w wersji 3 i 4).
4. Kontrola uprawnień aplikacji:
   - Kontroluje dostęp aplikacji do urządzeń rejestrujących dźwięk i obraz.

5. Kontrola sieci:

    - Konfiguruje reguły dostępu do zasobów sieciowych dla dodatkowych kategorii zasobów sieciowych.

6. Kontrola urządzeń:

    - Zapisuje zdarzenia związane z usuwaniem i zapisywaniem plików na urządzeniach USB.
    - Generuje listę zaufanych sieci Wi-Fi w oparciu o następujące ustawienia: nazwa, rodzaj szyfrowania i typ autoryzacji.
    - Zarządza uprawnieniami dostępu użytkownika do zapisu i odczytu plików na płytach CD/DVD.

7. Ochrona poczty:

    - Może usuwać i zmieniać nazwy określonych typów plików w archiwach.

8. Kaspersky Security Network:

    - Wyświetla KSN jako powód decyzji dotyczącej metody przetworzenia obiektu w raportach Kaspersky Endpoint Security i raportach Kaspersky Security Center.
    - Wysyła zapytanie do KSN odnośnie reputacji wybranego pliku.
    - Wyświetla stan dostępności serwerów KSN dla komputerów klienckich z zainstalowanym programem Kaspersky Endpoint Security.

Pakiet dystrybucyjny

Pakiet dystrybucyjny Kaspersky Endpoint Security zawiera następujące pliki:

- Pliki wymagane do instalacji aplikacji przy użyciu jednej z dostępnych metod:
- Pliki pakietu aktualizacji używanego podczas instalacji aplikacji.
- Plik klcfginst.msi do zainstalowania wtyczki zarządzającej Kaspersky Endpoint Security poprzez Kaspersky Security Center.
- Plik ksn_<ID języka>.txt, w którym znajdziesz warunki uczestnictwa w Kaspersky Security Network.
- Plik license.txt, w którym znajdziesz Umowę licencyjną.
- Plik incompatible.txt zawierający listę niekompatybilnego oprogramowania.
- Plik installer.ini, który zawiera wewnętrzne ustawienia pakietu dystrybucyjnego.

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

Aby uzyskać dostęp do plików, należy rozpakować pakiet dystrybucyjny.

Zarządzanie ochroną komputera

Kaspersky Endpoint Security zapewnia odpowiednią ochronę komputera przed różnymi typami zagrożeń, atakami sieciowymi i phishingowymi.

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

Poza ochroną w czasie rzeczywistym zapewnianą przez moduły aplikacji, zalecamy regularne *skanowanie* komputera w poszukiwaniu wirusów i innych zagrożeń. Pozwala to wyeliminować możliwość rozpowszechniania się szkodliwego oprogramowania, które nie jest wykrywane przez moduły ochrony z powodu ustawienia niskiego poziomu ochrony lub z innych powodów.

Aby wersje modułów i bazy danych programu Kaspersky Endpoint Security nie uległy przeterminowaniu, musisz je *aktualizować*. Domyślnie aplikacja jest aktualizowana automatycznie, ale w razie konieczności możesz zawsze uruchomić aktualizację baz danych i modułów aplikacji ręcznie.

Modułami kontroli są następujące składniki aplikacji:

- **Kontrola uruchamiania aplikacji**. Ten moduł śledzi próby uruchamiania aplikacji przez użytkownika i kontroluje uruchamianie aplikacji.

- **Kontrola uprawnień aplikacji**. Ten komponent rejestruje akcje wykonywane przez aplikacje w systemie i kontroluje aktywność aplikacji w zależności od grupy zaufania, do której należy dana aplikacja. Dla każdej grupy aplikacji określony jest zestaw reguł. Reguły te kontrolują dostęp aplikacji do danych użytkownika i zasobów systemu operacyjnego. Takie dane to pliki użytkownika (folder Moje Dokumenty, ciasteczka, informacje o aktywności użytkownika) oraz pliki, foldery i klucze rejestru zawierające ustawienia i ważne informacje dotyczące najczęściej używanych aplikacji.

- **Monitor wykrywania luk**. Monitor wykrywania luk wykonuje w czasie rzeczywistym zadanie wykrywania luk w uruchamianych aplikacjach i w aplikacjach już działających na komputerze użytkownika.

- **Kontrola urządzeń**. Ten moduł umożliwia ustawienie elastycznych ograniczeń dostępu do urządzeń przechowywania danych (takich jak dyski twarde, dyski wymienne, nośniki taśmowe, płyty CD/DVD), sprzętu przesyłającego dane (takiego jak modemy), sprzętu tworzącego kopie informacji (takiego jak drukarki) i interfejsów służących do podłączania urządzeń do komputerów (takich jak USB, Bluetooth czy podczerwień).

- **Kontrola sieci**. Ten składnik umożliwia ustawienie elastycznych ograniczeń dostępu do zasobów sieciowych dla różnych grup użytkowników.

Działanie modułów kontroli opiera się na następujących regułach:

- Kontrola uruchamiania aplikacji używa reguł Kontroli uruchamiania aplikacji.

- Kontrola uprawnień aplikacji używa reguł Kontroli aplikacji.

- Kontrola urządzeń używa reguł dostępu do urządzenia oraz reguł dostępu do magistrali połączenia.

- Kontrola sieci używa reguł dostępu do zasobu sieciowego.

Modułami ochrony są następujące składniki aplikacji:

- **Ochrona plików**. Ten moduł chroni system plików komputera przed infekcją. Ochrona plików uruchamia się przy starcie Kaspersky Endpoint Security, pozostaje aktywna w pamięci komputera i skanuje wszystkie pliki

otwierane, zapisywane i uruchamiane na komputerze oraz na wszystkich podłączonych dyskach. Ochrona plików przechwytuje każdy otwierany plik i skanuje go w poszukiwaniu wirusów i innych zagrożeń.

- **Kontrola systemu**. Ten moduł zbiera informacje o aktywności aplikacji na komputerze i udostępnia te informacje innym modułom w celu zapewnienia bardziej efektywnej ochrony komputera.

- **Ochrona poczty**. Ten moduł skanuje odbierane i wysyłane wiadomości e-mail w poszukiwaniu wirusów i innych zagrożeń.

- **Ochrona WWW**. Ten komponent skanuje ruch sieciowy przychodzący za pośrednictwem protokołu HTTP i FTP, a także sprawdza, czy adresy znajdują się na liście szkodliwych lub phishingowych adresów internetowych.

- **Ochrona komunikatorów**. Ten składnik skanuje informacje przysyłane na komputer za pośrednictwem protokołów klientów komunikatorów. Komponent umożliwia bezpieczne korzystanie z wielu klientów komunikatorów.

- **Zapora sieciowa**. Ten moduł chroni dane przechowywane na komputerze i blokuje możliwe zagrożenia systemu operacyjnego, gdy komputer jest podłączony do internetu lub sieci lokalnej. Komponent filtruje całą aktywność sieciową zgodnie z dwoma rodzajami reguł: regułami sieciowymi dla aplikacji i regułami dla pakietów sieciowych.

- **Monitor sieci**. Ten moduł pozwala śledzić aktywność sieciową komputera w czasie rzeczywistym.

- **Blokowanie ataków sieciowych**. Ten komponent bada przychodzący ruch sieciowy w poszukiwaniu aktywności typowych dla ataków sieciowych. Po wykryciu próby ataku sieciowego na Twój komputer, Kaspersky Endpoint Security blokuje aktywność sieciową atakującego komputera.

W Kaspersky Endpoint Security dostępne są następujące zadania:

- **Pełne skanowanie**. Kaspersky Endpoint Security skanuje system operacyjny, włączając w to pamięć RAM, obiekty ładowane podczas uruchamiania systemu, 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 obiekty ładowane podczas uruchamiania systemu, pamięć RAM i obiekty będące celem rootkitów.

- **Aktualizacja**. Kaspersky Endpoint Security pobiera uaktualnienia baz danych i modułów aplikacji. Aktualizacja zapewnia ochronę komputera przed najnowszymi wirusami i innymi zagrożeniami.

- **Wykrywanie luk**. Kaspersky Endpoint Security skanuje system operacyjny i zainstalowane oprogramowanie w poszukiwaniu luk. To zadanie zapewnia szybkie wykrywanie i usuwanie potencjalnych problemów, które mogą zostać wykorzystane przez cyberprzestępców.

Funkcja szyfrowania danych pozwala na szyfrowanie plików i folderów przechowywanych na lokalnych dyskach komputera. Funkcja szyfrowania dysku umożliwia szyfrowanie dysków twardych i nośników wymiennych.

Zdalne zarządzanie poprzez Kaspersky Security Center

Kaspersky Security Center umożliwia zdalne uruchamianie i zatrzymywanie działania Kaspersky Endpoint Security na komputerze klienckim oraz zdalne zarządzanie i konfigurację ustawień aplikacji.

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 i zadania. Raporty zawierają listę zdarzeń Kaspersky Endpoint Security i wszystkich działań podejmowanych przez aplikację. W przypadku wystąpienia problemu, można przesłać raporty do firmy Kaspersky, gdzie specjaliści z pomocy technicznej przyjrzą się problemowi i pomogą go rozwiązać.

- **Magazyn danych**. Jeżeli podczas skanowania komputera w poszukiwaniu wirusów i innych zagrożeń aplikacja wykryje zainfekowane lub podejrzane pliki, zablokuje je. Kaspersky Endpoint Security przenosi podejrzane pliki do specjalnego miejsca przechowywania zwanego *Kwarantanną*. 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 nieprzetworzonych plików*. Możesz skanować pliki, przywracać pliki do ich oryginalnych folderów i czyścić miejsca przechowywania danych.

- **Usługa powiadomień**. Usługa powiadomień informuje użytkownika o bieżącym stanie ochrony komputera i działaniach 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 zbieraniu w czasie rzeczywistym informacji o reputacji plików, zasobach sieciowych i oprogramowaniu 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.

- **Wsparcie użytkownika**. Wszyscy zarejestrowani użytkownicy Kaspersky Endpoint Security mogą skontaktować się ze specjalistami z pomocy technicznej Kaspersky Lab w celu uzyskania pomocy. Możesz wysłać zgłoszenie z poziomu usługi Moje konto na stronie internetowej pomocy technicznej lub uzyskać pomoc przez telefon.

Jeśli podczas działania aplikacja zwróci błąd 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.

Aplikacja pobierze informacje o powtarzających się błędach i awariach systemu przy użyciu specjalnie utworzonych do tych celów algorytmów, zdefiniowanych przez ekspertów z Kaspersky.

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 o częstotliwości taktowania 1 GHz (który obsługuje zestaw instrukcji SSE2)

- Pamięć RAM:
  - 1 GB dla 32-bitowych systemów operacyjnych;
  - 2 GB dla 64-bitowych systemów operacyjnych.

Obsługiwane systemy operacyjne dla komputerów osobistych:

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

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

Obsługiwane systemy operacyjne dla serwerów plików:

- Windows Small Business Server 2008 Standard / Premium (64-bitowy);
- Windows Small Business Server 2011 Essentials / Standard (64-bitowy);
- Windows MultiPoint Server 2011 (64-bitowy);
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 lub nowszy;
- 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.

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.

Instalowanie i dezinstalowanie aplikacji

Sekcja ta opisuje proces instalacji Kaspersky Endpoint Security na komputerze, wykonywanie wstępnej konfiguracji, aktualizowanie z poprzedniej wersji aplikacji i usuwanie aplikacji z komputera.

Instalowanie aplikacji

Ta sekcja opisuje sposób zainstalowania Kaspersky Endpoint Security na komputerze oraz sposób zakończenia wstępnej konfiguracji aplikacji.

Informacje o sposobach instalacji aplikacji

Program Kaspersky Endpoint Security 10 for Windows można zainstalować lokalnie (bezpośrednio na komputerze użytkownika) lub zdalnie, z poziomu stacji roboczej administratora.

Instalację lokalną Kaspersky Endpoint Security 10 for Windows można przeprowadzić w jednym z następujących trybów:

- W trybie interaktywnym, korzystając z Kreatora instalacji aplikacji.

  Ten tryb wymaga uczestniczenia w procesie instalacji.

- W trybie cichym, z poziomu wiersza poleceń.

  W tym trybie nie jest wymagany udział w procesie instalacji.

Aplikacja może zostać zainstalowana zdalnie na komputerach w sieci przy użyciu:

- Programu Kaspersky Security Center (zobacz *Przewodnik instalacji dla Kaspersky Security Center*).
- Edytora zasad grupy systemu Microsoft Windows (zobacz pliki pomocy systemu operacyjnego).
- Programu System Center Configuration Manager.

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

Instalowanie aplikacji przy użyciu Kreatora instalacji

Interfejs Kreatora instalacji aplikacji składa się z szeregu okien odpowiadających krokom instalacji aplikacji. Możesz przełączać między oknami Kreatora instalacji przy pomocy przycisków **Wstecz** i **Dalej**. W celu zamknięcia Kreatora instalacji po zakończeniu jego działania kliknij przycisk **Zakończ**. W celu zatrzymania Kreatora instalacji w dowolnym momencie użyj przycisku **Anuluj**.

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

1. Uruchom plik setup.exe z pakietu dystrybucyjnego.

Zostanie uruchomiony Kreator instalacji.

2. Postępuj zgodnie z instrukcjami Kreatora instalacji.

Po uruchomieniu pliku setup.exe, Kaspersky Endpoint Security sprawdza komputer pod kątem niekompatybilnego oprogramowania. Domyślnie, po wykryciu niekompatybilnego oprogramowania, proces instalacji zostaje przerwany i zostaje wyświetlona lista aplikacji niekompatybilnych z Kaspersky Endpoint Security. Aby kontynuować instalację, usuń te aplikacje z komputera.

Krok 1. Weryfikowanie wymagań instalacyjnych

Przed zainstalowaniem aplikacji Kaspersky Endpoint Security 10 for Windows lub jej aktualizacją z poprzedniej wersji, należy sprawdzić, czy spełnione są następujące wymagania:

- System operacyjny i dodatki Service Pack spełniają wymagania instalacyjne.
- Spełnione są wymagania sprzętowe i programowe.
- Użytkownik ma uprawnienia do zainstalowania produktu.

Jeżeli jakiekolwiek 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 10 Service Pack 2 for Windows, a poprzednia wersja aplikacji zostanie automatycznie usunięta. Dotyczy to następujących wersji aplikacji:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 / MP4 CF2
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 / MP4 CF2
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows

Krok 2. Okno powitalne Kreatora instalacji

Jeśli spełniono wszystkie wymagania dla instalacji aplikacji, po uruchomieniu pakietu instalacyjnego pojawi się ekran powitalny. Okno powitalne informuje o rozpoczęciu instalacji programu Kaspersky Endpoint Security na komputerze.

Aby przejść do następnego kroku Kreatora instalacji, kliknij przycisk **Dalej**.

Krok 3. Zapoznanie się z Umową Licencyjną

W tym kroku należy przeczytać umowę licencyjną zawieraną pomiędzy Tobą a Kaspersky.

Uważnie przeczytaj umowę licencyjną i, jeśli zgadzasz się ze wszystkimi jej warunkami i postanowieniami, zaznacz pole **Akceptuję warunki Umowy licencyjnej**.

Aby powrócić do poprzedniego kroku Kreatora instalacji, kliknij przycisk **Wstecz**. Aby przejść do następnego kroku Kreatora instalacji, kliknij przycisk **Dalej**. W celu zatrzymania Kreatora instalacji użyj przycisku **Anuluj**.

Krok 4. Wybieranie typu instalacji

Na tym etapie możesz wybrać najbardziej odpowiedni dla Ciebie typ instalacji programu Kaspersky Endpoint Security:

- **Instalacja podstawowa**. Jeśli wybierzesz ten typ instalacji, na komputerze zostaną zainstalowane składniki ochrony, Kontrola uprawnień aplikacji i Monitor wykrywania luk z ustawieniami zalecanymi przez ekspertów z Kaspersky.
- **Instalacja standardowa**. Jeśli wybierzesz ten typ instalacji, na komputerze zostaną zainstalowane składniki kontrolne i składniki ochrony z ustawieniami zalecanymi przez Kaspersky.
- **Instalacja niestandardowa**. Jeżeli wybierzesz ten typ instalacji, zostaniesz poproszony o wybranie instalowanych składników i o określenie folderu docelowego dla aplikacji.

  Ten typ instalacji umożliwia zainstalowanie komponentów, które nie znajdują się w instalacji podstawowej i standardowej.

Domyślnie wybrana jest standardowa instalacja.

Aby powrócić do poprzedniego kroku Kreatora instalacji, kliknij przycisk **Wstecz**. Aby przejść do następnego kroku Kreatora instalacji, kliknij przycisk **Dalej**. W celu zatrzymania Kreatora instalacji użyj przycisku **Anuluj**.

Krok 5. Wybieranie instalowanych składników aplikacji

Ten krok jest dostępny, jeżeli wybrałeś *Instalację niestandardową*.

W tym kroku możesz wybrać instalowane składniki Kaspersky Endpoint Security. Instalacja modułu Ochrona plików jest obowiązkowa. Nie możesz anulować jego instalacji.

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

- Ochrona przed atakami BadUSB.
- Szyfrowanie dysków.
- Szyfrowanie plików.
- Microsoft BitLocker Manager.

- KATA Endpoint Sensor.

Microsoft BitLocker Manager pełni następujące funkcje:

- Zarządza technologią Szyfrowanie funkcją BitLocker wbudowaną w system operacyjny Windows.
- Konfiguruje ustawienia profilu szyfrowania i sprawdza ich dostępność dla zarządzanego komputera.
- Uruchamia procesy szyfrowania i deszyfrowania.
- Monitoruje stan szyfrowania na zarządzanym komputerze.
- Realizuje funkcje scentralizowanego przechowywania kluczy odzyskiwania na Serwerze administracyjnym Kaspersky Security Center.

KATA Endpoint Sensor to komponent Kaspersky Anti Targeted Attack Platform. To rozwiązanie jest przeznaczone do szybkiego wykrywania zagrożeń takich jak ataki ukierunkowane. Komponent cały czas monitoruje procesy, aktywne połączenia sieciowe oraz pliki, które są modyfikowane, i przesyła te informacje do Kaspersky Anti Targeted Attack Platform.

Aby wybrać moduł do instalacji, kliknij ikonę obok jego nazwy i z menu kontekstowego wybierz **Składnik zostanie zainstalowany na lokalnym dysku twardym**. Aby uzyskać szczegółowe informacje o zadaniach wykonywanych przez wybrany komponent oraz o ilości miejsca na dysku potrzebnego do jego zainstalowania, skorzystaj z dolnej części tego okna Kreatora instalacji.

Aby wyświetlić szczegółowe informacje o dostępnym miejscu na dysku, kliknij przycisk **Wolumin**. Informacje zostaną wyświetlone w otwartym oknie **Dostępne miejsce na dysku**.

Aby anulować instalację składnika, w menu kontekstowym wybierz **Składnik będzie niedostępny**.

W celu powrotu do listy składników instalowanych domyślnie, należy kliknąć przycisk **Resetuj**.

Aby powrócić do poprzedniego kroku Kreatora instalacji, kliknij przycisk **Wstecz**. Aby przejść do następnego kroku Kreatora instalacji, kliknij przycisk **Dalej**. W celu zatrzymania Kreatora instalacji użyj przycisku **Anuluj**.

Krok 6. Wybieranie folderu docelowego

Ten krok jest dostępny, jeżeli wybrałeś *Instalację niestandardową*.

W tym kroku możesz określić ścieżkę dostępu do folderu docelowego, w którym zostanie zainstalowana aplikacja. W celu wybrania folderu użyj przycisku **Przeglądaj** .

Aby wyświetlić informacje o dostępnym miejscu na lokalnym dysku twardym, kliknij przycisk **Wolumin**. Informacje zostaną wyświetlone w otwartym oknie **Dostępne miejsce na dysku**.

Aby powrócić do poprzedniego kroku Kreatora instalacji, kliknij przycisk **Wstecz**. Aby przejść do następnego kroku Kreatora instalacji, kliknij przycisk **Dalej**. W celu zatrzymania Kreatora instalacji użyj przycisku **Anuluj**.

Krok 7. Dodawanie wykluczeń ze skanowania antywirusowego

Ten krok jest dostępny, jeżeli wybrałeś *Instalację niestandardową*.

W tym kroku możesz określić, które wykluczenia ze skanowania antywirusowego mają być uwzględnione w ustawieniach aplikacji.

Opcje **Wyłącz ze skanowania antywirusowego obszary zalecane przez Microsoft** / **Wyłącz ze skanowania antywirusowego obszary zalecane przez Kaspersky** są odpowiedzialne za wykluczenie z lub włączenie do strefy zaufanej obszarów zalecanych przez Microsoft lub Kaspersky.

W zależności od tego, która opcja została zaznaczona, Kaspersky Endpoint Security włączy do strefy zaufanej obszary zalecane przez Microsoft lub Kaspersky. Kaspersky Endpoint Security nie skanuje takich obszarów w poszukiwaniu wirusów i innych zagrożeń.

Pole **Wyłącz ze skanowania antywirusowego obszary zalecane przez Microsoft** jest dostępne, gdy Kaspersky Endpoint Security jest instalowany na komputerze działającym pod kontrolą Microsoft Windows dla serwerów plików.

Aby powrócić do poprzedniego kroku Kreatora instalacji, kliknij przycisk **Wstecz**. Aby przejść do następnego kroku Kreatora instalacji, kliknij przycisk **Dalej**. W celu zatrzymania Kreatora instalacji użyj przycisku **Anuluj**.

Krok 8. Przygotowywanie do zainstalowania aplikacji

Zalecane jest chronienie procesu instalacji, gdyż Twój komputer może zostać zainfekowany szkodliwym oprogramowaniem mogącym wpływać na instalację programu Kaspersky Endpoint Security 10 for Windows.

Domyślnie ochrona procesu instalacji jest włączona.

Jeżeli aplikacja nie może zostać zainstalowana (na przykład podczas zdalnej instalacji przy użyciu pulpitu zdalnego systemu Windows), zalecane jest wyłączenie ochrony procesu instalacji. W takim przypadku przerwij instalację i uruchom ponownie Kreator instalacji aplikacji. W kroku "Przygotowywanie do zainstalowania aplikacji" usuń zaznaczenie z pola **Chroń proces instalacji**.

Pole **Zapewnij kompatybilność z Citrix PVS** włącza / wyłącza funkcję instalowania sterowników w trybie kompatybilności z Citrix PVS.

Zaznacz to pole tylko wtedy, gdy pracujesz z technologią Citrix Provisioning Services.

Pole **Dodaj ścieżkę do pliku avp.com do zmiennej systemowej %PATH%** włącza / wyłącza opcję dodania ścieżki do pliku avp.com do zmiennej systemowej %PATH%.

Jeśli pole jest zaznaczone, uruchamianie Kaspersky Endpoint Security lub dowolnych jego zadań z wiersza poleceń nie będzie wymagać wprowadzania ścieżki do pliku wykonywalnego. Aby uruchomić określone zadanie, wystarczy wprowadzić nazwę pliku wykonywalnego i polecenie.

Aby powrócić do poprzedniego kroku Kreatora instalacji, kliknij przycisk **Wstecz**. Aby zainstalować program, kliknij przycisk **Instaluj**. W celu zatrzymania Kreatora instalacji użyj przycisku **Anuluj**.

Podczas instalacji aplikacji zerwane mogą zostać bieżące połączenia sieciowe. Większość z zerwanych połączeń zostanie przywrócona po zakończeniu instalacji aplikacji.

Krok 9. Instalowanie aplikacji

Instalacja programu może zająć trochę czasu. Poczekaj, aż zostanie ona pomyślnie zakończona.

Jeżeli aktualizujesz poprzednią wersję aplikacji, krok ten będzie zawierał także przeniesione ustawienia i opcję usunięcie poprzedniej wersji aplikacji.

Po zakończeniu instalacji Kaspersky Endpoint Security, zostanie uruchomiony Kreator wstępnej konfiguracji.

Instalowanie aplikacji z poziomu wiersza poleceń

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`.

W celu zainstalowania aplikacji lub zaktualizowania 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|0] [/pADDLOCAL=<komponent>] [/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/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|0] [ADDLOCAL=<komponent>] [SKIPPRODUCTCHECK=1|0] [SKIPPRODUCTUNINSTALL=1|0] [KLLOGIN=<nazwa użytkownika> KLPASSWD=<hasło> KLPASSWDAREA=<zakres działania hasła>] [ENABLETRACES=1|0 TRACESLEVEL=<poziom śledzenia>] /qn
   ```

`EULA`	Akceptacja lub odrzucenie warunków Umowy licencyjnej. Dostępne wartości: • `1` – akceptacja lub odrzucenie warunków Umowy licencyjnej. • `0` – odrzucenie warunków Umowy licencyjnej. Umowa licencyjna jest zawarta w pakiecie dystrybucyjnym Kaspersky Endpoint Security. Akceptacja warunków Umowy licencyjnej jest niezbędna do zainstalowania aplikacji lub jej aktualizacji.
`PRIVACYPOLICY`	Akceptacja lub odrzucenie Polityki prywatności. Dostępne wartości: • `1` – akceptacja Polityki prywatności. • `0` – odrzucenie Polityki prywatności.

	Treść Polityki prywatności znajduje się w pakiecie dystrybucyjnym Kaspersky Endpoint Security. Aby zainstalować aplikację lub zaktualizować wersję aplikacji, musisz zaakceptować Politykę prywatności.
KSN	Akceptacja lub odmowa uczestnictwa w Kaspersky Security Network. Jeśli nie ustawiono wartości dla tego parametru, Kaspersky Endpoint Security wyświetli monit o potwierdzenie zgody lub odmowę uczestniczenia w KSN przy pierwszym uruchomieniu Kaspersky Endpoint Security. Dostępne wartości: • `1` – zgoda na uczestniczenie w KSN. • `0` – odmowa uczestniczenia w KSN (wartość domyślna). Pakiet dystrybucyjny Kaspersky Endpoint Security jest zoptymalizowany do użycia z Kaspersky Security Network. Jeśli zdecydowałeś się nie uczestniczyć w Kaspersky Security Network, powinieneś zaktualizować Kaspersky Endpoint Security od razu po zakończeniu instalacji.
ALLOWREBOOT	Automatyczne ponowne uruchamianie komputera, jeśli jest wymagane po zainstalowaniu lub zaktualizowaniu aplikacji. Dostępne wartości: • `1` – automatyczne ponowne uruchomienie komputera, jeśli jest wymagane. • `0` – automatyczne ponowne uruchomienie komputera jest zablokowane (wartość domyślna). 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.
ADDLOCAL	Wybierz dodatkowe komponenty do zainstalowania. Domyślnie, wszystkie składniki aplikacji zostają wybrane do zainstalowania, za wyjątkiem następujących składników: Ochrona przed atakami BadUSB, Szyfrowanie plików, Szyfrowanie całego dysku, Zarządzanie Bitlocker i KATA Endpoint Sensor. Dostępne wartości: • `MSBitLockerFeature`. Komponent BitLocker Manager jest zainstalowany. • `AntiAPTFeature`. Komponent KATA Endpoint Sensor jest zainstalowany.
SKIPPRODUCTCHECK	Sprawdzanie niekompatybilnego oprogramowania. Lista niekompatybilnego oprogramowania jest dostępna w pliku incompatible.txt, który znajduje się w pakiecie dystrybucyjnym. Dostępne wartości: • `1` – wyszukiwanie niekompatybilnego oprogramowania jest włączone (wartość domyślna). • `0` – wyszukiwanie niekompatybilnego oprogramowania jest wyłączone.
SKIPPRODUCTUNINSTALL	Automatyczne usuwanie wykrytych niekompatybilnych programów. Dostępne wartości: • `1` – Kaspersky Endpoint Security próbuje usunąć niekompatybilne oprogramowanie (wartość domyślna).

	• `0` – automatyczne usuwanie niekompatybilnego oprogramowania jest zablokowane.
`KLLOGIN`	Ustaw nazwę użytkownika, aby uzyskać dostęp do funkcji i ustawień Kaspersky Endpoint Security (komponent Ochrona hasłem). Nazwa użytkownika jest ustawiana wraz z parametrami `KLPASSWD` i `KLPASSWDAREA`. Domyślna nazwa użytkownika to KLAdmin.
`KLPASSWD`	Określ hasło dostępu do funkcji i ustawień Kaspersky Endpoint Security (hasło jest określane wraz z parametrami `KLLOGIN` i `KLPASSWDAREA`). Jeśli określiłeś hasło, ale nie określiłeś nazwy użytkownika z parametrem `KLLOGIN`, domyślnie używana będzie nazwa użytkownika KLAdmin.
`KLPASSWDAREA`	Zakres działania hasła dostępu do funkcji i ustawień Kaspersky Endpoint Security. Jeśli użytkownik spróbuje wykonać działanie, które znajduje się w tym obszarze, Kaspersky Endpoint Security wyświetli monit o podanie danych uwierzytelniających konta użytkownika (parametry `KLLOGIN` i `KLPASSWD`). Użyj znaku „`;`”, aby określić kilka wartości. Dostępne wartości: • `SET` – modyfikowanie ustawień aplikacji. • `EXIT` – zakończenie działania aplikacji. • `DISPROTECT` – wyłączanie komponentów ochrony i zatrzymywanie zadań skanowania. • `DISPOLICY` – wyłączanie profilu 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. Dostępne wartości: • `1` – śledzenie jest włączone. • `0` – śledzenie jest wyłączone (wartość domyślna).
`TRACESLEVEL`	Poziom szczegółowości śledzenia. Dostępne wartości: • `100` (krytyczny). Tylko wiadomości o błędach krytycznych. • `200` (wysoki). Wiadomości o wszystkich błędach, w tym błędach krytycznych. • `300` (diagnostyczny). Wiadomości o wszystkich błędach oraz wybór wiadomości zawierających ostrzeżenia. • `400` (ważny). Wszystkie ostrzeżenia i wiadomości o błędach zwykłych i krytycznych oraz wybrane wiadomości zawierające dodatkowe informacje.

- `500` (normalny). Wszystkie ostrzeżenia i wiadomości o błędach zwykłych i krytycznych oraz wiadomości ze szczegółowymi informacjami o działaniu aplikacji w trybie normalnym (wartość domyślna).
- `600` (niski). Wszystkie możliwe wiadomości.

Przykład:

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1 /s

msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Po zainstalowaniu aplikacji, Kaspersky Endpoint Security aktywuje licencję testową, chyba że wskazałeś kod aktywacyjny 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, musisz aktywować licencję komercyjną.

Podczas instalacji aplikacji lub uaktualniania jej wersji w trybie cichym używane są następujące pliki:

- Setup.ini – ogólne ustawienia instalacyjne aplikacji;
- install.cfg – lokalne ustawienia 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.

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 application**.

   c. W sekcji **Standard application**:

      - 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 **Tryb wykonywania** wybrano element **Uruchom z uprawnieniami administratora**.

   d. W sekcji **Requirements**:

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

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

      - W sekcji **Platform requirements** zaznacz opcję **This application can be started only on the 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 podczas 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]` – ogólne opcje 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.
- `[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
`[Setup]`	`InstallDir`	Ścieżka do folderu instalacyjnego aplikacji.
	`ActivationCode`	Kod aktywacyjny Kaspersky Endpoint Security.
	`Eula`	Akceptacja lub odrzucenie warunków Umowy licencyjnej. Dostępne wartości: • `1` – akceptacja lub odrzucenie warunków Umowy licencyjnej. • `0` – odrzucenie warunków Umowy licencyjnej. Umowa licencyjna jest zawarta w pakiecie dystrybucyjnym Kaspersky Endpoint Security. Akceptacja warunków Umowy licencyjnej jest niezbędna do zainstalowania aplikacji lub jej aktualizacji.
	`PrivacyPolicy`	Akceptacja lub odrzucenie Polityki prywatności. Dostępne wartości: • `1` – akceptacja Polityki prywatności.

		• `0` – odrzucenie Polityki prywatności. Treść Polityki prywatności znajduje się w pakiecie dystrybucyjnym Kaspersky Endpoint Security. Aby zainstalować aplikację lub zaktualizować wersję aplikacji, musisz zaakceptować Politykę prywatności.
	`KSN`	Akceptacja lub odmowa uczestnictwa w Kaspersky Security Network. Jeśli nie ustawiono wartości dla tego parametru, Kaspersky Endpoint Security wyświetli monit o potwierdzenie zgody lub odmowę uczestniczenia w KSN przy pierwszym uruchomieniu Kaspersky Endpoint Security. Dostępne wartości: • `1` – zgoda na uczestniczenie w KSN. • `0` – odmowa uczestniczenia w KSN (wartość domyślna). Pakiet dystrybucyjny Kaspersky Endpoint Security jest zoptymalizowany do użycia z Kaspersky Security Network. Jeśli zdecydowałeś się nie uczestniczyć w Kaspersky Security Network, powinieneś zaktualizować Kaspersky Endpoint Security od razu po zakończeniu instalacji.
	`Login`	Ustaw nazwę użytkownika, aby uzyskać dostęp do funkcji i ustawień Kaspersky Endpoint Security (komponent Ochrona hasłem). Nazwa użytkownika jest ustawiana wraz z parametrami `Password` i `PasswordArea`. Domyślna nazwa użytkownika to KLAdmin.
	`Hasło`	Określ hasło dostępu do funkcji i ustawień Kaspersky Endpoint Security (hasło jest określane wraz z parametrami `Login` i `PasswordArea`). Jeśli określiłeś hasło, ale nie określiłeś nazwy użytkownika z parametrem `Login`, domyślnie używana będzie nazwa użytkownika KLAdmin.
	`PasswordArea`	Zakres działania hasła dostępu do funkcji i ustawień Kaspersky Endpoint Security. Jeśli użytkownik spróbuje wykonać działanie, które znajduje się w tym obszarze, Kaspersky Endpoint Security wyświetli monit o podanie danych uwierzytelniających konta użytkownika (parametry `Login` i `Password`). Użyj znaku „`;`”, aby określić kilka wartości. Dostępne wartości: • `SET` – modyfikowanie ustawień aplikacji. • `EXIT` – zakończenie działania aplikacji. • `DISPROTECT` – wyłączanie komponentów ochrony i zatrzymywanie zadań skanowania. • `DISPOLICY` – wyłączanie profilu Kaspersky Security Center.

		• `UNINST` – usunięcie aplikacji z komputera. • `DISCTRL` – wyłączenie składników kontroli. • `REMOVELIC` – usuwanie klucza. • `REPORTS` – wyświetlanie raportów.
	`SelfProtection`	Włączenie lub wyłączenie mechanizmu ochrony instalacji aplikacji. Dostępne wartości: • `1` – mechanizm ochrony instalacji aplikacji jest włączony. • `0` – mechanizm ochrony instalacji aplikacji jest wyłączony. Możesz wyłączyć ochronę instalacji. Ochrona instalacji obejmuje ochronę przed podszywaniem się przez szkodliwe oprogramowanie pod pakiet dystrybucyjny, blokowaniem dostępu do folderu instalacyjnego Kaspersky Endpoint Security, a także blokowaniem dostępu do gałęzi rejestru systemu zawierającej 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.
	`Reboot=1`	Automatyczne ponowne uruchamianie komputera, jeśli jest wymagane po zainstalowaniu lub zaktualizowaniu aplikacji. Jeśli dla tego parametru nie zostanie ustawiona żadna wartość, automatyczne ponowne uruchomienie komputera zostanie zablokowane. Ponowne uruchomienie nie jest wymagane podczas instalowania Kaspersky Endpoint Security. Ponowne uruchomienie jest wymagane tylko wtedy, gdy przed instalacją musisz usunąć niekompatybilne aplikacje. Ponowne uruchomienie może być też wymagane podczas aktualizowania wersji aplikacji.
	`AddEnvironment`	Do zmiennej %PATH% zostaje dodana ścieżka dostępu do plików wykonywalnych znajdujących się w folderze instalacyjnym Kaspersky Endpoint Security. Dostępne wartości: • `1` – do zmiennej %PATH% zostaje dodana ścieżka dostępu do plików wykonywalnych znajdujących się w folderze instalacyjnym Kaspersky Endpoint Security. • `0` – do zmiennej %PATH% nie zostaje dodana ścieżka dostępu do plików wykonywalnych znajdujących się w folderze instalacyjnym Kaspersky Endpoint Security.
	`AMPPL`	Włącza lub wyłącza ochronę usługi Kaspersky Endpoint Security przy użyciu technologii AM-PPL

		(Antimalware Protected Process Light). Dostępne wartości: • `1` – ochrona usługi Kaspersky Endpoint Security przy użyciu technologii AM-PPL jest włączona. • `0` – ochrona usługi Kaspersky Endpoint Security przy użyciu technologii AM-PPL jest wyłączona.
	`SetupReg`	Włącza zapisywanie kluczy rejestru z pliku setup.reg do rejestru. Wartość parametru `SetupReg: setup.reg`.
	`EnableTraces`	Włączanie lub wyłączanie śledzenia instalacji aplikacji. Kaspersky Endpoint Security zapisuje pliki śledzenia w folderze %ProgramData%/Kaspersky Lab. Dostępne wartości: • `1` – śledzenie instalacji aplikacji jest włączone. • `0` – śledzenie instalacji aplikacji jest wyłączone (wartość domyślna).
	`TracesLevel`	Poziom szczegółowości śledzenia. Dostępne wartości: • `100` (krytyczny). Tylko wiadomości o błędach krytycznych. • `200` (wysoki). Wiadomości o wszystkich błędach, w tym błędach krytycznych. • `300` (diagnostyczny). Wiadomości o wszystkich błędach oraz wybór wiadomości zawierających ostrzeżenia. • `400` (ważny). Wszystkie ostrzeżenia i wiadomości o błędach zwykłych i krytycznych oraz wybrane wiadomości zawierające dodatkowe informacje. • `500` (normalny). Wszystkie ostrzeżenia i wiadomości o błędach zwykłych i krytycznych oraz wiadomości ze szczegółowymi informacjami o działaniu aplikacji w trybie normalnym (wartość domyślna). • `600` (niski). Wszystkie możliwe wiadomości.
`[Components]`	`ALL`	Instalacja wszystkich komponentów. Jeśli dla parametru określono wartość `1`, zostaną zainstalowane wszystkie komponenty, niezależnie od ustawień instalacji pojedynczych składników.
	`MailAntiVirus`	Ochrona poczty.
	`IMAntiVirus`	Ochrona komunikatorów.
	`WebAntiVirus`	Ochrona WWW.

	`ApplicationPrivilegeControl`	Kontrola uprawnień aplikacji.
	`SystemWatcher`	Kontrola systemu.
	`Zapora sieciowa`	Zapora sieciowa.
	`NetworkAttackBlocker`	Blokowanie ataków sieciowych.
	`WebControl`	Kontrola sieci.
	`DeviceControl`	Kontrola urządzeń.
	`ApplicationStartupControl`	Kontrola uruchamiania aplikacji.
	`FileEncryption`	Biblioteki Szyfrowania na poziomie plików.
	`DiskEncryption`	Biblioteki Szyfrowania całego dysku.
	`VulnerabilityAssessment`	Monitor wykrywania luk.
	`KeyboardAuthorization`	Ochrona przed atakami BadUSB
	`AntiAPT`	KATA Endpoint Sensor.
	`MSBitLocker`	Microsoft BitLocker Manager.
	`AdminKitConnector`	Network Agent Connector do zdalnego zarządzania aplikacją poprzez Kaspersky Security Center. Dostępne wartości: • `1` – Wtyczka Network Agent Connector zostanie zainstalowana. • `0` – Wtyczka Network Agent Connector nie zostanie zainstalowana.
`[Zadania]`	`ScanMyComputer`	Zadanie Pełnego skanowania. Dostępne wartości: • `1` – zadanie zostaje włączone do listy zadań Kaspersky Endpoint Security. • `0` – zadanie nie zostaje włączone do listy zadań Kaspersky Endpoint Security.
	`ScanCritical`	Zadanie Skanowanie obszarów krytycznych. Dostępne wartości: • `1` – zadanie zostaje włączone do listy zadań Kaspersky Endpoint Security. • `0` – zadanie nie zostaje włączone do listy zadań Kaspersky Endpoint Security.
	`Updater`	Zadanie aktualizacji. Dostępne wartości: • `1` – zadanie zostaje włączone do listy zadań Kaspersky Endpoint Security. • `0` – zadanie nie zostaje włączone do listy zadań Kaspersky Endpoint Security.

Kreator wstępnej konfiguracji

Po zakończeniu instalacji programu Kaspersky Endpoint Security, zostanie uruchomiony Kreator wstępnej konfiguracji aplikacji. Kreator wstępnej konfiguracji umożliwia aktywowanie aplikacji oraz zebranie informacji o aplikacjach w systemie operacyjnym. Aplikacje te są dodawane do listy zaufanych aplikacji, których akcje w systemie operacyjnym nie są w żaden sposób ograniczane.

Interfejs Kreatora wstępnej konfiguracji składa się z szeregu okien (kroków). Możesz przełączać między oknami Kreatora wstępnej konfiguracji przy pomocy przycisków **Wstecz** i **Dalej**. Aby zakończyć działanie Kreatora wstępnej konfiguracji, kliknij przycisk **Zakończ**. W celu zatrzymania Kreatora wstępnej konfiguracji w dowolnym momencie użyj przycisku **Anuluj**.

Jeżeli działanie Kreatora wstępnej konfiguracji zostanie przerwane, wartości ustawień zdefiniowane podczas jego działania nie zostaną zapisane. Przy następnej próbie użycia aplikacji rozpoczęte zostanie działanie Kreatora wstępnej konfiguracji i będziesz musiał ponownie skonfigurować ustawienia.

Aktywowanie aplikacji

Aplikacja musi być aktywowana na komputerze z aktualną datą systemową. Jeśli data systemowa zostanie zmieniona po aktywacji aplikacji, klucz nie będzie działał. Aplikacja przełączy się do trybu działania, w którym nie są pobierane uaktualnienia, a usługa Kaspersky Security Network jest niedostępna. Klucz będzie ponownie działał po przeinstalowaniu systemu operacyjnego.

W tym kroku możesz wybrać jedną z następujących opcji aktywacji programu Kaspersky Endpoint Security:

- **Aktywuj przy użyciu kodu aktywacyjnego**. Aby aktywować aplikacje kodem aktywacyjnym, wybierz tę opcję i wprowadź kod aktywacyjny.
- **Aktywuj przy użyciu pliku klucza**. Wybierz tę opcję w celu aktywowania aplikacji przy użyciu pliku klucza.
- **Aktywuj wersję testową**. Aby aktywować wersję testową, wybierz tę opcję. Użytkownik może korzystać z pełnej wersji programu przez czas przeznaczony dla wersji testowej. Po wygaśnięciu licencji, funkcjonalność aplikacji zostaje zablokowana i nie będziesz mógł ponownie aktywować wersji testowej.
- **Aktywuj później**. Wybierz tę opcję, jeżeli chcesz pominąć etap aktywacji Kaspersky Endpoint Security. Możliwe będzie używanie tylko modułu Ochrona plików i Zapora sieciowa. Po zainstalowaniu programu Kaspersky Endpoint Security, będziesz mógł zaktualizować jego bazy danych i moduły tylko jeden raz. Opcja **Aktywuj później** jest dostępna tylko przy pierwszym uruchomieniu Kreatora wstępnej konfiguracji, zaraz po zainstalowaniu aplikacji.

Do aktywacji wersji testowej lub aktywacji aplikacji przy użyciu kodu aktywacyjnego wymagane jest połączenie internetowe.

Aby kontynuować działanie Kreatora wstępnej konfiguracji, wybierz opcję aktywacji aplikacji i kliknij przycisk **Dalej**. W celu zatrzymania Kreatora wstępnej konfiguracji użyj przycisku **Anuluj**.

Aktywacja przy użyciu kodu aktywacyjnego

Krok ten jest dostępny wyłącznie podczas aktywacji aplikacji przy pomocy kodu aktywacyjnego. Krok jest pomijany, gdy aktywujesz wersję testową aplikacji lub gdy aktywujesz aplikację przy użyciu pliku klucza.

W tym kroku Kaspersky Endpoint Security wysyła dane do serwera aktywacji w celu weryfikacji wprowadzonego kodu aktywacyjnego:

- Jeżeli weryfikacja kodu aktywacyjnego zostanie zakończona pomyślnie, Kreator wstępnej konfiguracji automatycznie przejdzie do następnego okna.
- Jeżeli weryfikacja kodu zakończy się błędem, pojawi się odpowiednia informacja. W takim przypadku zalecamy skontaktowanie się ze sprzedawcą Twojej licencji do oprogramowania Kaspersky Endpoint Security.
- Jeśli liczba aktywacji kodu aktywacyjnego zostanie przekroczona, na ekranie zostanie wyświetlone odpowiednie powiadomienie. Działanie Kreatora wstępnej konfiguracji zostanie przerwane, a aplikacja zasugeruje kontakt z pomocą techniczną Kaspersky.

Aby powrócić do poprzedniego kroku Kreatora wstępnej konfiguracji, kliknij przycisk **Wstecz**. W celu zatrzymania Kreatora wstępnej konfiguracji użyj przycisku **Anuluj**.

Aktywacja przy pomocy pliku klucza

Krok ten jest dostępny tylko podczas aktywacji aplikacji przy pomocy pliku klucza.

W tym kroku określ ścieżkę do pliku klucza. W tym celu kliknij przycisk **Przeglądaj** i wybierz plik klucza w postaci `<Numer ID pliku>.key`.

Po wybraniu pliku klucza, w dolnej części okna wyświetlone są następujące informacje:

- Klucz
- Typ licencji (komercyjna lub testowa) i na ilu komputerach można ją aktywować
- Data aktywacji aplikacji na komputerze
- Data wygaśnięcia licencji
- Funkcjonalność aplikacji dostępna w zakresie licencji
- Powiadomienia o problemach z kluczem, o ile takowe wystąpiły. Na przykład, *Czarna lista kluczy jest uszkodzona*.

Aby powrócić do poprzedniego kroku Kreatora wstępnej konfiguracji, kliknij przycisk **Wstecz**. Aby przejść do następnego kroku Kreatora wstępnej konfiguracji, kliknij przycisk **Dalej**. W celu zatrzymania Kreatora wstępnej konfiguracji użyj przycisku **Anuluj**.

Wybieranie funkcji, które zostaną włączone

Krok ten jest dostępny tylko podczas aktywowania wersji testowej aplikacji.

W tym kroku możesz wybrać funkcję, która stanie się dostępna po aktywacji aplikacji:

- **Instalacja podstawowa**. Jeśli ta opcja jest zaznaczona, po aktywacji aplikacji będą dostępne tylko komponenty ochrony, Kontrola uprawnień aplikacji oraz Monitor wykrywania luk.
- **Instalacja standardowa**. Jeśli ta opcja jest zaznaczona, po aktywacji będą dostępne tylko komponenty ochrony i kontroli.
- **Pełna instalacja**. Jeśli ta opcja jest zaznaczona, po aktywacji będą dostępne wszystkie zainstalowane komponenty aplikacji, w tym funkcja szyfrowania danych.

Jeśli podczas instalacji wybrałeś większą liczbę komponentów niż jest dozwolone w licencji, po aktywacji aplikacji, komponenty, które nie są dostępne w zakresie licencji, zostaną zainstalowane, ale nie będą działać. Jeśli zakupiona licencja umożliwia korzystanie większej ilości komponentów niż są aktualnie zainstalowane, po aktywacji aplikacji, komponenty, które nie zostały zainstalowane, będą wyświetlone w sekcji **Licencjonowanie**.

Domyślnie wybrana jest standardowa instalacja.

Aby powrócić do poprzedniego kroku Kreatora wstępnej konfiguracji, kliknij przycisk **Wstecz**. Aby przejść do następnego kroku Kreatora wstępnej konfiguracji, kliknij przycisk **Dalej**. W celu zatrzymania Kreatora wstępnej konfiguracji użyj przycisku **Anuluj**.

Finalizowanie procesu aktywacji

W tym kroku Kreator wstępnej konfiguracji informuje o pomyślnej aktywacji Kaspersky Endpoint Security. Dostępne są następujące informacje o licencji:

- Typ licencji (komercyjna lub testowa) i na ilu komputerach można ją aktywować
- Data wygaśnięcia licencji
- Funkcjonalność aplikacji dostępna w zakresie licencji

Aby przejść do następnego kroku Kreatora wstępnej konfiguracji, kliknij przycisk **Dalej**. W celu zatrzymania Kreatora wstępnej konfiguracji użyj przycisku **Anuluj**.

Analizowanie systemu operacyjnego

W tym kroku gromadzone są informacje o aplikacjach, które znajdują się w systemie operacyjnym. Aplikacje te są dodawane do listy zaufanych aplikacji, których akcje w systemie operacyjnym nie są w żaden sposób ograniczane.

Pozostałe aplikacje są analizowane przy pierwszym uruchomieniu, po zainstalowaniu Kaspersky Endpoint Security.

W celu zatrzymania Kreatora wstępnej konfiguracji użyj przycisku **Anuluj**.

Kończenie wstępnej konfiguracji aplikacji

Okno kończenia działania Kreatora wstępnej konfiguracji zawiera informacje o zakończeniu procesu instalacji Kaspersky Endpoint Security.

Jeżeli chcesz uruchomić Kaspersky Endpoint Security, kliknij przycisk **Zakończ**.

Jeżeli chcesz wyjść z Kreatora wstępnej konfiguracji bez uruchamiania Kaspersky Endpoint Security, usuń zaznaczenie z pola **Uruchom Kaspersky Endpoint Security 10 for Windows** i kliknij **Zakończ**.

Umowa Kaspersky Security Network

W tym kroku Kreatora zaproponowane zostanie uczestnictwo w Kaspersky Security Network.

Przeczytaj treść Oświadczenia o Gromadzeniu Danych Kaspersky Security Network:

- Jeżeli akceptujesz wszystkie warunki, zaznacz opcję **Akceptuję warunki uczestnictwa w Kaspersky Security Network**.
- Jeśli nie akceptujesz warunków uczestnictwa w Kaspersky Security Network, zaznacz opcję **Nie akceptuję warunków uczestnictwa w Kaspersky Security Network**.

Aby kontynuować działanie Kreatora, kliknij **OK**.

Informacje o sposobach aktualizacji starszej wersji aplikacji

Aby zaktualizować poprzednią wersję aplikacji do Kaspersky Endpoint Security 10 Service Pack 2 for Windows, odszyfruj wszystkie zaszyfrowane dyski twarde.

Możesz zaktualizować następujące aplikacje do Kaspersky Endpoint Security 10 Service Pack 2 for Windows:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 (wersja 6.0.4.1424) / MP4 CF2 (wersja 6.0.4.1611)
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 (wersja 6.0.4.1424) / MP4 CF2 (wersja 6.0.4.1611)
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (wersja 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows (wersja 10.2.2.10535(MR1))
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (wersja 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (wersja 10.2.5.3201).

Jeżeli do Kaspersky Endpoint Security 10 Service Pack 2 for Windows aktualizowana jest dowolna z wymienionych powyżej aplikacji, wówczas nie jest przenoszona zawartość Kwarantanny i Kopii zapasowej.

Starszą wersję aplikacji możesz zaktualizować w następujący sposób:

- Lokalnie w trybie interaktywnym, korzystając z Kreatora instalacji aplikacji.
- Lokalnie w trybie nieinteraktywnym, z poziomu wiersza poleceń

- Zdalnie, przy użyciu programu Kaspersky Security Center (więcej informacji znajdziesz w *Przewodniku instalacji dla Kaspersky Security Center*)
- Zdalnie, poprzez Edytor zasad grupy systemu Microsoft Windows (zobacz pliki pomocy systemu operacyjnego)

Podczas aktualizacji z poprzedniej wersji aplikacji do Kaspersky Endpoint Security 10 Service Pack 2 for Windows nie ma potrzeby usuwania poprzedniej wersji. Przed aktualizacją poprzedniej wersji aplikacji zalecamy zamknięcie wszystkich uruchomionych aplikacji.

Dezinstalowanie aplikacji

Ta sekcja opisuje sposób odinstalowania programu Kaspersky Endpoint Security z komputera.

Informacje o sposobach dezinstalacji aplikacji

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

Program Kaspersky Endpoint Security można usunąć z komputera na kilka sposobów:

- Lokalnie w trybie interaktywnym, korzystając z Kreatora instalacji
- Lokalnie w trybie nieinteraktywnym, z poziomu wiersza poleceń
- Zdalnie, przy użyciu programu Kaspersky Security Center (więcej informacji znajdziesz w *Przewodniku instalacji dla Kaspersky Security Center*)
- Zdalnie, poprzez Edytor zasad grupy systemu Microsoft Windows (zobacz pliki pomocy systemu operacyjnego)

Usuwanie aplikacji przy użyciu Kreatora instalacji

W celu usunięcia Kaspersky Endpoint Security przy użyciu Kreatora instalacji:

1. W menu **Start** wybierz **Aplikacje** → **Kaspersky Endpoint Security 10 for Windows** → **Modyfikuj, Napraw lub Usuń**.

   Zostanie uruchomiony Kreator instalacji.

2. W oknie **Modyfikuj, Napraw lub Usuń** Kreatora instalacji kliknij przycisk **Usuń**.

3. Postępuj zgodnie z instrukcjami Kreatora instalacji.

Krok 1. Zapisywanie danych aplikacji do ponownego użycia

W tym kroku możesz określić, które dane używane przez aplikację chcesz zatrzymać do użycia przy kolejnej instalacji aplikacji (na przykład, podczas instalacji nowej wersji). Jeśli nie określisz żadnych danych, aplikacja zostanie całkowicie usunięta.

W celu zapisania danych aplikacji do ponownego użycia:

Zaznacz pola obok typów danych, które chcesz zapisać:

- **Dane aktywacji** – dane eliminujące potrzebę aktywacji aplikacji przy następnej instalacji. Jest aktywowana automatycznie przy pomocy bieżącej licencji, o ile licencja nie wygasła do momentu instalacji.
- **Pliki Kopii zapasowej i kwarantanny** – pliki przeskanowane przez program i umieszczone w Kwarantannie lub Kopii zapasowej.

  Dostęp do plików Kopii zapasowej i Kwarantanny, 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 i Kwarantanny po usunięciu aplikacji, przed usunięciem aplikacji musisz przywrócić je z ich miejsc przechowywania. Jednakże eksperci z Kaspersky nie zalecają przywracania plików z Kopii zapasowej i Kwarantanny, 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 bezpośredni dostęp do plików i dysków zaszyfrowanych przed usunięciem aplikacji. Dostęp do zaszyfrowanych plików i dysków można uzyskać bezpośrednio po ponownym zainstalowaniu aplikacji z funkcją szyfrowania.

  Domyślnie pole to jest zaznaczone.

Aby przejść do następnego kroku Kreatora instalacji, kliknij przycisk **Dalej**. W celu zatrzymania Kreatora instalacji użyj przycisku **Anuluj**.

Krok 2. Potwierdzenie dezinstalacji aplikacji

Ponieważ usunięcie aplikacji zagraża bezpieczeństwu Twojego komputera, będziesz musiał potwierdzić jej usunięcie. W tym celu kliknij przycisk **Usuń**.

W celu zatrzymania usuwania aplikacji w dowolnym momencie użyj przycisku **Anuluj**.

Krok 3. Dezinstalowanie aplikacji. Kończenie dezinstalacji

W tym kroku Kreator instalacji usuwa aplikację z komputera. Poczekaj na zakończenie procesu dezinstalacji aplikacji.

Podczas dezinstalacji aplikacji wymagane będzie ponowne uruchomienie systemu operacyjnego. Jeżeli anulujesz ponowne uruchomienie komputera, zakończenie procedury dezinstalacji zostanie odroczone do czasu ponownego uruchomienia systemu operacyjnego.

Dezinstalowanie programu z poziomu wiersza poleceń

Proces dezinstalacji aplikacji można uruchomić z poziomu wiersza poleceń. Dezinstalacja odbywa się w trybie interaktywnym lub cichym (bez uruchamiania Kreatora instalacji aplikacji).

W celu uruchomienia procesu dezinstalacji aplikacji w trybie interaktywnym:

w wierszu poleceń wpisz `setup.exe /x` lub `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

Zostanie uruchomiony Kreator instalacji. Postępuj zgodnie z instrukcjami Kreatora instalacji.

W celu uruchomienia procesu dezinstalacji aplikacji w trybie cichym:

w wierszu poleceń wpisz `setup.exe /s /x` lub `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`.

Zostanie uruchomiony proces dezinstalacji aplikacji w trybie cichym (bez uruchamiania Kreatora instalacji).

Jeśli operacja usunięcia aplikacji jest zabezpieczona hasłem, w wierszu polecenia należy wpisać nazwę użytkownika i hasło.

W celu odinstalowania aplikacji z poziomu wiersza poleceń w trybie interaktywnym, gdy ustawiona jest nazwa użytkownika i hasło do autoryzacji usunięcia, modyfikacji lub naprawy Kaspersky Endpoint Security:

W wierszu poleceń wpisz `setup.exe /pKLLOGIN=<Nazwa użytkownika> /pKLPASSWD=***** /x` lub

`msiexec.exe KLLOGIN=<Nazwa użytkownika> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-56E6EF762275}.`

Zostanie uruchomiony Kreator instalacji. Postępuj zgodnie z instrukcjami Kreatora instalacji.

W celu odinstalowania aplikacji z poziomu wiersza poleceń w trybie cichym, gdy ustawiona jest nazwa użytkownika i hasło do autoryzacji usunięcia, modyfikacji lub naprawy Kaspersky Endpoint Security:

W wierszu poleceń wpisz `setup.exe /pKLLOGIN=<Nazwa użytkownika> /pKLPASSWD=***** /s /x` lub

`msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLOGIN=<Nazwa użytkownika> KLPASSWD=***** /qn`.

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 dwa 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 użycia Narzędzia przywracania zaszyfrowanego urządzenia do usunięcia obiektów i danych, które pozostały po testowym działaniu Agenta autoryzacji:

1. Uruchom Narzędzie przywracania zaszyfrowanego urządzenia, uruchamiając plik wykonywalny fdert.exe utworzony przy pomocy Kaspersky Endpoint Security na komputerze z podłączonym dyskiem twardym, na którym pozostały obiekty i dane po testowym działaniu Agenta autoryzacji.
2. W oknie Narzędzia przywracania zaszyfrowanego urządzenia, z listy rozwijalnej **Wybierz urządzenie** wybierz dysk twardy z obiektami i danymi, które mają zostać usunięte.
3. Kliknij przycisk **Skanuj**.
4. Kliknij przycisk **Usuń dane i obiekty AA**.

Uruchomi to proces usuwania obiektów i danych pozostałych po testowym działaniu Agenta autoryzacji.

Po usunięciu obiektów i danych pozostałych po testowym działaniu Agenta autoryzacji, dodatkowo konieczne może być usunięcie informacji dotyczących niekompatybilności aplikacji z Agentem autoryzacji.

W celu usunięcia informacji o niekompatybilności aplikacji z Agentem autoryzacji:

w wierszu polecenia wprowadź `avp pbatestreset`.

Aby polecenie `avp pbatestreset` zostało wykonane, muszą być zainstalowane moduły szyfrujące.

Interfejs aplikacji

W tej sekcji są opisane główne elementy interfejsu aplikacji.

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.

Wskaźnik aktywności aplikacji

Ikona aplikacji służy jako wskaźnik aktywności aplikacji:

- Ikona oznacza, że wszystkie moduły ochrony są włączone.
- Ikona wskazuje na wystąpienie podczas działania Kaspersky Endpoint Security ważnego zdarzenia, wymagającego uwagi użytkownika. Na przykład moduł Ochrona plików jest wyłączony lub bazy danych aplikacji są nieaktualne.
- Ikona oznacza, że podczas działania Kaspersky Endpoint Security wystąpiło zdarzenie krytyczne. Na przykład w działaniu składnika wystąpił błąd, bądź też uszkodzone są bazy danych aplikacji.

Menu kontekstowe ikony aplikacji

Menu kontekstowe ikony aplikacji zawiera następujące elementy:

- **Kaspersky Endpoint Security 10 for Windows**. Otwiera zakładkę **Ochrona i kontrola** w oknie głównym aplikacji. Zakładka **Ochrona i kontrola** umożliwia skonfigurowanie działania składników i zadań aplikacji oraz przeglądanie statystyk przetworzonych plików i wykrytych zagrożeń.
- **Ustawienia**. Otwiera zakładkę **Ustawienia** w oknie głównym aplikacji. Zakładka **Ustawienia** umożliwia zmianę domyślnych ustawień aplikacji.
- **Wstrzymaj ochronę i kontrolę** / **Wznów ochronę i kontrolę**. Tymczasowo wstrzymuje / wznawia działanie modułów kontroli i ochrony. Ten element menu kontekstowego nie wpływa na zadanie aktualizacji i zadania skanowania, będąc dostępnym tylko wtedy, gdy wyłączony jest profil Kaspersky Security Center.
- **Wyłącz profil** / **Włącz profil**. Wyłącza / włącza profil Kaspersky Security Center. Ten element menu kontekstowego jest dostępny, gdy Kaspersky Endpoint Security działa zgodnie z profilem i ustawiono hasło do wyłączania profilu Kaspersky Security Center.
- **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

Menu kontekstowe ikony aplikacji można otworzyć, przesuwając wskaźnik myszy na ikonę aplikacji w obszarze powiadomień paska zadań Microsoft Windows i klikając ją prawym przyciskiem myszy.

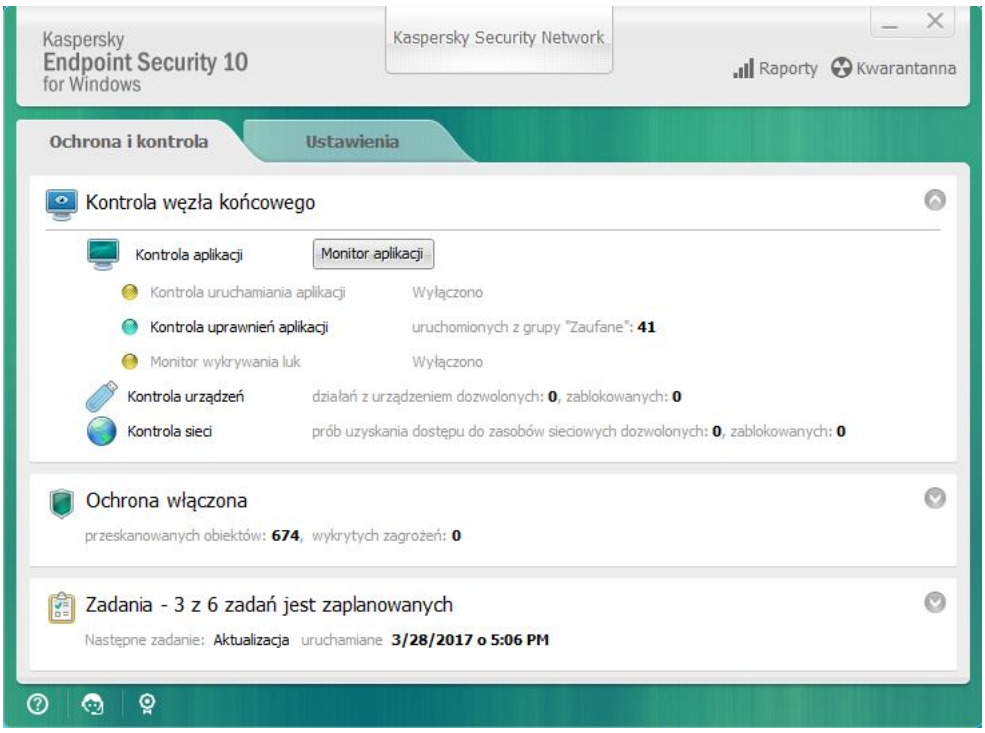
Okno główne aplikacji

Okno główne aplikacji Kaspersky Endpoint Security zawiera elementy interfejsu oferujące dostęp do wszystkich głównych funkcji programu.

Okno główne aplikacji jest podzielone na cztery części (zobacz poniższy obrazek):

- W górnej części okna znajdują się elementy interfejsu umożliwiające wyświetlenie następujących informacji:
  - Szczegółowych informacji o aplikacji
  - Statystyk Kaspersky Security Network
  - Listy nieprzetworzonych plików
  - Listy wykrytych luk
  - Listy plików poddanych kwarantannie
  - Miejsca przechowywania kopii zainfekowanych plików usuniętych przez aplikację
  - Raportów dotyczących zdarzeń, które wystąpiły podczas działania aplikacji lub poszczególnych jej składników bądź też podczas wykonywania zadań
- Zakładka **Ochrona i kontrola** umożliwia dostosowanie działania składników i wykonania zadań aplikacji. Zakładka **Ochrona i kontrola** jest wyświetlana, gdy otwierasz okno główne aplikacji.
- Zakładka **Ustawienia** umożliwia zmianę domyślnych ustawień aplikacji.
- Dolna część okna zawiera następujące elementy:
  - **Przycisk** . Kliknięcie tego przycisku przeniesie Cię do systemu pomocy Kaspersky Endpoint Security.
  - **Przycisk** . Kliknięcie tego przycisku otwiera okno **Pomoc techniczna**, które zawiera informacje o systemie operacyjnym, bieżącej wersji Kaspersky Endpoint Security oraz odnośniki do zasobów informacyjnych Kaspersky.
  - **Przycisk** / . Kliknięcie tego przycisku otwiera okno **Licencjonowanie**, które zawiera informacje o bieżącej licencji.
  - **Przycisk** / / Kliknięcie tego przycisku otwiera okno **Zdarzenia**, które zawiera informacje o dostępnych aktualizacjach, a także zgłoszenia dostępu do zaszyfrowanych plików i urządzeń.

Przycisk jest dostępny tylko wtedy, gdy są żądania dostępu lub niezainstalowane aktualizacje.



Okno główne aplikacji

W celu otwarcia okna głównego aplikacji Kaspersky Endpoint Security wykonaj jedną z następujących czynności:

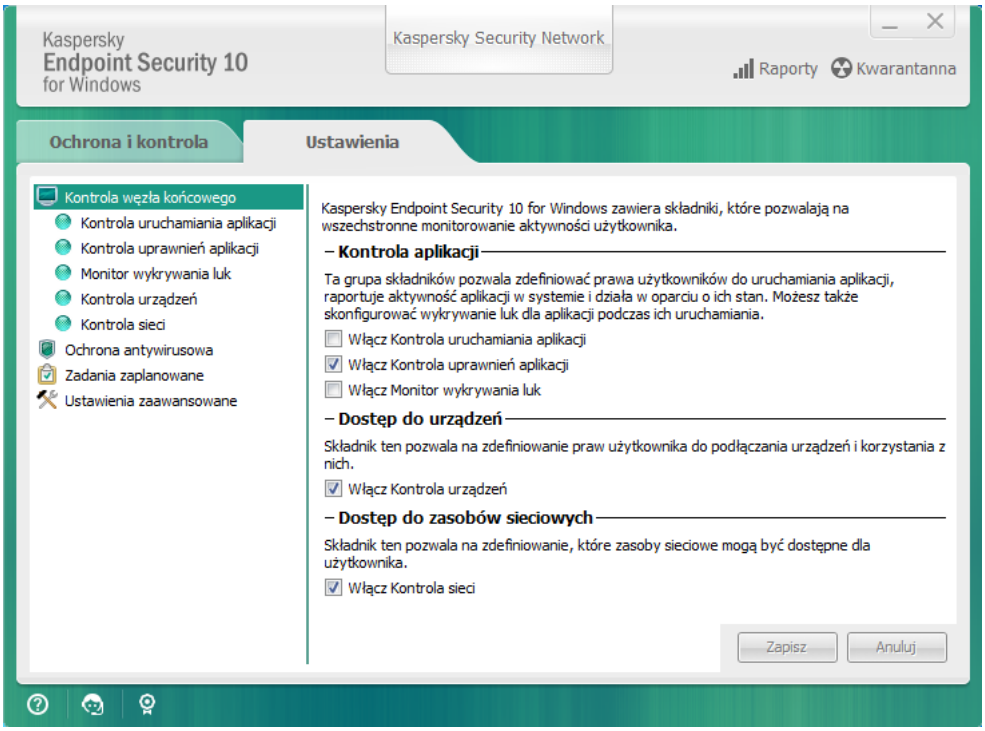
- Kliknij ikonę aplikacji w obszarze powiadomień paska zadań systemu Microsoft Windows.
- W menu kontekstowym ikony aplikacji wybierz **Kaspersky Endpoint Security 10 for Windows**.

Zakładka Konfiguracja ustawień aplikacji

Zakładka ustawień Kaspersky Endpoint Security umożliwia skonfigurowanie wszystkich ustawień aplikacji, indywidualnych składników, raportów i miejsc przechowywania, zadań skanowania, zadań aktualizacji, zadań wykrywania luk oraz komunikacji z serwerami Kaspersky Security Network.

Zakładka ustawień aplikacji składa się z dwóch części (zobacz poniższy rysunek):

- W lewej części znajdują się składniki aplikacji, zadania oraz sekcja ustawień zaawansowanych zawierająca kilka podsekcji.
- W prawej części znajdują się elementy kontroli, których można użyć do skonfigurowania ustawień komponentu lub zadania wybranego w lewej części okna, a także ustawień zaawansowanych.



Zakładka Konfiguracja ustawień aplikacji

W celu otwarcia zakładki ustawień aplikacji wykonaj jedną z następujących czynności:

- W oknie głównym aplikacji przejdź na zakładkę **Ustawienia**.
- Z otwartego menu kontekstowego ikony aplikacji wybierz **Ustawienia**.

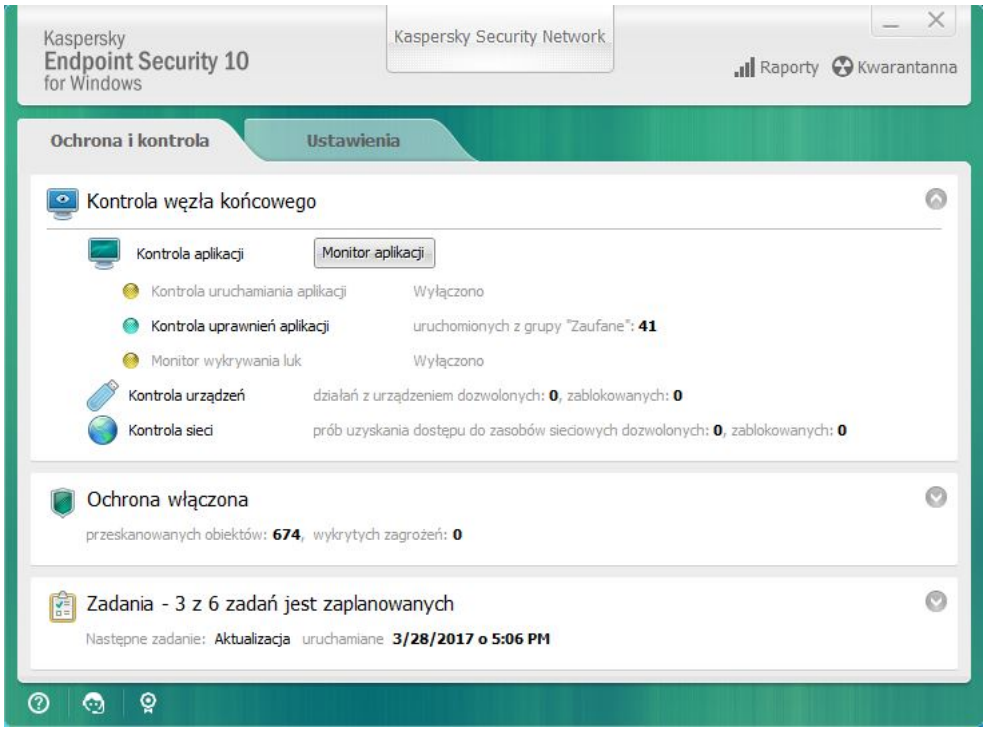
Zakładka Ochrona i kontrola aplikacji

Zakładka Ochrona i kontrola aplikacji Kaspersky Endpoint Security dostarcza ogólnych informacji o wykonaniu wszystkich zadań i działaniu wszystkich komponentów aplikacji. Na tej zakładce możesz także kontrolować działanie komponentów i wykonanie zadań.

Zakładka Ochrona i kontrola składa się z trzech części (patrz poniższy rysunek):

- Sekcja **Kontrola węzła końcowego** zawiera listę komponentów kontroli.
- Sekcja **Zarządzanie ochroną** zawiera listę komponentów ochrony antywirusowej.
- Sekcja **Zadania** zawiera listę zadań lokalnych, które są uruchomione na komputerze.

Każda sekcja zawiera elementy kontroli, których można użyć do włączenia lub wyłączenia działania komponentu, przejścia do ustawień wybranego modułu lub zadania, a także do wyświetlenia statystyk działania wybranego komponentu lub zadania.



Zakładka Ochrona i kontrola aplikacji

W celu otwarcia zakładki Ochrona i kontrola wykonaj jedną z następujących czynności:

- W oknie głównym aplikacji wybierz zakładkę **Ochrona i kontrola**.
- Kliknij ikonę aplikacji w obszarze powiadomień paska zadań systemu Microsoft Windows.
- W menu kontekstowym ikony aplikacji wybierz **Kaspersky Endpoint Security 10 for Windows**.

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 instalacji Kaspersky Endpoint Security w trybie interaktywnym.
- W pliku license.txt. Ten dokument znajduje się w pakiecie dystrybucyjnym aplikacji.

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.

Ważna licencja umożliwia korzystanie z następujących usług:

- Korzystania z aplikacji zgodnie z warunkami Umowy licencyjnej
- Pomoc techniczna

Zakres świadczonych usług 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:

- 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 (data wygaśnięcia subskrypcji, 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.

W przypadku ograniczonej subskrypcji, w momencie jej wygaśnięcia może zostać zaoferowany okres karencji dla odnowienia subskrypcji, w trakcie którego aplikacji zachowa swoją funkcjonalność. Dostawca usługi decyduje, czy przyznać okres karencji oraz określa czas dostępu okresu karencji.

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. Dodatkowy klucz może zostać zainstalowany tylko przy użyciu kodu aktywacyjnego, a nie przy użyciu pliku klucza lub podczas korzystania z subskrypcji.

Funkcjonalność aplikacji dostępna w subskrypcji może odpowiadać funkcjonalności aplikacji w następujących rodzajach licencji komercyjnej: Standard, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Licencje tego typu służą do ochrony serwerów plików, stacji roboczych i urządzeń mobilnych, a także obsługują użycie komponentów kontroli na stacjach roboczych i urządzeniach mobilnych.

Możliwe opcje zarządzania subskrypcją mogą różnić się w zależności od dostawcy usługi. Dostawca usługi może nie oferować okresu karencji dla odnowienia subskrypcji, w trakcie którego aplikacji zachowa swoją funkcjonalność.

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

Informacje o kodzie aktywacyjnym

Kod aktywacyjny to unikatowa kombinacja znaków alfanumerycznych, składająca się z dwudziestu liter i cyfr, którą otrzymasz po zakupieniu licencji komercyjnej dla 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, instalowany jest aktywny klucz. Dodatkowy klucz może zostać zainstalowany tylko przy użyciu kodu aktywacyjnego, a nie przy użyciu pliku klucza lub podczas korzystania z subskrypcji.

Jeśli po aktywacji aplikacji utracono kod aktywacyjny, będzie można go odzyskać. Kod aktywacyjny jest niezbędny, na przykład, do rejestracji w Kaspersky CompanyAccount. Aby odzyskać kod aktywacyjny, należy skontaktować się z działem pomocy technicznej Kaspersky.

Informacje o kluczu

Klucz to unikalna kombinacja znaków alfanumerycznych. Klucz umożliwia skorzystanie z aplikacji na warunkach określonych w Certyfikacie licencyjnym (typ licencji, okres ważności licencji, ograniczenia licencji).

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

Klucz można dodać do aplikacji przy pomocy kodu aktywacyjnego lub pliku klucza.

Możliwe jest dodawanie, modyfikowanie lub usuwanie kluczy. W przypadku naruszenia warunków Umowy licencyjnej, Kaspersky może zablokować klucz. Jeśli klucz został umieszczony na czarnej liście, aby kontynuować korzystanie z aplikacji, należy dodać inny klucz.

Jeśli usunięto klucz dla licencji, która utraciła ważność, funkcjonalność aplikacji będzie niedostępna. Po usunięciu tego klucza nie można dodać go ponownie.

Istnieją dwa typy kluczy: zapasowy i dodatkowy.

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.

Dodatkowy klucz to klucz, który daje użytkownikowi prawo do korzystania z aplikacji, chociaż nie jest on aktualnie w użyciu. W momencie wygaśnięcia aktywnego klucza dodatkowy klucz staje się automatycznie aktywny. Dodatkowy 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 dodatkowy. Klucz dla licencji testowej nie może zastąpić aktywnego klucza dla licencji komercyjnej.

Jeśli klucz znajdzie się na czarnej liście, funkcjonalność aplikacji określona przez licencję, zgodnie z którą działa aplikacja, pozostanie dostępna przez osiem dni. Usługa Kaspersky Security Network oraz aktualizacje modułów i baz danych aplikacji są dostępne bez ograniczeń. Aplikacja informuje użytkownika, że klucz znalazł się na czarnej liście. Po ośmiu dniach funkcjonalność aplikacji zostaje ograniczona w takim stopniu, jak w momencie wygaśnięcia licencji: aplikacja dalej działa, ale bez możliwości aktualizacji i z niedostępną usługą Kaspersky Security Network.

Informacje o pliku klucza

Plik klucza to plik z rozszerzeniem .key, który otrzymasz od Kaspersky po zakupie Kaspersky Endpoint Security. Przeznaczeniem pliku klucza jest dodanie klucza aktywującego aplikację.

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 z dostawcą licencji.
- Uzyskaj plik klucza na stronie internetowej Kaspersky w oparciu o istniejący kod aktywacyjny.

Informacje o przekazywaniu danych

Akceptując Umowę licencyjną, wyrażasz zgodę na automatyczne wysyłanie informacji związanych z korzystaniem z produktu, a także informacji dotyczących typu, wersji oraz wersji językowej zainstalowanego programu, unikatowego identyfikatora instalatora programu i typu instalacji oraz danych dotyczących aktywnego i dodatkowego klucza (w tym rodzaju licencji, okresu ważności, daty aktywacji programu i daty wygaśnięcia licencji, liczby stanowisk, bieżącego stanu licencji, wersji protokołu interakcji z serwerem aktywacji).

Jeśli program zostanie aktywowany kodem aktywacyjnym, w celu otrzymania informacji statystycznych dotyczących dystrybucji i użycia produktów Posiadacza licencji, wyrażasz zgodę na automatyczne dostarczenie wersji używanego programu (w tym informacji o zainstalowanych aktualizacjach programu, identyfikatorze instalacji programu, a także informacji o licencjach), wersji systemu operacyjnego i identyfikatorów komponentów programu aktywnych w momencie dostarczania informacji.

Kaspersky chroni otrzymywane informacje zgodnie z wymogami wynikającymi z przepisów prawa oraz zasadami obowiązującymi w Kaspersky.

Kaspersky wykorzystuje zebrane informacje w sposób całkowicie anonimowy i tylko w postaci ogólnych danych statystycznych. Ogólne statystyki są generowane automatycznie przy użyciu oryginalnych informacji i nie zawierają żadnych danych osobistych lub innych poufnych informacji. Zebrane oryginalne informacje są usuwane po zebraniu nowych informacji (raz do roku). Ogólne dane statystyczne są przechowywane cały czas.

Przeczytaj Umowę licencyjną i odwiedź stronę internetową Kaspersky, aby dowiedzieć się więcej o gromadzeniu, przetwarzaniu, przechowywaniu i niszczeniu przez Kaspersky informacji dotyczących korzystania z aplikacji po zaakceptowaniu Umowy licencyjnej i Umowy KSN. Pliki license.txt i ksn.txt zawierają Umowę licencyjną i Umowę KSN i są częścią pakietu dystrybucyjnego programu.

Przeglądanie informacji o licencji

W celu przejrzenia informacji o licencji:

1. Otwórz okno główne aplikacji.
2. Kliknij przycisk / znajdujący się w dolnej części okna głównego aplikacji.

   Zostanie otwarte okno **Licencjonowanie**. Informacje o licencji są wyświetlane w sekcji znajdującej się w górnej części okna **Licencjonowanie**.

Kupowanie licencji

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

W celu zakupienia licencji:

1. Otwórz okno główne aplikacji.
2. Kliknij przycisk / znajdujący się w dolnej części okna głównego aplikacji.

   Zostanie otwarte okno **Licencjonowanie**.
3. W oknie **Licencjonowanie** wykonaj jedną z następujących 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 licencji

Po wygaśnięciu licencji możliwe będzie jej odnowienie. Dzięki temu komputer pozostaje chroniony po wygaśnięciu bieżącej licencji i przed aktywacją aplikacji nową licencją.

W celu odnowienia licencji:

1. Uzyskaj nowy kod aktywacyjny lub plik klucza.
2. Dodaj dodatkowy klucz wraz z otrzymanym kodem aktywacyjnym lub plikiem klucza.

   W rezultacie zostanie dodany dodatkowy klucz. Stanie się aktywny po wygaśnięciu licencji.

Aktualizacja klucza z dodatkowego do aktywnego może trochę potrwać ze względu na obciążenie serwerów aktywacji Kaspersky.

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 używasz aplikacji z ograniczoną subskrypcją, w dniu wygaśnięcia subskrypcji (lub w czasie okresu karencji po wygaśnięciu subskrypcji, gdy możliwe jest odnowienie subskrypcji) program Kaspersky Endpoint Security wyświetli odpowiedni komunikat i zaprzestanie prób 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.

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

Odwiedzanie strony dostawcy usługi

W celu odwiedzenia strony dostawcy usługi z poziomu interfejsu aplikacji:

1. Otwórz okno główne aplikacji.
2. Kliknij przycisk / znajdujący się w dolnej części okna głównego aplikacji.
   Zostanie otwarte okno **Licencjonowanie**.
3. W oknie **Licencjonowanie** kliknij **Skontaktuj się z dostawcą usługi**.

Informacje o metodach aktywacji aplikacji

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

Możesz aktywować aplikację na jeden z następujących sposobów:

- W trakcie instalowania aplikacji, przy pomocy Kreatora wstępnej konfiguracji. W ten sposobów możesz dodać aktywny klucz.
- Lokalnie, z poziomu interfejsu aplikacji, używając Kreatora aktywacji. W ten sposób możesz dodać aktywny i dodatkowy klucz.
- Zdalnie, przy użyciu programu Kaspersky Security Center, tworząc i uruchamiając zadanie dodania klucza. W ten sposób możesz dodać aktywny i dodatkowy klucz.

- Zdalnie, poprzez dystrybucję kluczy i kodów aktywacyjnych, które są przechowywane w magazynie kluczy na Serwerze administracyjnym Kaspersky Security Center, na komputery klienckie (szczegółowy opis znajduje się w *Podręczniku administratora dla Kaspersky Security Center*). W ten sposób możesz dodać aktywny i dodatkowy 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.

Aktywacja aplikacji za pomocą Kreatora aktywacji

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

1. Kliknij przycisk / znajdujący się w dolnej części okna głównego aplikacji.

   Zostanie otwarte okno **Licencjonowanie**.

2. W oknie **Licencjonowanie** kliknij przycisk **Aktywuj aplikację przy użyciu nowej licencji**.

   Zostanie uruchomiony Kreator aktywacji aplikacji.

3. Postępuj zgodnie z instrukcjami Kreatora aktywacji.

Więcej informacji na temat procedury aktywacji aplikacji można znaleźć w sekcji dotyczącej Kreatora wstępnej konfiguracji.

Aktywowanie programu z poziomu wiersza poleceń

W celu aktywowania programu z poziomu wiersza poleceń:

w wierszu poleceń wpisz `avp.com license /add <kod aktywacyjny lub plik klucza> /password= <hasło>`.

Uruchamianie i zatrzymywanie działania aplikacji

Sekcja zawiera informacje dotyczące konfiguracji automatycznego uruchamiania aplikacji, ręcznego uruchamiania i zatrzymywania działania aplikacji oraz wstrzymywania i wznawiania działania modułów ochrony i kontroli.

Włączanie i wyłączanie automatycznego uruchamiania aplikacji

Automatyczne uruchamianie oznacza, że Kaspersky Endpoint Security uruchamia się przy starcie systemu operacyjnego, bez udziału użytkownika. Ta opcja uruchamiania aplikacji jest włączona domyślnie.

Po instalacji Kaspersky Endpoint Security uruchamia się automatycznie po raz pierwszy. Kolejne uruchomienia aplikacji odbywają się automatycznie podczas ładowania 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.

W celu włączenia lub wyłączenia automatycznego uruchamiania aplikacji:

1. Otwórz okno ustawień aplikacji.
2. Wybierz sekcję **Ochrona antywirusowa** znajdującą się po lewej stronie.

   W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.
3. Wykonaj jedną z poniższych czynności:
   - Jeśli chcesz włączyć automatyczne uruchamianie aplikacji, zaznacz pole **Uruchom Kaspersky Endpoint Security 10 for Windows podczas ładowania systemu**.
   - Jeśli chcesz wyłączyć automatyczne uruchamianie aplikacji, odznacz pole **Uruchom Kaspersky Endpoint Security 10 for Windows podczas ładowania systemu**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Ręczne uruchamianie i zatrzymywanie działania aplikacji

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

Kaspersky Endpoint Security musi zostać uruchomiony ręcznie, jeśli wcześniej wyłączyłeś automatyczne uruchamianie aplikacji.

W celu ręcznego uruchomienia aplikacji:

W menu **Start** wybierz **Aplikacje** → **Kaspersky Endpoint Security 10 for Windows**.

W celu ręcznego zatrzymania działania aplikacji:

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

Wstrzymywanie i wznawianie kontroli i ochrony komputera

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

Stan aplikacji jest wyświetlany przy pomocy ikony aplikacji w obszarze powiadomień paska zadań.

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

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

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

W celu wstrzymania kontroli i ochrony komputera:

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

   Zostanie otwarte okno **Wstrzymaj ochronę**.
3. Wybierz jedną z następujących opcji:
   - **Wstrzymaj na określony czas** – kontrola i ochrona komputera zostaną wznowione po upłynięciu czasu wybranego z listy rozwijalnej dostępnej poniżej.
   - **Wstrzymaj do restartu** – 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. Jeśli w poprzednim kroku wybrałeś opcję **Wstrzymaj na określony czas**, z listy rozwijalnej wybierz żądany przedział czasu.

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 i kontrolę**.

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

Ochrona systemu plików komputera. Ochrona plików

Sekcja ta zawiera informacje o module Ochrona plików oraz instrukcje dotyczące konfiguracji jego ustawień.

Informacje o module Ochrona plików

Moduł Ochrona plików zapobiega zainfekowaniu systemu plików komputera. Domyślnie Ochrona plików uruchamia się wraz z Kaspersky Endpoint Security, pozostaje w pamięci komputera i skanuje wszystkie pliki otwierane, zapisywane i uruchamiane na komputerze i wszystkich podłączonych do niego dyskach w poszukiwaniu wirusów i innych zagrożeń.

Po wykryciu zagrożenia w pliku Kaspersky Endpoint Security wykonuje następujące czynności:

1. Wykrywa typ obiektu wykrytego w pliku (taki jak *wirus* lub *trojan*).
2. Stan *prawdopodobnie zainfekowany* jest przypisywany w sytuacji, gdy nie można jednoznacznie określić, czy plik jest zainfekowany. Plik może zawierać sekwencję kodu typową dla wirusów i innych szkodliwych programów lub zmodyfikowany kod znanego wirusa.
3. Następnie aplikacja wyświetla powiadomienie o wykryciu szkodliwego obiektu w pliku (jeśli skonfigurowano powiadomienia) i wykonuje na nim akcję określoną w ustawieniach Ochrony plików.

Włączanie i wyłączanie modułu Ochrona plików

Domyślnie moduł Ochrona plików jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky. W razie konieczności możesz wyłączyć Ochronę plików.

Istnieją dwa sposoby włączania i wyłączania komponentu:

- W oknie głównym aplikacji, na zakładce**Ochrona i kontrola**
- Z poziomu okna ustawień aplikacji

W celu włączenia lub wyłączenia modułu Ochrona plików w oknie głównym aplikacji, na zakładce Ochrona i kontrola:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Ochrona**.

   Zostanie otwarta sekcja **Ochrona**.
4. Kliknij prawym przyciskiem myszy wiersz z informacjami o module Ochrona plików, aby otworzyć menu kontekstowe.

   Zostanie otwarte menu wyboru działań.
5. Wykonaj jedną z poniższych czynności:
   - Aby włączyć moduł Ochrona plików, wybierz z menu opcję **Włącz**.

Ikona stanu modułu , wyświetlana w lewej części wiersza **Ochrona plików**, zmieni się na ikonę .

- Aby wyłączyć moduł Ochrona plików, wybierz z menu opcję **Wyłącz**.

  Ikona stanu modułu , wyświetlana w lewej części wiersza **Ochrona plików**, zmieni się na ikonę .

W celu włączenia lub wyłączenia modułu Ochrona plików z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona plików**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona plików.
3. Wykonaj jedną z poniższych czynności:
   - Jeżeli chcesz włączyć Ochronę plików, zaznacz pole **Włącz moduł Ochrona plików**.
   - Jeżeli chcesz wyłączyć Ochronę plików, usuń zaznaczenie z pola **Włącz moduł Ochrona plików**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Automatyczne wstrzymywanie modułu Ochrona plików

Możesz skonfigurować moduł Ochrona plików tak, aby był automatycznie wstrzymywany o określonym czasie lub przy uruchamianiu określonych programów.

Wstrzymywanie modułu Ochrona plików w sytuacji, gdy powoduje konflikty z innymi programami, jest działaniem wyjątkowym. Jeżeli podczas pracy modułów wystąpią jakieś problemy, skontaktuj się ze specjalistami z działu pomocy technicznej firmy Kaspersky (https://companyaccount.kaspersky.com). Specjaliści z pomocy technicznej pomogą Ci skonfigurować Ochronę plików do jednoczesnego działania z innymi programami na Twoim komputerze.

W celu skonfigurowania automatycznego wstrzymywania Ochrony plików:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona plików**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona plików.
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona plików**.
4. W oknie **Ochrona plików** przejdź na zakładkę **Dodatkowe**.
5. W sekcji **Wstrzymaj zadanie**:
   - Aby skonfigurować automatyczne wstrzymywanie Ochrony plików o określonym czasie, zaznacz pole **Zgodnie z terminarzem** i kliknij przycisk **Terminarz**.

     Zostanie otwarte okno **Wstrzymaj zadanie**.
   - Aby skonfigurować automatyczne wstrzymywanie Ochrony plików przy uruchamianiu określonych aplikacji, zaznacz pole **Podczas uruchamiania aplikacji** i kliknij przycisk **Wybierz**.

Zostanie otwarte okno **Aplikacje**.

6. Wykonaj jedną z poniższych czynności:

   - Jeżeli chcesz skonfigurować automatyczne wstrzymywanie Ochrony plików o określonym czasie, w oknie **Wstrzymaj zadanie** użyj pól **Wstrzymaj zadanie o** i **Wznów zadanie o**, aby określić przedział czasu (w formacie GG:MM), podczas którego działanie modułu Ochrona plików zostanie wstrzymane. Kliknij **OK**.

   - Jeśli chcesz skonfigurować automatyczne wstrzymywanie Ochrony plików po uruchomieniu określonych aplikacji, użyj przycisków **Dodaj**, **Modyfikuj** i **Usuń** znajdujących się w oknie **Aplikacje**, aby utworzyć listę aplikacji, podczas pracy których działanie modułu Ochrona plików ma być wstrzymane. Kliknij **OK**.

7. W oknie **Ochrona plików** kliknij **OK**.

8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Konfigurowanie ustawień modułu Ochrona plików

Podczas konfigurowania modułu Ochrona plików można:

- Zmienić poziom ochrony.

  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.

- Zmienić akcję podejmowaną przez Ochronę plików po wykryciu zainfekowanego pliku.

- Zmodyfikować obszar ochrony modułu Ochrona plików.

  Możesz poszerzyć lub ograniczyć obszar ochrony, dodając bądź usuwając skanowane obiekty lub zmieniając typ skanowanych plików.

- Skonfigurować analizator heurystyczny.

  Ochrona plików wykorzystuje technologię zwaną analizą sygnatur. Podczas analizy sygnatur Ochrona plików porównuje wykryty obiekt z wpisami w antywirusowych bazach danych aplikacji. Zgodnie z zaleceniami ekspertów z Kaspersky, analiza sygnatur jest zawsze włączona.

  Aby zwiększyć efektywność ochrony, możesz użyć analizy heurystycznej. Podczas analizy heurystycznej Ochrona plików analizuje aktywność obiektów w systemie operacyjnym. Analiza heurystyczna może wykrywać szkodliwe programy, dla których nie ma jeszcze wpisów w antywirusowych bazach danych aplikacji.

- Zoptymalizować skanowanie.

  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.

- Skonfigurować skanowanie plików złożonych.

- Zmienić tryb skanowania plików.

Zmienianie poziomu ochrony

Aby chronić system plików komputera, Ochrona plików stosuje różne grupy ustawień. Takie grupy ustawień nazywane są *poziomami ochrony*. Dostępne są trzy predefiniowane poziomy ochrony: **Wysoki**, **Zalecany** i **Niski**. Ustawienia poziomu ochrony **Zalecany** są uważane za optymalne ustawienia zalecane przez ekspertów z Kaspersky.

W celu zmiany poziomu ochrony:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona plików**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona plików.
3. W sekcji **Poziom ochrony** wykonaj jedną z poniższych czynności:

   - Jeśli chcesz ustawić jeden z predefiniowanych poziomów ochrony (**Wysoki**, **Zalecany** lub **Niski**), wybierz go, korzystając z suwaka.
   - Jeżeli chcesz skonfigurować niestandardowy poziom ochrony, kliknij przycisk **Ustawienia** i w otwartym oknie **Ochrona plików** wprowadź swoje ustawienia.

     Po skonfigurowaniu niestandardowego poziomu ochrony, nazwa poziomu ochrony w sekcji **Poziom ochrony** zmieni się na **Niestandardowy**.
   - Jeżeli chcesz zmienić poziom ochrony na **Zalecany**, kliknij przycisk **Domyślny**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zmienianie akcji podejmowanej przez Ochronę plików na zainfekowanych plikach

W celu zmiany akcji podejmowanej przez Ochronę plików na zainfekowanych plikach:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona plików**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona plików.
3. W sekcji **Działanie podejmowane w przypadku wykrycia zagrożenia** wybierz żądaną opcję:

   - **Automatycznie wybierz akcję**.
   - **Wybierz akcję: Wykonaj leczenie. Usuń, jeśli leczenie nie jest możliwe**.
   - **Wybierz akcję: Wykonaj leczenie**.

     Nawet jeśli wybrano tę opcję, Kaspersky Endpoint Security zastosuje akcję **Usuń** dla plików będących częścią aplikacji ze Sklepu Windows.

- **Wybierz akcję: Usuń**.
- **Wybierz akcję: Zablokuj**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Modyfikowanie 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 Ochrona plików skanuje tylko potencjalnie infekowalne pliki uruchamiane z dysków twardych, dysków sieciowych lub nośników wymiennych.

W celu utworzenia obszaru ochrony:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona plików**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona plików.
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona plików**.
4. W oknie **Ochrona plików** przejdź na zakładkę **Ogólne**.
5. W sekcji **Typy plików** określ typy plików, które mają być skanowane:
   - Jeżeli skanowane mają być wszystkie pliki, zaznacz pole **Wszystkie pliki**.
   - Jeżeli skanowaniu mają podlegać pliki o formatach najbardziej podatnych na infekcje, wybierz opcję **Pliki skanowane według formatu**.
   - Jeżeli skanowaniu mają podlegać pliki z rozszerzeniami najbardziej podatnymi na infekcje, zaznacz pole **Pliki skanowane według rozszerzenia**.

   Podczas wybierania typu skanowanych plików należy pamiętać, że:
   - Istnieją formaty plików (takie jak .txt), dla których prawdopodobieństwo zarażenia szkodliwym kodem i jego późniejszej aktywacji jest dość niskie. Istnieją jednak formaty zawierające lub mogące zawierać kod wykonywalny (na przykład .exe, .dll, .doc). Ryzyko przeniknięcia i aktywacji szkodliwego kodu w takich plikach jest bardzo wysokie.
   - Haker może przesłać na Twój komputer wirusa lub inne szkodliwe oprogramowanie w pliku wykonywalnym posiadającym rozszerzenie txt. Jeżeli wybrałeś opcję skanowania plików według rozszerzenia, taki plik zostanie pominięty podczas skanowania. Jeśli wybrałeś skanowanie plików według formatu, bez względu na rozszerzenie Ochrona plików przeanalizuje nagłówek pliku. Taka analiza może wykryć, że plik ma format .exe. Taki plik zostanie poddany szczegółowemu skanowaniu antywirusowemu.
6. Na liście **Obszar ochrony** należy wykonać jedną z następujących czynności:
   - Jeśli chcesz dodać nowy obiekt do obszaru skanowania, kliknij przycisk **Dodaj**.

- Jeżeli chcesz zmienić lokalizację obiektu, wybierz go z obszaru skanowania i kliknij przycisk **Modyfikuj**.

Zostanie otwarte okno **Określ obszar skanowania**.

- Jeżeli chcesz usunąć obiekt z listy skanowanych obiektów, wybierz go z listy i kliknij przycisk **Usuń**.

  Zostanie wyświetlone okno potwierdzenia usunięcia obiektu.

7. Wykonaj jedną z poniższych czynności:

   - Jeżeli chcesz dodać nowy obiekt do listy skanowanych lub zmienić lokalizację obiektu znajdującego się na liście, wybierz go w oknie **Określ obszar skanowania** i kliknij przycisk **Dodaj**.

     Wszystkie obiekty wybrane w oknie **Określ obszar skanowania** są wyświetlane w oknie **Ochrona plików**, na liście **Obszar ochrony**.

     Kliknij **OK**.

   - Jeżeli chcesz usunąć obiekt, kliknij przycisk **Tak** w oknie potwierdzenia usunięcia obiektu.

8. Jeżeli to konieczne, powtórz kroki 6-7, aby dodać, przenieść lub usunąć obiekty z listy skanowanych.

9. Aby wykluczyć obiekt z listy skanowanych, na liście **Obszar ochrony** usuń zaznaczenie z pola znajdującego się obok niego. Obiekt zostaje wykluczony ze skanowania, ale nadal znajduje się na liście.

10. W oknie **Ochrona plików** kliknij **OK**.

11. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Używanie Analizatora heurystycznego z Ochroną plików

W celu skonfigurowania korzystania z Analizatora heurystycznego w trakcie działania Ochrony plików:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona plików**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona plików.

3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona plików**.

4. W oknie **Ochrona plików** przejdź na zakładkę **Wydajność**.

5. W sekcji **Metody skanowania**:

   - Jeżeli chcesz, aby Ochrona plików korzystała z analizy heurystycznej, zaznacz pole **Analiza heurystyczna** i użyj suwaka w celu ustawienia poziomu analizy heurystycznej: **Niski**, **Średni** lub **Szczegółowy**.

   - Jeżeli nie chcesz, aby Ochrona plików korzystała z analizy heurystycznej, usuń zaznaczenie z pola **Analiza heurystyczna**.

6. Kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Wykorzystywanie technologii skanowania w działaniu Ochrony plików

W celu skonfigurowania korzystania z technologii skanowania w trakcie działania Ochrony plików:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona plików**.
   W prawej części okna wyświetlone są ustawienia modułu Ochrona plików.
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
   Zostanie otwarte okno **Ochrona plików**.
4. W oknie **Ochrona plików** przejdź na zakładkę **Dodatkowe**.
5. W sekcji **Technologie skanowania**:
   - Zaznacz pola obok nazw technologii, które mają być wykorzystane w działaniu Ochrony plików.
   - Usuń zaznaczenia z pól obok nazw technologii, które nie będą wykorzystywane w działaniu Ochrony plików.
6. Kliknij **OK**.
7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Optymalizowanie skanowania plików

W celu zoptymalizowania skanowania plików:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona plików**.
   W prawej części okna wyświetlone są ustawienia modułu Ochrona plików.
3. Kliknij przycisk **Ustawienia**.
   Zostanie otwarte okno **Ochrona plików**.
4. W oknie **Ochrona plików** przejdź na zakładkę **Wydajność**.
5. W sekcji **Optymalizacja skanowania** zaznacz pole **Skanuj tylko nowe i zmienione pliki**.
6. Kliknij **OK**.
7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Skanowanie plików złożonych

Popularną techniką ukrywania wirusów i innego szkodliwego oprogramowania jest osadzanie ich w plikach złożonych, takich jak archiwa czy pocztowe 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 zbiór 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. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona plików**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona plików.
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona plików**.
4. W oknie **Ochrona plików** przejdź na zakładkę **Wydajność**.
5. W sekcji **Skanowanie plików złożonych** określ, które pliki złożone mają być skanowane: archiwa, pakiety instalacyjne lub pliki w formatach pakietu Office.
6. Aby skanować tylko nowe i zmienione pliki złożone, zaznacz pole **Skanuj tylko nowe i zmienione pliki**.

   Ochrona plików będzie skanowała tylko nowe i zmienione pliki złożone wszystkich typów.
7. Kliknij przycisk **Dodatkowe**.

   Zostanie otwarte okno **Pliki złożone**.
8. W sekcji **Skanowanie w tle** wykonaj jedną z poniższych czynności:

   - Jeżeli nie chcesz, aby Ochrona plików rozpakowywała pliki złożone w tle, usuń zaznaczenie z pola **Rozpakowywanie plików złożonych w tle**.
   - Jeżeli chcesz, aby Ochrona plików rozpakowywała duże pliki złożone w tle, zaznacz pole **Rozpakowywanie plików złożonych w tle** i określ żądaną wartość w polu **Minimalny rozmiar pliku**.
9. W sekcji **Ograniczenie rozmiaru** wykonaj jedną z poniższych czynności:

   - Aby Ochrona plików nie rozpakowywała dużych plików złożonych, zaznacz pole **Nie rozpakowuj dużych plików złożonych** i określ żądaną wartość w polu **Maksymalny rozmiar pliku**. Ochrona plików nie będzie rozpakowywać plików złożonych, których rozmiar jest większy niż określona wartość.
   - Aby Ochrona plików rozpakowywała duże pliki złożone, usuń zaznaczenie z pola **Nie rozpakowuj dużych plików złożonych**.

Plik zostanie zaklasyfikowany jako duży, jeśli jego rozmiar przekroczy wartość zdefiniowaną w polu **Maksymalny rozmiar pliku**.

Ochrona plików skanuje duże pliki wypakowane z archiwów, bez względu na to, czy pole **Nie rozpakowuj dużych plików złożonych** jest zaznaczone.

10. Kliknij **OK**.
11. W oknie **Ochrona plików** kliknij **OK**.
12. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zmienianie trybu skanowania

Tryb skanowania to warunek, zgodnie z którym Ochrona plików rozpoczyna skanowanie 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. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona plików**.
   W prawej części okna wyświetlone są ustawienia modułu Ochrona plików.
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
   Zostanie otwarte okno **Ochrona plików**.
4. W oknie **Ochrona plików** przejdź na zakładkę **Dodatkowe**.
5. W sekcji **Tryb skanowania** wybierz żądany tryb:
   - **Tryb smart**.
   - **Podczas dostępu i modyfikacji**.
   - **Podczas dostępu**.
   - **Podczas wykonywania**.
6. Kliknij **OK**.
7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Ochrona poczty. Ochrona poczty

Komponent jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów plików.

Sekcja ta zawiera informacje o Ochronie poczty oraz instrukcje dotyczące konfiguracji ustawień modułu.

Informacje o module Ochrona poczty

Ochrona poczty skanuje odbierane i wysyłane wiadomości e-mail w poszukiwaniu wirusów i innych zagrożeń. Ochrona poczty uruchamia się wraz z Kaspersky Endpoint Security, pozostaje w pamięci komputera i skanuje wszystkie wiadomości pocztowe przesyłane za pośrednictwem protokołów POP3, SMTP, IMAP, MAPI i NNTP. Jeżeli program nie wykryje zagrożenia w wiadomości, stanie się ona dostępna dla użytkownika.

Po wykryciu zagrożenia w wiadomości e-mail, Ochrona poczty wykona następujące czynności:

1. Identyfikuje typ obiektu wykrytego w wiadomości e-mail (taki jak *trojan*).
2. Do wiadomości zostaje przypisany jeden z następujących stanów:
   - *Prawdopodobnie zainfekowany*. Ten stan jest przypisywany, gdy nie można jednoznacznie uznać wiadomości za zainfekowaną. Wiadomość może zawierać sekwencję kodu typową dla wirusów lub innych szkodliwych programów lub zmodyfikowany kod znanego wirusa.
   - *Zainfekowany*. Ten stan jest przydzielany do obiektu, jeśli skanowanie wiadomości wykryje sekwencję kodu znanego wirusa, znajdującego się w antywirusowych bazach danych Kaspersky Endpoint Security.
   - *Nie wykryto*. Ten stan jest przypisywany do obiektu, jeśli skanowanie wiadomości e-mail nie wykryje wirusa ani innych zagrożeń.

Następnie aplikacja blokuje wiadomość e-mail, wyświetla powiadomienie o wykrytym obiekcie (jeśli zostało to określone w ustawieniach powiadomień) oraz wykonuje akcję określoną w ustawieniach Ochrony poczty.

Składnik współdziała z klientami poczty e-mail zainstalowanymi na komputerze. Dla klienta poczty e-mail Microsoft Office Outlook® dostępne jest rozszerzenie, które umożliwia wygodną konfigurację ustawień skanowania poczty. Rozszerzenie Ochrony poczty jest integrowane z programem pocztowymi Microsoft Office Outlook w trakcie instalacji Kaspersky Endpoint Security.

Działanie Ochrony poczty jest sygnalizowane przez ikonę aplikacji w obszarze powiadomień paska zadań. Gdy Ochrona poczty skanuje wiadomość pocztową, ikona aplikacji zmienia się na .

Włączanie i wyłączanie modułu Ochrona poczty

Domyślnie moduł Ochrona poczty jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky. W razie konieczności możesz wyłączyć Ochronę poczty.

Istnieją dwa sposoby włączania i wyłączania komponentu:

- W oknie głównym aplikacji, na zakładce**Ochrona i kontrola**

- Z poziomu okna ustawień aplikacji

W celu włączenia lub wyłączenia modułu Ochrona poczty w oknie głównym aplikacji, na zakładce Ochrona i kontrola:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Ochrona**.

   Zostanie otwarta sekcja **Ochrona**.
4. Kliknij prawym przyciskiem myszy wiersz z informacjami o module Ochrona poczty, aby otworzyć menu kontekstowe.

   Zostanie otwarte menu wyboru działań.
5. Wykonaj jedną z poniższych czynności:

   - Aby włączyć moduł Ochrona poczty, wybierz z menu opcję **Włącz**.

     Ikona stanu modułu , wyświetlana w lewej części wiersza **Ochrona poczty**, zmieni się na ikonę .
   - Aby wyłączyć moduł Ochrona poczty, wybierz z menu opcję **Wyłącz**.

     Ikona stanu modułu , wyświetlana w lewej części wiersza **Ochrona poczty**, zmieni się na ikonę .

W celu włączenia lub wyłączenia modułu Ochrona poczty z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona poczty**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona poczty.
3. Wykonaj jedną z poniższych czynności:

   - Jeżeli chcesz włączyć Ochronę poczty, zaznacz pole **Włącz moduł Ochrona poczty**.
   - Jeżeli chcesz wyłączyć Ochronę poczty, usuń zaznaczenie z pola **Włącz moduł Ochrona poczty**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Konfigurowanie ustawień modułu Ochrona poczty

Podczas konfigurowania modułu Ochrona poczty można:

- Zmienić poziom ochrony poczty.

  Możesz wybrać jeden z predefiniowanych poziomów ochrony poczty lub skonfigurować niestandardowy poziom ochrony poczty.

  Jeśli zmieniłeś ustawienia poziomu ochrony poczty, możesz zawsze powrócić do zalecanych ustawień poziomu ochrony poczty.
- Zmienić akcję podejmowaną przez Kaspersky Endpoint Security na zainfekowanych wiadomościach.

- Zmodyfikować obszar ochrony modułu Ochrona poczty.
- Skonfigurować 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.
- Skonfigurować filtrowanie według typu załączników w wiadomościach.

  Filtrowanie załączników według typu umożliwia automatyczne zmienianie nazw i usuwanie plików określonych typów.
- Skonfigurować analizator heurystyczny.

  Aby zwiększyć efektywność ochrony, możesz użyć analizy heurystycznej. Podczas analizy heurystycznej Kaspersky Endpoint Security analizuje aktywność aplikacji w systemie operacyjnym. Analiza heurystyczna może wykryć w wiadomościach zagrożenia, dla których aktualnie nie ma wpisów w bazach danych Kaspersky Endpoint Security.
- Skonfigurować skanowanie poczty elektronicznej w programie Microsoft Office Outlook.

  Dla klienta poczty e-mail Microsoft Office Outlook dostępne jest rozszerzenie, które umożliwia wygodną konfigurację ustawień skanowania poczty.

  Podczas pracy z innymi klientami poczty e-mail (w tym Microsoft Outlook Express®, Poczta systemu Windows i Mozilla™ Thunderbird™) moduł Ochrona poczty skanuje ruch przesyłane po protokołach SMTP, POP3, IMAP oraz NNTP.

  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**.

Zmienianie poziomu ochrony poczty

Aby chronić pocztę elektroniczną, Ochrona poczty stosuje różne grupy ustawień. Te grupy ustawień są zwane *poziomami ochrony poczty*. Dostępne są trzy predefiniowane poziomy ochrony poczty: **Wysoki**, **Zalecany** i **Niski**. **Zalecany** poziom ochrony plików jest uważany za optymalne ustawienie i jest zalecany przez Kaspersky.

W celu zmiany poziomu ochrony poczty:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona poczty**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona poczty.
3. W sekcji **Poziom ochrony** wykonaj jedną z poniższych czynności:
   - Jeżeli chcesz wybrać jeden z predefiniowanych poziomów ochrony poczty (**Wysoki**, **Zalecany** lub **Niski**), użyj suwaka.
   - Jeżeli chcesz skonfigurować niestandardowy poziom ochrony poczty, kliknij przycisk **Ustawienia** i w otwartym oknie **Ochrona poczty** określ swoje ustawienia.

     Po skonfigurowaniu niestandardowego poziomu ochrony poczty, nazwa poziomu ochrony w sekcji **Poziom ochrony** zmieni się na **Niestandardowy**.

- Jeżeli chcesz zmienić poziom ochrony poczty na **Zalecany**, kliknij przycisk **Domyślny**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zmienianie akcji podejmowanej na zainfekowanych wiadomościach e-mail

W celu zmiany akcji podejmowanej na zainfekowanych wiadomościach e-mail:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona poczty**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona poczty.

3. W sekcji **Działanie podejmowane w przypadku wykrycia zagrożenia** wybierz akcję, jaką Kaspersky Endpoint Security wykona po wykryciu zainfekowanej wiadomości:

   - **Automatycznie wybierz akcję**.
   - **Wybierz akcję: Wykonaj leczenie. Usuń, jeśli leczenie nie jest możliwe**.
   - **Wybierz akcję: Wykonaj leczenie**.
   - **Wybierz akcję: Usuń**.
   - **Wybierz akcję: Zablokuj**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Modyfikowanie 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. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona poczty**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona poczty.

3. Kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona poczty**.

4. Przejdź na zakładkę **Ogólne**.

5. W sekcji **Obszar ochrony** należy wykonać jedną z następujących czynności:

   - Jeżeli chcesz, aby Ochrona poczty skanowała wszystkie przychodzące i wychodzące wiadomości na Twoim komputerze, wybierz opcję **Wiadomości odbierane i wysyłane**.

   - Jeśli chcesz, aby Ochrona poczty skanowała tylko wiadomości przychodzące, wybierz opcję **Tylko wiadomości odbierane**.

     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.

6. 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 Twój komputer, zaznacz pole **Ruch POP3 / SMTP / NNTP / IMAP**.

     Jeśli nie chcesz, aby Ochrona poczty skanowała wiadomości pocztowe przesyłane poprzez protokoły POP3, SMTP, NNTP i IMAP zanim dotrą one na Twój komputer, usuń zaznaczenie z pola **Ruch POP3 / SMTP / NNTP / IMAP**. W tym przypadku wiadomości są skanowane przez rozszerzenie Ochrony poczty osadzone w programie pocztowym Microsoft Office Outlook po dotarciu na komputer (jeśli zaznaczone jest pole **Dodatkowe: rozszerzenie do Microsoft Office Outlook**).

     Jeśli korzystasz z klientów poczty innych niż Microsoft Office Outlook, wiadomości przesyłane poprzez protokoły POP3, SMTP, NNTP i IMAP nie są skanowane przez moduł Ochrona poczty, jeżeli pole **Ruch POP3 / SMTP / NNTP / 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 **Dodatkowe: rozszerzenie do Microsoft Office 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 **Dodatkowe: rozszerzenie do Microsoft Office Outlook**.

     Rozszerzenie Ochrony poczty jest integrowane z programem pocztowymi Microsoft Office Outlook w trakcie instalacji Kaspersky Endpoint Security.

7. Kliknij **OK**.

8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Skanowanie plików złożonych załączonych do wiadomości e-mail

W celu skanowania plików złożonych załączonych do wiadomości e-mail:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona poczty**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona poczty.

3. Kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona poczty**.

4. Przejdź na zakładkę **Ogólne**.

5. W sekcji **Skanowanie plików złożonych** wykonaj następujące czynności:

   - Jeśli chcesz, aby Ochrona poczty pomijała archiwa załączone do wiadomości pocztowych, usuń zaznaczenie z pola **Skanuj załączone archiwa**.
   - Jeśli chcesz, aby Ochrona poczty pomijała załączniki większe niż N megabajtów, zaznacz pole **Nie skanuj archiwów większych niż N MB**. Jeśli zaznaczysz tę opcję, określ maksymalny rozmiar archiwum w polu obok nazwy opcji.
   - Jeśli chcesz, aby Ochrona poczty skanowała załączniki wiadomości e-mail, których skanowanie trwa więcej niż N sekund, usuń zaznaczenie z pola **Nie skanuj archiwów dłużej niż** N s.

6. Kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Filtrowanie załączników w wiadomościach e-mail

Szkodliwe programy 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 szkodliwego programu.

W celu skonfigurowania filtrowania załączników:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona poczty**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona poczty.

3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona poczty**.

4. W oknie **Ochrona poczty** przejdź na zakładkę **Filtr załączników**.

5. Wykonaj jedną z poniższych czynności:

   - Jeżeli nie chcesz, aby Ochrona poczty filtrowała załączniki w wiadomościach, zaznacz opcję **Wyłącz filtrowanie**.
   - Jeżeli chcesz, aby Ochrona poczty zmieniała nazwy załączników **określonych typów**, zaznacz opcję **Zmień nazwę wybranych typów załączników**.

Należy pamiętać, że rzeczywisty format pliku może nie odpowiadać jego rozszerzeniu.

Jeśli włączysz filtrowanie obiektów załączonych do wiadomości e-mail, Ochrona poczty może usunąć lub zmienić nazwy plików posiadających następujące rozszerzenia:

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 Microsoft Outlook Express

nws – nowa wiadomość pocztowa Microsoft Outlook Express

msg – wiadomość pocztowa Microsoft Mail

plg – wiadomość pocztowa

mbx – rozszerzenie dla zapisanych wiadomości 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. Następna generacja metaplików systemu Microsoft Windows OS. Pliki EMF nie są obsługiwane przez 16-bitowe systemy Microsoft Windows.

ico – plik ikony obiektu

ov? – pliki wykonywalne Microsoft Office Word

xl* – pliki i dokumenty Microsoft Office Excel, takie jak: xla dla rozszerzeń dla Microsoft Office Excel, xlc dla diagramów, xlt dla szablonów dokumentów, xlsx dla skoroszytów Microsoft Office Excel 2007, xltm dla skoroszytów Microsoft Office Excel 2007 z obsługą makr, xlsb dla skoroszytów Microsoft Office Excel 2007 w formacie binarnym (nie XML), xltx dla szablonów Microsoft Office Excel 2007, xlsm dla szablonów Microsoft Office Excel 2007 z obsługą makr oraz xlam dla wtyczek Microsoft Office Excel 2007 z obsługą makr

pp* – pliki i dokumenty Microsoft Office PowerPoint®, takie jak: pps dla slajdów Microsoft Office PowerPoint, ppt dla prezentacji, pptx dla prezentacji Microsoft Office PowerPoint 2007, pptm dla prezentacji Microsoft Office PowerPoint 2007 z obsługą makr, potx dla szablonów prezentacji Microsoft Office PowerPoint 2007, potm dla szablonów prezentacji Microsoft Office PowerPoint 2007 z obsługą makr, ppsx dla pokazów slajdów Microsoft Office PowerPoint 2007, ppsm dla pokazów slajdów Microsoft Office PowerPoint 2007 z obsługą makr oraz ppam dla wtyczek Microsoft Office PowerPoint 2007 z obsługą makr

md* – pliki i dokumenty Microsoft Office Access®, takie jak: mda dla grup roboczych Microsoft Office Access oraz mdb dla baz danych

sldx – slajd Microsoft PowerPoint 2007

sldm – slajd Microsoft PowerPoint 2007 z obsługą makr

thmx – motyw Microsoft Office 2007

- Jeżeli chcesz, aby Ochrona poczty usuwała załączniki określonych typów, zaznacz opcję **Usuwaj określone typy załączników**.

6. Jeśli w poprzednim kroku wybrałeś opcję **Zmień nazwę wybranych typów załączników** lub opcję **Usuwaj określone typy załączników**, zaznacz pola obok odpowiednich typów plików.

   W celu modyfikacji zawartości listy typów plików użyj przycisków **Dodaj**, **Modyfikuj** i **Usuń**.

7. Kliknij **OK**.

8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Skanowanie poczty elektronicznej w programie Microsoft Office Outlook

Podczas instalacji Kaspersky Endpoint Security rozszerzenie Ochrony poczty jest osadzane w kliencie poczty Microsoft Office Outlook (zwany dalej także Outlook). 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.

Ustawienia Ochrony poczty mogą zostać skonfigurowane bezpośrednio w programie Outlook, jeśli w interfejsie Kaspersky Endpoint Security zaznaczono pole **Dodatkowe: rozszerzenie do Microsoft Office Outlook**.

W programie Outlook wiadomości przychodzące są najpierw skanowane przez Ochronę poczty (jeżeli w interfejsie Kaspersky Endpoint Security zaznaczone jest pole **Ruch POP3 / SMTP / NNTP / IMAP**), a dopiero później przez rozszerzenie Ochrony poczty osadzone w programie Outlook. Jeżeli Ochrona poczty wykryje w wiadomości szkodliwy obiekt, wyświetli odpowiedni komunikat.

Wybór działania w oknie powiadomienia określa, który komponent wyeliminuje zagrożenie w wiadomości: Ochrona poczty lub rozszerzenie Ochrony poczty osadzone w programie Outlook.

- Jeżeli w oknie powiadomienia wybierzesz **Wykonaj leczenie** lub **Usuń**, zagrożenie zostanie wyeliminowane przez Ochronę poczty.
- Jeżeli w oknie powiadomienia wybierzesz **Pomiń**, zagrożenie zostanie wyeliminowane przez rozszerzenie Ochrony poczty osadzone w programie Outlook.

Wychodzące wiadomości są najpierw skanowane przez rozszerzenie Ochrony poczty osadzone w programie Outlook, a dopiero później przez Ochronę poczty.

Konfigurowanie ustawień skanowania poczty w programie Outlook

W celu skonfigurowania ustawień skanowania poczty w programie Outlook 2007:

1. Otwórz okno główne programu Outlook 2007.
2. Na pasku menu wybierz **Usługa** → **Ustawienia**.

   Zostanie otwarte okno **Opcje**.
3. W oknie **Opcje** wybierz zakładkę **Ochrona poczty**.

W celu skonfigurowania ustawień skanowania poczty w programie Outlook 2010/2013:

1. Otwórz okno główne aplikacji Outlook.

   W lewym górnym rogu okna wybierz zakładkę **Plik**.
2. Kliknij przycisk **Opcje**.

   Zostanie otwarte okno **Opcje programu Outlook**.
3. Wybierz sekcję **Dodatki**.

   W prawej części okna zostaną wyświetlone ustawienia wtyczki osadzonej w programie Outlook.
4. Kliknij przycisk **Opcje dodatków**.

Konfigurowanie ustawień skanowania poczty przy użyciu Kaspersky Security Center

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: https://technet.microsoft.com/pl-pl/library/cc179175.aspx.

W celu skonfigurowania trybu działania rozszerzenia Ochrony poczty dla programu Outlook przy użyciu Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz skonfigurować skanowanie poczty.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona poczty**.
7. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
   Zostanie otwarte okno **Ochrona poczty**.
8. W sekcji **Łączność** kliknij przycisk **Ustawienia**.
   Zostanie otwarte okno **Ochrona poczty**.
9. 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.
10. W oknie **Ochrona poczty** kliknij **OK**.
11. W oknie **Ochrona poczty** kliknij **OK**.
12. Zastosuj profil.

Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

Ochrona komputera w internecie. Ochrona WWW

Komponent jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów plików.

Sekcja ta zawiera informacje o Ochronie WWW oraz instrukcje dotyczące konfiguracji ustawień modułu.

Informacje o module Ochrona WWW

Za każdym razem, gdy korzystasz z internetu, narażasz informacje przechowywane na Twoim komputerze na działanie wirusów i innego szkodliwego oprogramowania. Mogą one przedostać się na komputer podczas pobierania darmowego oprogramowania lub przeglądania stron internetowych, które zostały zainfekowane przez hakerów. Robaki sieciowe mogą przedostać się do systemu w momencie nawiązania połączenia internetowego, zanim nawet otworzysz stronę lub pobierzesz plik.

Ochrona WWW chroni dane odbierane i wysyłane za pośrednictwem protokołów HTTP i FTP, sprawdza również adresy internetowe, korzystając z list szkodliwych i phishingowych adresów internetowych.

Ochrona WWW przechwytuje i analizuje w poszukiwaniu wirusów i innego szkodliwego oprogramowania każdą stronę internetową i plik, do których użytkownik lub aplikacja uzyskuje dostęp za pośrednictwem protokołów HTTP lub FTP. Następnie:

- Jeśli strona lub plik nie zawierają szkodliwego kodu, użytkownik uzyskuje do nich dostęp.
- Jeśli strona internetowa lub plik, do którego użytkownik uzyskuje dostęp, zawierają szkodliwy kod, aplikacja podejmie akcję określoną w ustawieniach Ochrony WWW.

Włączanie i wyłączanie modułu Ochrona WWW

Domyślnie moduł Ochrona WWW jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky. W razie konieczności możesz wyłączyć Ochronę WWW.

Istnieją dwa sposoby włączania i wyłączania komponentu:

- W oknie głównym aplikacji, na zakładce **Ochrona i kontrola**
- Z poziomu okna ustawień aplikacji

W celu włączenia lub wyłączenia modułu Ochrona WWW w oknie głównym aplikacji, na zakładce Ochrona i kontrola:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Ochrona**.

   Zostanie otwarta sekcja **Ochrona**.

4. Kliknij prawym przyciskiem myszy wiersz z informacjami o module Ochrona WWW, aby otworzyć menu kontekstowe.

   Zostanie otwarte menu wyboru działań.

5. Wykonaj jedną z poniższych czynności:

   - Aby włączyć moduł Ochrona WWW, wybierz z menu opcję **Włącz**.

     Ikona stanu modułu , wyświetlana w lewej części wiersza **Ochrona WWW**, zmieni się na ikonę .

   - Aby wyłączyć moduł Ochrona WWW, wybierz z menu opcję **Wyłącz**.

     Ikona stanu modułu , wyświetlana w lewej części wiersza **Ochrona WWW**, zmieni się na ikonę .

W celu włączenia lub wyłączenia modułu Ochrona WWW z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona WWW**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona WWW.

3. Wykonaj jedną z poniższych czynności:

   - Jeżeli chcesz włączyć Ochronę WWW, zaznacz pole **Włącz moduł Ochrona WWW**.
   - Jeżeli chcesz wyłączyć Ochronę WWW, usuń zaznaczenie z pola **Włącz moduł Ochrona WWW**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Konfigurowanie ustawień modułu Ochrona WWW

Podczas konfigurowania modułu Ochrona WWW można:

- Zmienić poziom ochrony ruchu sieciowego.

  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.

- Zmienić akcję podejmowaną przez Kaspersky Endpoint Security na szkodliwych obiektach w ruchu sieciowym.

  Jeżeli analiza obiektu HTTP wykaże, że zawiera on szkodliwy kod, to reakcja modułu Ochrona WWW będzie zależeć od akcji, która została wcześniej wybrana.

- Skonfigurować skanowanie adresów internetowych przez Ochronę WWW przy pomocy baz danych szkodliwych i phishingowych adresów internetowych.

- Skonfigurować użycie analizy heurystycznej podczas skanowania ruchu sieciowego w poszukiwaniu wirusów i innych szkodliwych programów.

  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.

- Skonfigurować użycie analizy heurystycznej podczas skanowania stron internetowych w poszukiwaniu odnośników phishingowych.
- Optymalizować skanowanie ruchu sieciowego przesyłanego poprzez protokoły HTTP i FTP.
- Utworzyć listę zaufanych adresów internetowych.

  Możesz utworzyć listę adresów internetowych, którym ufasz co do zawartości. Ochrona WWW nie sprawdza informacji pochodzących od zaufanych adresów 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.

Zmienianie poziomu ochrony ruchu sieciowego

Aby chronić dane odbierane i przesyłane poprzez protokoły HTTP i FTP, Ochrona WWW stosuje różne grupy ustawień. Takie grupy ustawień nazywane są *poziomami ochrony ruchu sieciowego*. Dostępne są trzy predefiniowane poziomy ochrony ruchu sieciowego: **Wysoki**, **Zalecany** i **Niski**. **Zalecany** poziom ochrony ruchu sieciowego jest uważany za optymalne ustawienie i jest zalecany przez Kaspersky.

W celu zmiany poziomu ochrony ruchu internetowego:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona WWW**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona WWW.
3. W sekcji **Poziom ochrony** wykonaj jedną z poniższych czynności:
   - Jeżeli chcesz wybrać jeden z predefiniowanych poziomów ochrony ruchu sieciowego (**Wysoki**, **Zalecany** lub **Niski**), użyj suwaka.
   - Jeżeli chcesz skonfigurować niestandardowy poziom ochrony ruchu sieciowego, kliknij przycisk **Ustawienia** i w otwartym oknie **Ochrona WWW** określ swoje ustawienia.

     Po skonfigurowaniu niestandardowego poziomu ochrony ruchu sieciowego, nazwa poziomu ochrony w sekcji **Poziom ochrony** zmieni się na **Niestandardowy**.
   - Jeżeli chcesz zmienić poziom ochrony ruchu sieciowego na **Zalecany**, kliknij przycisk **Domyślny**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zmienianie akcji podejmowanej na szkodliwych obiektach w ruchu sieciowym

W celu zmiany akcji podejmowanej na szkodliwych obiektach w ruchu sieciowym:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona WWW**.

W prawej części okna wyświetlone są ustawienia modułu 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:

   - **Automatycznie wybierz akcję**.
   - **Zablokuj pobranie**.
   - **Zezwól na pobranie**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Skanowanie adresów internetowych przez Ochronę WWW przy użyciu baz danych szkodliwych i phishingowych 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 adresy URL znajdują się w bazie danych szkodliwych adresów i adresów typu phishing:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona WWW**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona WWW.

3. Kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona WWW**.

4. W oknie **Ochrona WWW** przejdź na zakładkę **Ogólne**.

5. Wykonaj następujące czynności:

   - Jeśli chcesz, aby Ochrona WWW sprawdzała adresy internetowe przy pomocy baz danych szkodliwych adresów internetowych, zaznacz pole **Sprawdź, czy odsyłacze są umieszczone w bazie danych szkodliwych adresów** w sekcji **Metody skanowania**.
   - Jeśli chcesz, aby Ochrona WWW sprawdzała adresy internetowe przy pomocy baz danych phishingowych adresów internetowych, zaznacz pole **Sprawdź, czy odsyłacze znajdują się w bazie danych odnośników zawierających phishing** w sekcji **Ustawienia anti-phishing**.

Możesz również sprawdzać odnośniki, korzystając z baz danych reputacji pochodzących z Kaspersky Security Network.

6. Kliknij **OK**.
7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Używanie Analizatora heurystycznego z Ochroną WWW

W celu skonfigurowania korzystania z analizy heurystycznej:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona WWW**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona WWW.
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona WWW**.
4. Przejdź na zakładkę **Ogólne**.
5. Jeśli chcesz, aby podczas skanowania ruchu sieciowego w poszukiwaniu wirusów i innych szkodliwych programów Ochrona WWW korzystała z analizy heurystycznej, w sekcji **Metody skanowania** zaznacz pole **Wykrywanie wirusów przy użyciu analizy heurystycznej** i użyj suwaka, aby ustawić poziom szczegółowości analizy heurystycznej: **Niski**, **Średni** lub **Szczegółowy**.
6. Jeżeli chcesz, aby podczas skanowania stron internetowych w poszukiwaniu odnośników phishingowych Ochrona WWW używała analizy heurystycznej, w sekcji **Ustawienia Anti-phishing** zaznacz pole **Wykrywanie odsyłaczy zawierających phishing przy użyciu analizy heurystycznej**.
7. Kliknij **OK**.
8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Modyfikowanie listy zaufanych adresów internetowych

W celu utworzenia listy zaufanych adresów internetowych:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona WWW**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona WWW.
3. Kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona WWW**.
4. Wybierz zakładkę **Zaufane adresy URL**.

5. Zaznacz pole **Nie skanuj ruchu sieciowego z zaufanych adresów internetowych**.

6. Utwórz listę adresów internetowych / stron internetowych, którym ufasz co do zawartości. W celu utworzenia llisty:

   a. Kliknij przycisk **Dodaj**.

      Zostanie otwarte okno **Adres / Maska adresu**.

   b. Wprowadź adres strony lub maskę adresu strony.

   c. Kliknij **OK**.

      Nowy wpis pojawi się na liście zaufanych adresów internetowych.

7. Kliknij **OK**.

8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Ochrona ruchu klientów komunikatorów internetowych. Ochrona komunikatorów

Komponent jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów plików.

Sekcja ta zawiera informacje o Ochronie komunikatorów oraz instrukcje dotyczące konfiguracji ustawień modułu.

Informacje o module Ochrona komunikatorów

Moduł Ochrona komunikatorów skanuje ruch klientów komunikatorów internetowych (zwane również *klientami komunikatorów*).

Ochrona komunikatorów nie skanuje wiadomości przesyłanych za pośrednictwem kanałów szyfrowanych.

Wiadomości przesyłane przez klienty komunikatorów mogą zawierać następujące rodzaje zagrożeń bezpieczeństwa:

- Odnośniki internetowe, poprzez które może nastąpić pobranie szkodliwego programu na komputer.
- Odnośniki do szkodliwych programów i stron, które cyberprzestępcy wykorzystują w celu ataków phishingowych.

  Ataki phishingowe mają na celu kradzież danych osobowych użytkowników, takich jak numery kart płatniczych, informacje z paszportów, hasła do systemów bankowych i innych usług internetowych (takich jak strony sieci społecznościowych lub konta pocztowe).

Poprzez klienty komunikatorów można przesyłać pliki. Przy próbie zapisu takich plików są one skanowane przez moduł Ochrona plików.

Ochrona komunikatorów przechwytuje wszystkie wiadomości wysyłane lub odbierane przez użytkownika poprzez klienty komunikatorów i skanuje je w poszukiwaniu odnośników, które mogą stanowić zagrożenie dla bezpieczeństwa komputera:

- Jeżeli w wiadomości nie zostanie wykryty niebezpieczny adres internetowy, stanie się ona dostępna dla użytkownika.
- Jeżeli w wiadomości zostaną wykryte niebezpieczne odnośniki, Ochrona komunikatorów zastąpi wiadomość informacją o zagrożeniu w aktywnym oknie klienta komunikatorów.

Włączanie i wyłączanie modułu Ochrona komunikatorów

Domyślnie moduł Ochrona komunikatorów jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky. W razie konieczności możesz wyłączyć Ochronę komunikatorów.

Istnieją dwa sposoby włączania i wyłączania komponentu:

- W oknie głównym aplikacji, na zakładce**Ochrona i kontrola**
- Z poziomu okna ustawień aplikacji

W celu włączenia lub wyłączenia modułu Ochrona komunikatorów w oknie głównym aplikacji, na zakładce Ochrona i kontrola:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Ochrona**.

   Zostanie otwarta sekcja **Ochrona**.
4. Kliknij prawym przyciskiem myszy wiersz **Ochrona komunikatorów**, aby otworzyć menu kontekstowe z akcjami modułu.
5. Wykonaj jedną z poniższych czynności:
   - Aby włączyć moduł Ochrona komunikatorów, wybierz z menu opcję **Włącz**.

     Ikona stanu modułu , wyświetlana w lewej części wiersza **Ochrona komunikatorów**, zmieni się na ikonę .
   - Aby wyłączyć moduł Ochrona komunikatorów, wybierz z menu opcję **Wyłącz**.

     Ikona stanu modułu , wyświetlana w lewej części wiersza **Ochrona komunikatorów**, zmieni się na ikonę .

W celu włączenia lub wyłączenia modułu Ochrona komunikatorów z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona komunikatorów**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona komunikatorów.
3. Wykonaj jedną z poniższych czynności:
   - Jeżeli chcesz włączyć Ochronę komunikatorów, zaznacz pole **Włącz moduł Ochrona komunikatorów**.
   - Jeżeli chcesz wyłączyć Ochronę komunikatorów, usuń zaznaczenie z pola **Włącz moduł Ochrona komunikatorów**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Konfigurowanie ustawień modułu Ochrona komunikatorów

Podczas konfigurowania modułu Ochrona komunikatorów można:

- Skonfigurować obszar ochrony.

  Możesz poszerzyć lub zawęzić obszar ochrony przez zmodyfikowanie typu skanowanych wiadomości klientów komunikatorów.

- Skonfigurować skanowanie odnośników w wiadomościach klientów komunikatorów z wykorzystaniem baz danych szkodliwych i phishingowych adresów internetowych.

Tworzenie obszaru ochrony modułu Ochrona komunikatorów

Obszar ochrony oznacza obiekty, które są skanowane przez moduł, gdy jest on włączony. Obszary ochrony różnych modułów mają odmienne właściwości. Typ skanowanych wiadomości klientów komunikatorów, odbieranych lub wysyłanych, jest właściwością obszaru ochrony modułu Ochrona komunikatorów. Domyślnie Ochrona komunikatorów skanuje wiadomości zarówno przychodzące, jak i wychodzące. Możesz wyłączyć skanowanie ruchu wychodzącego.

W celu utworzenia obszaru ochrony:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona komunikatorów**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona komunikatorów.
3. W sekcji **Obszar ochrony** należy wykonać jedną z następujących czynności:
   - Jeżeli chcesz, aby Ochrona komunikatorów skanowała wszystkie przychodzące i wychodzące wiadomości klientów komunikatorów, zaznacz opcję **Wiadomości odbierane i wysyłane**.
   - Jeśli chcesz, aby Ochrona komunikatorów skanowała tylko wiadomości przychodzące, wybierz opcję **Tylko wiadomości odbierane**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Skanowanie adresów internetowych przez Ochronę komunikatorów przy pomocy baz danych szkodliwych i phishingowych adresów internetowych

W celu skonfigurowania modułu Ochrona komunikatorów, aby sprawdzał, czy adresy internetowe znajdują się w bazie danych szkodliwych i phishingowych adresów internetowych:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona komunikatorów**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona komunikatorów.
3. W sekcji **Metody skanowania** wybierz metody, które mają być wykorzystywane przez Ochronę komunikatorów:
   - Jeśli chcesz sprawdzać odnośniki w wiadomościach klientów komunikatorów przy pomocy bazy danych szkodliwych adresów internetowych, zaznacz pole **Sprawdź, czy odsyłacze znajdują się w bazie danych szkodliwych odnośników**.
   - Jeśli chcesz sprawdzać odnośniki w wiadomościach klientów komunikatorów przy pomocy bazy danych phishingowych adresów internetowych, zaznacz pole **Sprawdź, czy odsyłacze znajdują się w bazie danych odnośników zawierających phishing**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Kontrola systemu

Komponent jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów plików.

Sekcja ta zawiera informacje o Kontroli systemu oraz instrukcje dotyczące konfiguracji ustawień modułu.

Informacje o module Kontrola systemu

Kontrola systemu zbiera dane o działaniach programów na komputerze i udostępnia te informacje innym modułom w celu lepszej ochrony.

Sygnatury strumieni zachowań (BBS - Behavior Stream Signature)

Sygnatury strumieni zachowań (BSS) (zwane również wzorcami/schematami niebezpiecznej aktywności) zawierają sekwencje działań aplikacji, które Kaspersky Endpoint Security klasyfikuje jako niebezpieczne. Jeśli aktywność aplikacji odpowiada sygnaturze strumienia zachowań, Kaspersky Endpoint Security wykona określone działanie. Funkcjonalność Kaspersky Endpoint Security oparta na sygnaturach strumieni zachowań zapewnia ochronę proaktywną komputera.

Domyślnie, jeśli aktywność aplikacji odpowiada sygnaturze strumienia zachowań, Kontrola systemu przenosi plik wykonywalny tej aplikacji do Kwarantanny.

Cofanie akcji wykonanych przez szkodliwe oprogramowanie

W oparciu o informacje zebrane przez Kontrolę systemu, Kaspersky Endpoint Security może **wycofać akcje wykonane w systemie operacyjnym przez szkodliwe oprogramowanie** w trakcie leczenia.

Podczas cofania szkodliwej aktywności w systemie operacyjnym Kaspersky Endpoint Security podejmuje działanie na następujących typach szkodliwej aktywności:

- Aktywność plikowa.

  Kaspersky Endpoint Security usuwa pliki wykonywalne, które zostały utworzone przez szkodliwy program i znajdują się na dowolnym nośniku, za wyjątkiem sieciowego.

  Kaspersky Endpoint Security usuwa pliki wykonywalne utworzone przez program, do którego przeniknął szkodliwy program.

  Kaspersky Endpoint Security nie przywraca zmienionych lub usuniętych plików.

- Aktywność w rejestrze.

  Kaspersky Endpoint Security usuwa partycje i klucze rejestru, które zostały utworzone przez szkodliwe oprogramowanie.

  Kaspersky Endpoint Security nie przywraca zmodyfikowanych lub usuniętych partycji i kluczy rejestru.

- Aktywność w systemie.

  Kaspersky Endpoint Security zakańcza procesy zainicjowane przez szkodliwy program.

  Kaspersky Endpoint Security zakańcza procesy, do których przeniknął szkodliwy program.

  Kaspersky Endpoint Security nie wznawia procesów zatrzymanych przez szkodliwy program.

- Aktywność sieciowa.

  Kaspersky Endpoint Security blokuje aktywność sieciową szkodliwych programów.

  Kaspersky Endpoint Security blokuje aktywność sieciową procesów, do których przeniknął szkodliwy program.

Wycofanie działań szkodliwych programów może być zainicjowane przez Ochronę plików lub skanowanie antywirusowe.

Wycofywanie działań szkodliwego oprogramowania oddziałuje na ściśle określony zestaw danych. Nie ma negatywnego wpływu na system operacyjny i integralność danych komputera.

Włączanie i wyłączanie modułu Kontrola systemu

Domyślnie moduł Kontrola systemu jest włączony i działa w trybie zalecanym przez specjalistów z Kaspersky. W razie konieczności możesz wyłączyć Kontrolę systemu.

Nie zaleca się wyłączać Kontroli systemu bez wyraźnej konieczności, ponieważ wpłynie to na działanie modułów ochrony. Moduły ochrony mogą żądać danych zebranych przez Kontrolę systemu, aby móc dokładniej zidentyfikować wykryte zagrożenie.

Istnieją dwa sposoby włączania i wyłączania Kontroli systemu:

- W oknie głównym aplikacji, na zakładce **Ochrona i kontrola**
- Z poziomu okna ustawień aplikacji

*W celu włączenia lub wyłączenia modułu Kontrola systemu w oknie głównym aplikacji, na zakładce **Ochrona i kontrola**:*

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Ochrona**.

   Zostanie otwarta sekcja **Ochrona**.
4. Kliknij prawym przyciskiem myszy wiersz z informacjami o module Kontrola systemu, aby otworzyć menu kontekstowe.

   Zostanie otwarte menu wyboru działań.
5. Wykonaj jedną z poniższych czynności:

   - Aby włączyć Kontrolę systemu, wybierz **Włącz**.

     Ikona stanu modułu , wyświetlana w lewej części wiersza **Kontrola systemu**, zmieni się na ikonę .
   - Aby wyłączyć Kontrolę systemu, wybierz **Wyłącz**.

     Ikona stanu modułu , wyświetlana w lewej części wiersza **Kontrola systemu**, zmieni się na ikonę .

W celu włączenia lub wyłączenia modułu Kontrola systemu z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Kontrola systemu**.

   W prawej części okna wyświetlone są ustawienia modułu **Kontrola systemu**.
3. Wykonaj jedną z poniższych czynności:

   - Aby włączyć Kontrolę systemu, zaznacz pole **Włącz moduł Kontrola systemu**.
   - Aby wyłączyć Kontrolę systemu, usuń zaznaczenie z pola **Włącz moduł Kontrola systemu**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Konfigurowanie modułu Kontrola systemu

Podczas konfigurowania ustawień Kontroli systemu możesz wykonać następujące czynności:

- Włączyć lub wyłączyć ochronę przed exploitami;
- Wybrać opcję wykrywania szkodliwej aktywności w programie;
- Włączyć lub wyłączyć wycofywanie działań szkodliwego oprogramowania podczas leczenia.

Włączanie lub wyłączanie ochrony przed exploitami

W celu włączenia lub wyłączenia ochrony przed exploitami:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Kontrola systemu**.

   W prawej części okna wyświetlone są ustawienia modułu **Kontrola systemu**.
3. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz, żeby program Kaspersky Endpoint Security monitorował pliki wykorzystywane przez podatne programy podczas ich uruchamiania, zaznacz pole **Włącz ochronę przed exploitami**.

     Jeśli Kaspersky Endpoint Security wykryje, że plik używany przez podatny program nie został uruchomiony przez użytkownika, wykona działanie wybrane na liście **Działanie podejmowane w przypadku wykrycia zagrożenia**.
   - Jeśli chcesz, żeby program Kaspersky Endpoint Security monitorował pliki wykorzystywane przez podatne programy podczas ich uruchamiania, zaznacz pole **Włącz ochronę przed exploitami**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Wybieranie opcji wykrywania szkodliwej aktywności w programie

W celu wybrania akcji, jaka ma zostać wykonana, gdy program wykryje szkodliwą aktywność:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Kontrola systemu**.

   W prawej części okna wyświetlone są ustawienia modułu **Kontrola systemu**.
3. W sekcji **Działanie podejmowane w przypadku wykrycia zagrożenia**, na liście rozwijalnej **Po wykryciu aktywności szkodliwego oprogramowania** wybierz następujące działanie:

   - **Automatycznie wybierz akcję**.
   - **Przenieś plik do Kwarantanny**.
   - **Zakończ działanie szkodliwego programu**.
   - **Pomiń**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Włączanie i wyłączanie wycofywania akcji szkodliwego oprogramowania podczas leczenia

W celu włączenia lub wyłączenia cofania akcji szkodliwego oprogramowania podczas leczenia:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Kontrola systemu**.

   W prawej części okna wyświetlone są ustawienia modułu **Kontrola systemu**.

3. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz, aby podczas leczenia Kaspersky Endpoint Security cofał akcje wykonane przez szkodliwe oprogramowanie w systemie operacyjnym, zaznacz pole **Podczas leczenia wycofaj zmiany wprowadzone przez szkodliwe oprogramowanie**.

   - Jeśli chcesz, aby podczas leczenia Kaspersky Endpoint Security ignorował akcje wykonane przez szkodliwe oprogramowanie w systemie operacyjnym, usuń zaznaczenie z pola **Podczas leczenia wycofaj zmiany wprowadzone przez szkodliwe oprogramowanie**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zapora sieciowa

Sekcja ta zawiera informacje o Zaporze sieciowej oraz instrukcje dotyczące konfiguracji ustawień modułu.

Informacje o module Zapora sieciowa

Podczas korzystania z sieci LAN i internetu komputer jest narażony na wirusy i inne szkodliwe programy, a także różnego rodzaju ataki wykorzystujące luki systemu operacyjnego i oprogramowania.

Zapora sieciowa chroni dane osobowe przechowywane na komputerze użytkownika i blokuje większość możliwych zagrożeń systemu operacyjnego, gdy komputer jest podłączony do internetu lub sieci lokalnej. Zapora sieciowa wykrywa wszystkie połączenia sieciowe komputera użytkownika i dostarcza listę adresów IP wraz ze stanem domyślnego połączenia sieciowego.

Moduł Zapora sieciowa filtruje całą aktywność sieciową zgodnie z regułami sieciowymi. Konfigurowanie reguł sieciowych pozwala na określenie żądanego poziomu ochrony komputera - od blokowania dostępu do internetu dla wszystkich aplikacji po zezwalanie na nieograniczony dostęp.

Włączanie i wyłączanie modułu Zapora sieciowa

Domyślnie moduł Zapora sieciowa jest włączony i działa w trybie optymalnym. W razie konieczności możesz wyłączyć Zaporę sieciową.

Istnieją dwa sposoby włączania i wyłączania komponentu:

- W oknie głównym aplikacji, na zakładce**Ochrona i kontrola**
- Z poziomu okna ustawień aplikacji

W celu włączenia lub wyłączenia modułu Zapora sieciowa w oknie głównym aplikacji, na zakładce Ochrona i kontrola:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Ochrona**.
   Zostanie otwarta sekcja **Ochrona**.
4. Kliknij prawym przyciskiem myszy wiersz **Zapora sieciowa**, aby otworzyć menu kontekstowe z akcjami modułu.
5. Wykonaj jedną z poniższych czynności:
   - Aby włączyć moduł Zapora sieciowa, wybierz z menu **Włącz**.
     Ikona stanu modułu , wyświetlana w lewej części wiersza **Zapora sieciowa**, zmieni się na ikonę .
   - Aby wyłączyć moduł Zapora sieciowa, wybierz z menu opcję **Wyłącz**.
     Ikona stanu modułu , wyświetlana w lewej części wiersza **Zapora sieciowa**, zmieni się na ikonę .

W celu włączenia lub wyłączenia modułu Zapora sieciowa z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Zapora sieciowa**.

   W prawej części okna wyświetlone są ustawienia modułu Zapora sieciowa.
3. Wykonaj jedną z poniższych czynności:
   - Aby włączyć Zaporę sieciową, zaznacz pole **Włącz moduł Zapora sieciowa**.
   - Aby wyłączyć Zaporę sieciową, zaznacz pole **Wyłącz moduł Zapora sieciowa**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Informacje o regułach sieciowych

Reguły sieciowe są to akcje zezwalające lub blokujące wykonywane przez Zaporę sieciową po wykryciu próby połączenia sieciowego.

Zapora sieciowa chroni przed atakami sieciowymi różnych rodzajów na dwóch poziomach: poziomie sieci i poziomie programu. Ochrona na poziomie sieci jest realizowana poprzez stosowanie reguł dla pakietów sieciowych. Ochrona na poziomie programu jest realizowana poprzez stosowanie reguł, zgodnie z którymi zainstalowane aplikacje mogą uzyskiwać dostęp do zasobów sieciowych.

W oparciu o dwa poziomy ochrony Zapory sieciowej możesz utworzyć:

- *Reguły pakietów sieciowych*. Reguły pakietów sieciowych nakładają ograniczenia na pakiety sieciowe, niezależnie od programu. Takie reguły ograniczają ruch sieciowy wychodzący i przychodzący przez określone porty wybranego protokołu. Domyślnie Zapora sieciowa definiuje określone reguły pakietów sieciowych.
- *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. Reguły takie umożliwiają optymalizację filtrowania aktywności sieciowej, na przykład, gdy pewien typ połączenia sieciowego jest zablokowany dla niektórych aplikacji, a dla innych dozwolony.

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.

Dla każdej reguły dla pakietu sieciowego i reguły sieciowej dla aplikacji możesz określić priorytet jej wykonania.

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.

Informacje o stanie połączenia sieciowego

Zapora sieciowa kontroluje wszystkie połączenia sieciowe na komputerze użytkownika i automatycznie przypisuje stan do każdego wykrytego połączenia sieciowego.

Połączenie sieciowe może mieć jeden z następujących typów stanu:

- **Sieć publiczna**. Zalecamy wybór tego stanu dla sieci, która nie jest chroniona przez żadną aplikację antywirusową, zaporę sieciową lub nie ma ona określonych filtrów (na przykład dla sieci kawiarenek internetowych). 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**. Stan ten jest przypisywany do sieci, których użytkownicy będą mieli dostęp do plików i drukarek tego komputera (na przykład do sieci LAN lub sieci domowej).

- **Sieć zaufana**. Stan ten jest dla sieci, w których 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.

Zmienianie stanu połączenia sieciowego

W celu zmiany stanu połączenia sieciowego:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Zapora sieciowa**.

   W prawej części okna wyświetlone są ustawienia modułu Zapora sieciowa.
3. Kliknij przycisk **Dostępne sieci**.

   Zostanie otwarte okno **Zapora sieciowa**.
4. Wybierz połączenie sieciowe, którego stan chcesz zmienić.
5. Z menu kontekstowego wybierz stan połączenia sieciowego:

   - **Sieć publiczna**.
   - **Sieć lokalna**.
   - **Sieć zaufana**.

6. W oknie **Zapora sieciowa** kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

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 i modyfikowanie reguły dla pakietu sieciowego

> Podczas tworzenia reguł dla pakietów sieciowych należy pamiętać, że posiadają one wyższy priorytet niż reguły sieciowe dla aplikacji.

W celu utworzenia lub zmodyfikowania reguły dla pakietu sieciowego:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Zapora sieciowa**.
3. Kliknij przycisk **Reguły pakietów sieciowych**.
4. Zostanie otwarte okno **Zapora sieciowa** na zakładce **Reguły pakietów sieciowych**.

   Zakładka ta wyświetla listę domyślnych reguł dla pakietów sieciowych, ustawionych przez Zaporę sieciową.
5. Wykonaj jedną z poniższych czynności:

   - Aby utworzyć nową regułę dla pakietu sieciowego, kliknij przycisk **Dodaj**.
   - Aby zmodyfikować regułę dla pakietu sieciowego, wybierz ją na liście reguł dla pakietów sieciowych i kliknij przycisk **Modyfikuj**.

   Zostanie otwarte okno **Reguła sieciowa**.
6. Z listy rozwijalnej **Akcja** wybierz akcję, jaka zostanie wykonana przez Zaporę sieciową po wykryciu tego rodzaju aktywności sieciowej:

   - **Zezwól**
   - **Zablokuj**
   - **Zgodnie z regułami aplikacji**.
7. W polu **Nazwa** określ nazwę usługi sieciowej w jeden z następujących sposobów:

   - Kliknij ikonę znajdującą się po prawej stronie pola **Nazwa** i z dostępnej listy rozwijalnej wybierz nazwę usługi sieciowej.

     Lista rozwijalna zawiera usługi sieciowe, które odpowiadają najczęściej używanym połączeniom sieciowym.
   - W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.
8. Określ protokół transmisji danych:

   a. Zaznacz pole **Protokół**.

   b. Z listy rozwijalnej wybierz typ protokołu, dla którego monitorowana będzie aktywność sieciowa.

   Zapora sieciowa kontroluje połączenia sieciowe korzystające z protokołów TCP, UDP, ICMP, ICMPv6, IGMP i GRE.

   Jeżeli wybierzesz usługę sieciową z listy rozwijalnej **Nazwa**, pole **Protokół** będzie zaznaczone automatycznie, a lista rozwijalna znajdująca się obok pola będzie zawierała typ protokołu odpowiadającego wybranej usłudze sieciowej. Domyślnie pole **Protokół** nie jest zaznaczone.
9. Z listy rozwijalnej **Kierunek** wybierz kierunek monitorowanej aktywności sieciowej.

   Zapora sieciowa monitoruje połączenia sieciowe w następujących kierunkach:

   - **Przychodzący (pakiet)**.
   - **Przychodzący**.
   - **Przychodzący / Wychodzący**

- **Wychodzący (pakiet)**.
- **Wychodzący**.

10. Jeśli wybrałeś protokół ICMP lub ICMPv6, możesz określić typ i kod pakietu ICMP:
    a. Zaznacz pole **Typ ICMP** i z lity rozwijalnej wybierz typ pakietu ICMP.
    b. Zaznacz pole **Kod ICMP** i z lity rozwijalnej wybierz kod pakietu ICMP.
11. Jeżeli jako typ protokołu wybrałeś TCP lub UDP, możesz określić porty komputera lokalnego oraz komputera zdalnego (rozdzielając je przecinkami), między którymi połączenie będzie kontrolowane:
    a. Typy portów komputera zdalnego określ w polu **Porty zdalne**.
    b. Typy portów komputera lokalnego określ w polu **Porty lokalne**.
12. W tabeli **Karty sieciowe** określ ustawienia kart sieciowych, z których mogą być wysyłane pakiety sieciowe lub które mogą odbierać pakiety sieciowe. W tym celu użyj przycisków **Dodaj**, **Modyfikuj** i **Usuń**.
13. Jeśli chcesz ograniczyć kontrolę pakietów sieciowych w oparciu o ich czas życia (czas wygaśnięcia, TTL), zaznacz pole **TTL**, a w polu obok określ górną granicę zakresu wartości czasu życia dla przychodzących i/lub wychodzących pakietów sieciowych.
    Reguła sieciowa będzie kontrolować przesyłanie pakietów sieciowych, których czas życia nie przekracza określonej wartości.
    W innym przypadku usuń zaznaczenie z pola **TTL**.
14. Określ adresy sieciowe zdalnych komputerów, które mogą wysyłać i/lub odbierać pakiety sieciowe. W tym celu, z listy rozwijalnej **Adresy zdalne** wybierz jedną z następujących wartości:
    - **Dowolny adres**. Reguła sieciowa kontroluje pakiety sieciowe wysyłane i/lub odbierane przez zdalne komputery o dowolnym adresie IP.
    - **Adresy podsieci**. Reguła sieciowa kontroluje pakiety sieciowe wysyłane i/lub odbierane przez zdalne komputery o adresach IP skojarzonych z wybranym typem sieci: **Sieci zaufane**, **Sieci lokalne** lub **Sieci publiczne**.
    - **Adresy z listy**. Reguła sieciowa kontroluje pakiety sieciowe wysyłane i/lub odbierane przez zdalne komputery o adresach IP, które można określić na liście znajdującej się poniżej, korzystając z przycisków **Dodaj**, **Modyfikuj**, i **Usuń**.
15. Określ adresy sieciowe komputerów z zainstalowanym programem Kaspersky Endpoint Security, które mogą wysyłać i/lub odbierać pakiety sieciowe. W tym celu, z listy rozwijalnej **Adresy lokalne** wybierz jedną z następujących wartości:
    - **Dowolny adres**. Reguła sieciowa kontroluje pakiety sieciowe wysyłane i/lub odbierane przez komputery z zainstalowanym programem Kaspersky Endpoint Security o dowolnym adresie IP.
    - **Adresy z listy**. Reguła sieciowa kontroluje pakiety sieciowe wysyłane i/lub odbierane przez komputery z zainstalowanym programem Kaspersky Endpoint Security o adresach IP, które można określić na liście znajdującej się poniżej, korzystając z przycisków **Dodaj**, **Modyfikuj**, i **Usuń**.

Zdarza się, że dla aplikacji, które działają z pakietami sieciowymi, nie można uzyskać adresu lokalnego. W takim przypadku ustawienie **Adresy lokalne** jest ignorowane.

16. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w raporcie, zaznacz pole **Zapisuj zdarzenia**.

17. W oknie **Reguła sieciowa** kliknij **OK**.

    Jeżeli utworzysz nową regułę sieciową, zostanie ona wyświetlona w oknie **Zapora sieciowa**, na zakładce **Reguły pakietów sieciowych**. Domyślnie nowa reguła sieciowa jest umieszczana na końcu listy reguł dla pakietów sieciowych.

18. W oknie **Zapora sieciowa** kliknij **OK**.

19. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Włączanie i wyłączanie reguły dla pakietu sieciowego

W celu włączenia lub wyłączenia reguły dla pakietu sieciowego:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Zapora sieciowa**.

   W prawej części okna wyświetlone są ustawienia modułu Zapora sieciowa.

3. Kliknij przycisk **Reguły pakietów sieciowych**.

   Zostanie otwarte okno **Zapora sieciowa** na zakładce **Reguły pakietów sieciowych**.

4. Na liście wybierz żądaną regułę dla pakietu sieciowego.

5. Wykonaj jedną z poniższych czynności:

   - Aby włączyć regułę, zaznacz pole obok nazwy reguły dla pakietu sieciowego.
   - Aby wyłączyć regułę, usuń zaznaczenie z pola obok nazwy reguły dla pakietu sieciowego.

6. Kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zmienianie akcji Zapory sieciowej dla reguły dla pakietu sieciowego

W celu zmiany akcji Zapory sieciowej stosowanej do reguły dla pakietu sieciowego:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Zapora sieciowa**.

   W prawej części okna wyświetlone są ustawienia modułu Zapora sieciowa.

3. Kliknij przycisk **Reguły pakietów sieciowych**.

   Zostanie otwarte okno **Zapora sieciowa** na zakładce **Reguły pakietów sieciowych**.

4. Z listy wybierz regułę dla pakietu sieciowego, której akcję chcesz zmienić.

5. Kliknij prawym przyciskiem myszy w kolumnie **Pozwolenie** i z otwartego menu kontekstowego wybierz akcję, którą chcesz przypisać:

   - **Zezwól**
   - **Zablokuj**
   - **Zgodnie z regułą aplikacji**
   - **Zapisuj zdarzenia**

6. W oknie **Zapora sieciowa** kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zmienianie priorytetu reguły dla pakietu sieciowego

Priorytet reguły dla pakietu sieciowego zależy od jej pozycji na liście reguł dla pakietów sieciowych. Reguła znajdująca się na najwyższej pozycji na liście reguł dla pakietów sieciowych ma najwyższy priorytet.

Każda ręcznie utworzona reguła dla pakietu sieciowego jest umieszczana na końcu listy i posiada najniższy priorytet.

Zapora sieciowa wykonuje reguły w kolejności, w jakiej występują na liście reguł dla pakietów sieciowych (od góry do dołu). Zgodnie z każdą przetworzoną regułą dla pakietu sieciowego, która odpowiada określonemu połączeniu sieciowemu, Zapora sieciowa zezwala na lub blokuje dostęp sieciowy do adresu i portu określonego w ustawieniach tego połączenia sieciowego.

W celu zmiany priorytetu reguły dla pakietu sieciowego:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Zapora sieciowa**.

   W prawej części okna wyświetlone są ustawienia modułu Zapora sieciowa.

3. Kliknij przycisk **Reguły pakietów sieciowych**.

   Zostanie otwarte okno **Zapora sieciowa** na zakładce **Reguły pakietów sieciowych**.

4. Z listy wybierz regułę dla pakietu sieciowego, której priorytet chcesz zmienić.

5. Użyj przycisków **W górę** i **W dół**, aby przesunąć regułę dla pakietu sieciowego na żądaną pozycję na liście.

6. Kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

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.

Domyślnie moduł Zapora sieciowa, tak jak moduł Kontrola uprawnień aplikacji, stosuje reguły sieciowe dla grupy aplikacji podczas filtrowania aktywności sieciowej wszystkich aplikacji w 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.

Podczas zarządzania regułami sieciowymi dla aplikacji możesz wykonać następujące czynności:

- Utworzyć nową regułę sieciową.

  Możesz utworzyć nową regułę sieciową, według której Zapora sieciowa musi kontrolować aktywność sieciową jednej lub kilku aplikacji należących do wybranej grupy aplikacji.

- Włączyć lub wyłączyć regułę sieciową.

  Wszystkie reguły sieciowe są dodawane do listy reguł sieciowych dla aplikacji ze stanem *Włączona*. Jeżeli reguła sieciowa jest włączona, Zapora sieciowa stosuje tę regułę.

  Możesz wyłączyć regułę sieciową, która została utworzona ręcznie. Jeżeli reguła sieciowa jest wyłączona, Zapora sieciowa tymczasowo nie stosuje tej reguły.

- Zmienić ustawienia reguły sieciowej.

  Po utworzeniu nowej reguły sieciowej można zawsze zmodyfikować jej ustawienia.

- Zmienić akcję Zapory sieciowej dla reguły sieciowej.

  Na liście reguł sieciowych możesz zmienić akcję Zapory sieciowej, która jest stosowana do reguły sieciowej po wykryciu aktywności sieciowej tej aplikacji lub grupy aplikacji.

- Zmienić priorytet reguły sieciowej.

  Możesz zwiększyć lub zmniejszyć priorytet niestandardowej reguły sieciowej.

- Usunąć regułę sieciową.

  Możesz usunąć niestandardową regułę sieciową, aby Zapora sieciowa nie stosowała jej do wybranej aplikacji lub grupy aplikacji po wykryciu aktywności sieciowej, a także aby reguła ta nie była wyświetlana na liście reguł sieciowych dla aplikacji.

Tworzenie i modyfikowanie reguły sieciowej dla aplikacji

W celu utworzenia lub zmodyfikowania reguły sieciowej dla grupy aplikacji:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Zapora sieciowa**.

3. Kliknij przycisk **Reguły sieciowe dla aplikacji**.

   Zostanie otwarte okno **Zapora sieciowa** na zakładce **Reguły kontroli aplikacji**.

4. Na liście aplikacji wybierz aplikację lub grupę aplikacji, dla której chcesz utworzyć lub zmodyfikować regułę sieciową.

5. Kliknij ją prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Reguły aplikacji** lub **Reguły grupy**, w zależności od tego, co chcesz zrobić.

   Zostanie otwarte okno **Reguły kontroli aplikacji** lub **Reguły kontroli grupy aplikacji**.

6. W otwartym oknie wybierz zakładkę **Reguły sieciowe**.

7. Wykonaj jedną z poniższych czynności:

   - Aby utworzyć nową regułę sieciową, kliknij przycisk **Dodaj**.
   - Aby zmodyfikować regułę sieciową, wybierz ją na liście reguł dla pakietów sieciowych i kliknij przycisk **Modyfikuj**.

   Zostanie otwarte okno **Reguła sieciowa**.

8. Z listy rozwijalnej **Akcja** wybierz akcję, jaka zostanie wykonana przez Zaporę sieciową po wykryciu tego rodzaju aktywności sieciowej:

   - **Zezwól**
   - **Zablokuj**

9. W polu **Nazwa** określ nazwę usługi sieciowej w jeden z następujących sposobów:

   - Kliknij ikonę znajdującą się po prawej stronie pola **Nazwa** i z dostępnej listy rozwijalnej wybierz nazwę usługi sieciowej.

     Lista rozwijalna zawiera usługi sieciowe, które odpowiadają najczęściej używanym połączeniom sieciowym.

   - W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.

10. Określ protokół transmisji danych:

    a. Zaznacz pole **Protokół**.

    b. Z listy rozwijalnej wybierz typ protokołu, dla którego monitorowana będzie aktywność sieciowa.

       Zapora sieciowa kontroluje połączenia sieciowe korzystające z protokołów TCP, UDP, ICMP, ICMPv6, IGMP i GRE.

       Jeżeli wybierzesz usługę sieciową z listy rozwijalnej **Nazwa**, pole **Protokół** będzie zaznaczone automatycznie, a lista rozwijalna znajdująca się obok pola będzie zawierała typ protokołu odpowiadającego wybranej usłudze sieciowej. Domyślnie pole **Protokół** nie jest zaznaczone.

11. Z listy rozwijalnej **Kierunek** wybierz kierunek monitorowanej aktywności sieciowej.

    Zapora sieciowa monitoruje połączenia sieciowe w następujących kierunkach:

    - **Przychodzący**.

- **Przychodzący / Wychodzący**.
- **Wychodzący**.

12. Jeśli wybrałeś protokół ICMP lub ICMPv6, możesz określić typ i kod pakietu ICMP:
    a. Zaznacz pole **Typ ICMP** i z lity rozwijalnej wybierz typ pakietu ICMP.
    b. Zaznacz pole **Kod ICMP** i z lity rozwijalnej wybierz kod pakietu ICMP.
13. Jeżeli jako typ protokołu wybrałeś TCP lub UDP, możesz określić porty komputera lokalnego oraz komputera zdalnego (rozdzielając je przecinkami), między którymi połączenie będzie kontrolowane:
    a. Typy portów komputera zdalnego określ w polu **Porty zdalne**.
    b. Typy portów komputera lokalnego określ w polu **Porty lokalne**.
14. Określ adresy sieciowe zdalnych komputerów, które mogą wysyłać i/lub odbierać pakiety sieciowe. W tym celu, z listy rozwijalnej **Adresy zdalne** wybierz jedną z następujących wartości:
    - **Dowolny adres**. Reguła sieciowa kontroluje pakiety sieciowe wysyłane i/lub odbierane przez zdalne komputery o dowolnym adresie IP.
    - **Adresy podsieci**. Reguła sieciowa kontroluje pakiety sieciowe wysyłane i/lub odbierane przez zdalne komputery o adresach IP skojarzonych z wybranym typem sieci: **Sieci zaufane**, **Sieci lokalne** lub **Sieci publiczne**.
    - **Adresy z listy**. Reguła sieciowa kontroluje pakiety sieciowe wysyłane i/lub odbierane przez zdalne komputery o adresach IP, które można określić na liście znajdującej się poniżej, korzystając z przycisków **Dodaj**, **Modyfikuj**, i **Usuń**.
15. Określ adresy sieciowe komputerów z zainstalowanym programem Kaspersky Endpoint Security, które mogą wysyłać i/lub odbierać pakiety sieciowe. W tym celu, z listy rozwijalnej **Adresy lokalne** wybierz jedną z następujących wartości:
    - **Dowolny adres**. Reguła sieciowa kontroluje pakiety sieciowe wysyłane i/lub odbierane przez komputery z zainstalowanym programem Kaspersky Endpoint Security o dowolnym adresie IP.
    - **Adresy z listy**. Reguła sieciowa kontroluje pakiety sieciowe wysyłane i/lub odbierane przez komputery z zainstalowanym programem Kaspersky Endpoint Security o adresach IP, które można określić na liście znajdującej się poniżej, korzystając z przycisków **Dodaj**, **Modyfikuj**, i **Usuń**.

    Zdarza się, że dla aplikacji, które działają z pakietami sieciowymi, nie można uzyskać adresu lokalnego. W takim przypadku ustawienie **Adresy lokalne** jest ignorowane.
16. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w raporcie, zaznacz pole **Zapisuj zdarzenia**.
17. W oknie **Reguła sieciowa** kliknij **OK**.
    Jeżeli utworzysz nową regułę sieciową, zostanie ona wyświetlona na zakładce **Reguły sieciowe**.
18. Kliknij **OK** w oknie **Reguły kontroli grupy aplikacji**, jeśli reguła jest przeznaczona dla grupy aplikacji, lub w oknie **Reguły kontroli aplikacji**, jeśli reguła jest przeznaczona dla aplikacji.
19. W oknie **Zapora sieciowa** kliknij **OK**.

20. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Włączanie i wyłączanie reguły sieciowej dla aplikacji

W celu włączenia lub wyłączenia reguły sieciowej dla aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Zapora sieciowa**.

   W prawej części okna wyświetlone są ustawienia modułu Zapora sieciowa.
3. Kliknij przycisk **Reguły sieciowe dla aplikacji**.

   Zostanie otwarte okno **Zapora sieciowa** na zakładce **Reguły kontroli aplikacji**.
4. Na liście wybierz aplikację lub grupę aplikacji, dla której chcesz włączyć lub wyłączyć regułę sieciową.
5. Kliknij ją prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Reguły aplikacji** lub **Reguły grupy**, w zależności od tego, co chcesz zrobić.

   Zostanie otwarte okno **Reguły kontroli aplikacji** lub **Reguły kontroli grupy aplikacji**.
6. W otwartym oknie wybierz zakładkę **Reguły sieciowe**.
7. Na liście reguł sieciowych dla grupy aplikacji wybierz wymaganą regułę sieciową.
8. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz włączyć regułę, zaznacz pole obok nazwy reguły sieciowej.
   - Jeśli chcesz wyłączyć regułę, usuń zaznaczenie z pola obok nazwy reguły sieciowej.

   Nie możesz wyłączyć reguły sieciowej dla grupy aplikacji utworzonej domyślnie przez Zaporę sieciową.
9. Kliknij **OK** w oknie **Reguły kontroli grupy aplikacji**, jeśli reguła jest przeznaczona dla grupy aplikacji, lub w oknie **Reguły kontroli aplikacji**, jeśli reguła jest przeznaczona dla aplikacji.
10. W oknie **Zapora sieciowa** kliknij **OK**.
11. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zmienianie akcji Zapory sieciowej dla reguły sieciowej dla aplikacji

Możesz zmienić akcję Zapory sieciowej stosowaną do wszystkich domyślnie utworzonych reguł sieciowych dla aplikacji lub grupy aplikacji, a także możesz zmienić akcję Zapory sieciowej stosowaną do pojedynczej niestandardowej reguły sieciowej dla aplikacji lub grupy aplikacji.

W celu zmiany akcji Zapory sieciowej stosowanej do wszystkich reguł sieciowych dla aplikacji lub grupy aplikacji:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Zapora sieciowa**.

   W prawej części okna wyświetlone są ustawienia modułu Zapora sieciowa.

3. Kliknij przycisk **Reguły sieciowe dla aplikacji**.

   Zostanie otwarte okno **Zapora sieciowa** na zakładce **Reguły kontroli 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 w kolumnie **Sieć** i z otwartego menu kontekstowego wybierz akcję, którą chcesz przypisać:

   - **Dziedzicz**
   - **Zezwól**
   - **Zablokuj**

6. Kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

W celu zmiany odpowiedzi Zapory sieciowej dla reguły sieciowej dla aplikacji lub grupy aplikacji:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Zapora sieciowa**.

   W prawej części okna wyświetlone są ustawienia modułu Zapora sieciowa.

3. Kliknij przycisk **Reguły sieciowe dla aplikacji**.

   Zostanie otwarte okno **Zapora sieciowa** na zakładce **Reguły kontroli aplikacji**.

4. Na liście wybierz aplikację lub grupę aplikacji, dla której chcesz zmienić regułę sieciową.

5. Kliknij ją prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Reguły aplikacji** lub **Reguły grupy**, w zależności od tego, co chcesz zrobić.

   Zostanie otwarte okno **Reguły kontroli aplikacji** lub **Reguły kontroli grupy aplikacji**.

6. W otwartym oknie wybierz zakładkę **Reguły sieciowe**.

7. Wybierz regułę sieciową, dla której chcesz zmienić działanie Zapory sieciowej.

8. Kliknij prawym przyciskiem myszy w kolumnie **Pozwolenie** i z otwartego menu kontekstowego wybierz akcję, którą chcesz przypisać:

   - **Zezwól**
   - **Zablokuj**
   - **Zapisuj zdarzenia**

9. Kliknij **OK** w oknie **Reguły kontroli grupy aplikacji**, jeśli reguła jest przeznaczona dla grupy aplikacji, lub w oknie **Reguły kontroli aplikacji**, jeśli reguła jest przeznaczona dla aplikacji.

10. W oknie **Zapora sieciowa** kliknij **OK**.

11. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zmienianie priorytetu reguły sieciowej dla aplikacji

Priorytet reguły sieciowej zależy od jej pozycji na liście reguł sieciowych. Zapora sieciowa wykonuje reguły w kolejności, w jakiej występują na liście reguł sieciowych (od góry do dołu). Zgodnie z każdą przetworzoną regułą sieciową, która odpowiada określonemu połączeniu sieciowemu, Zapora sieciowa zezwala na lub blokuje dostęp sieciowy do adresu i portu określonego w ustawieniach tego połączenia sieciowego.

Ręcznie utworzone reguły sieciowe mają wyższy priorytet niż domyślne reguły sieciowe.

Nie można zmieniać priorytetu domyślnie utworzonych reguł sieciowych dla grupy aplikacji.

W celu zmiany priorytetu reguły sieciowej:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz moduł **Zapora sieciowa**.
   W prawej części okna wyświetlone są ustawienia modułu Zapora sieciowa.
3. Kliknij przycisk **Reguły sieciowe dla aplikacji**.
   Zostanie otwarte okno **Zapora sieciowa** na zakładce **Reguły kontroli aplikacji**.
4. Na liście aplikacji wybierz aplikację lub grupę aplikację, dla której chcesz zmienić priorytet reguły sieciowej.
5. Kliknij ją prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Reguły aplikacji** lub **Reguły grupy**, w zależności od tego, co chcesz zrobić.
   Zostanie otwarte okno **Reguły kontroli aplikacji** lub **Reguły kontroli grupy aplikacji**.
6. W otwartym oknie wybierz zakładkę **Reguły sieciowe**.
7. Wybierz regułę sieciową, której priorytet chcesz zmienić.
8. Użyj przycisków **W górę** i **W dół**, aby przesunąć regułę sieciową na żądaną pozycję na liście.
9. Kliknij **OK** w oknie **Reguły kontroli grupy aplikacji**, jeśli reguła jest przeznaczona dla grupy aplikacji, lub w oknie **Reguły kontroli aplikacji**, jeśli reguła jest przeznaczona dla aplikacji.
10. W oknie **Zapora sieciowa** kliknij **OK**.
11. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Monitor sieci

Ta sekcja zawiera informacje o Monitorze sieci oraz instrukcje dotyczące sposobu jego włączenia.

Informacje o Monitorze sieci

Monitor sieci to narzędzie służące do wyświetlania informacji o aktywności sieciowej komputera użytkownika w czasie rzeczywistym.

Uruchamianie Monitora sieci

W celu uruchomienia Monitora sieci:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Ochrona**.

   Zostanie otwarta sekcja **Ochrona**.
4. Kliknij prawym przyciskiem myszy wiersz **Zapora sieciowa**, aby otworzyć menu kontekstowe z działaniami modułu.
5. Z menu kontekstowego wybierz **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 zakładce **Otwarte porty** wyświetlane są wszystkie otwarte porty sieciowe komputera.
   - 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 Blokowanie ataków sieciowych po wykryciu prób ataków sieciowych pochodzących z tych adresów IP.

Blokowanie ataków sieciowych

Sekcja ta zawiera informacje o Blokowaniu ataków sieciowych oraz instrukcje dotyczące konfiguracji ustawień modułu.

Informacje o module Blokowanie ataków sieciowych

Moduł Blokowanie ataków sieciowych bada przychodzący ruch sieciowy pod kątem aktywności typowych dla ataków sieciowych. Po wykryciu próby ataku sieciowego na Twój komputer, Kaspersky Endpoint Security blokuje aktywność sieciową atakującego komputera. Na ekranie zostanie wyświetlone ostrzeżenie o próbie podjęcia ataku sieciowego oraz informacje o atakującym komputerze.

Ruch sieciowy pochodzący z atakującego komputera jest blokowany na godzinę. Możesz zmodyfikować ustawienia używane do blokowania atakującego komputera.

Opisy znanych typów ataków sieciowych oraz sposoby ich zwalczania znajdują się w bazach danych programu Kaspersky Endpoint Security. Lista ataków sieciowych, wykrywanych przez komponent Blokowanie ataków sieciowych, jest uaktualniana podczas aktualizacji baz danych i modułów aplikacji.

Włączanie i wyłączanie modułu Blokowanie ataków sieciowych

Domyślnie moduł Blokowanie ataków sieciowych jest włączony i działa w trybie optymalnym. W razie konieczności możesz wyłączyć Blokowanie ataków sieciowych.

Istnieją dwa sposoby włączania i wyłączania komponentu:

- W oknie głównym aplikacji, na zakładce**Ochrona i kontrola**
- Z poziomu okna ustawień aplikacji

W celu włączenia lub wyłączenia modułu Blokowanie ataków sieciowych w oknie głównym aplikacji, na zakładce Ochrona i kontrola:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Ochrona**.

   Zostanie otwarta sekcja **Ochrona**.
4. Kliknij prawym przyciskiem myszy wiersz **Blokowanie ataków sieciowych**, aby otworzyć menu kontekstowe z akcjami modułu.
5. Wykonaj jedną z poniższych czynności:
   - Aby włączyć moduł Blokowanie ataków sieciowych, wybierz z menu opcję **Włącz**.

     Ikona stanu modułu , wyświetlana w lewej części wiersza **Blokowanie ataków sieciowych**, zmieni się na ikonę .
   - Aby wyłączyć moduł Blokowanie ataków sieciowych, wybierz z menu opcję **Wyłącz**.

Ikona stanu modułu , wyświetlana w lewej części wiersza **Blokowanie ataków sieciowych**, zmieni się na ikonę .

W celu włączenia lub wyłączenia modułu Blokowanie ataków sieciowych z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Blokowanie ataków sieciowych**.

   W prawej części okna wyświetlone są ustawienia modułu Blokowanie ataków sieciowych.
3. Wykonaj następujące czynności:
   - Aby włączyć Blokowanie ataków sieciowych, zaznacz pole **Włącz moduł Blokowanie ataków sieciowych**.
   - Aby wyłączyć Blokowanie ataków sieciowych, usuń zaznaczenie z pola **Włącz moduł Blokowanie ataków sieciowych**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Ustawienia modułu Blokowanie ataków sieciowych

Podczas konfiguracji ustawień modułu Blokowanie ataków sieciowych możesz wykonać następujące czynności:

- Skonfigurować ustawienia używane do blokowania atakującego komputera.
- Wygenerować listę adresów wykluczonych z blokowania.

Modyfikowanie ustawień używanych do blokowania atakującego komputera

W celu zmodyfikowania ustawień używanych do blokowania atakującego komputera:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Blokowanie ataków sieciowych**.

   W prawej części okna wyświetlone są ustawienia modułu Blokowanie ataków sieciowych.
3. Zaznacz pole **Dodaj atakujący komputer do listy blokowanych komputerów na**.

   Jeżeli pole to zostanie zaznaczone, po wykryciu próby ataku sieciowego moduł Blokowanie ataków sieciowych zablokuje ruch sieciowy pochodzący z atakującego komputera na określony czas. Chroni to komputer automatycznie przed przyszłymi atakami sieciowymi pochodzącymi z tego samego adresu.

   Jeżeli zaznaczenie z tego pola jest usunięte, po wykryciu próby ataku sieciowego moduł Blokowanie ataków sieciowych nie włączy automatycznej ochrony przed przyszłymi atakami sieciowymi pochodzącymi z tego samego adresu.
4. W polu obok opcji **Dodaj atakujący komputer do listy blokowanych komputerów na** zmień czas, na jaki atakujący komputer będzie blokowany.
5. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Konfigurowanie wykluczania adresów z blokowania

W celu skonfigurowania wykluczenia adresów z blokowania:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Blokowanie ataków sieciowych**.
   W prawej części okna wyświetlone są ustawienia modułu Blokowanie ataków sieciowych.
3. Kliknij przycisk **Wykluczenia**.
   Zostanie otwarte okno **Wykluczenia**.
4. Wykonaj jedną z poniższych czynności:
   - Jeżeli chcesz dodać nowy adres IP, kliknij przycisk **Dodaj**.
   - Jeśli chcesz zmodyfikować wcześniej dodany adres IP, wybierz go na liście adresów i kliknij przycisk **Modyfikuj**.

   Zostanie otwarte okno **Adres IP**.
5. Wprowadź adres IP komputera, z którego ataki sieciowe nie będą blokowane.
6. W oknie **Adres IP** kliknij **OK**.
7. W oknie **Wykluczenia** kliknij **OK**.
8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Ochrona przed atakami BadUSB

Ta sekcja zawiera informacje o module Ochrona przed atakami BadUSB

Informacje o module Ochrona przed atakami BadUSB

Niektóre wirusy modyfikują oprogramowanie wbudowane urządzeń USB w celu zmylenia systemu operacyjnego do wykrywania urządzenia USB jako klawiatury.

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

Po podłączeniu urządzenia USB do komputera i zidentyfikowaniu go przez aplikację jako klawiatury, aplikacja wyświetli pytanie o wprowadzenie kodu numerycznego, wygenerowanego przez aplikację, z poziomu tej klawiatury lub Klawiatury ekranowej (jeśli jest dostępna). Ta procedura jest znana jako autoryzacja klawiatury. Aplikacja zezwoli na użycie zautoryzowanej klawiatury, a zablokuje klawiaturę, która nie została zautoryzowana.

Moduł Ochrona przed atakami BadUSB zaczyna działać w tle natychmiast po zainstalowaniu. Jeśli aplikacja nie podlega profilowi Kaspersky Security Center, możesz włączyć lub wyłączyć Ochronę przed atakami BadUSB poprzez tymczasowe wstrzymanie lub wznowienie ochrony i kontroli komputera.

Instalowanie modułu Ochrona przed atakami BadUSB

Jeśli podczas instalacji Kaspersky Endpoint Security wybierzesz instalację podstawową lub standardową, komponent Ochrona przed atakami BadUSB będzie niedostępny. Aby go zainstalować, należy zmienić zestaw komponentów aplikacji.

W celu zainstalowania modułu Ochrona przed atakami BadUSB:

1. W menu **Start** wybierz **Aplikacje** → **Kaspersky Endpoint Security 10 for Windows** → **Modyfikuj, Napraw lub Usuń**.

   Zostanie uruchomiony Kreator instalacji.

2. W oknie **Modyfikuj, Napraw lub Usuń** Kreatora instalacji aplikacji kliknij przycisk **Modyfikuj**.

   Zostanie otwarte okno **Instalacja niestandardowa** Kreatora instalacji aplikacji.

3. Z menu kontekstowego ikony, znajdującej się obok nazwy modułu **Ochrona przed atakami BadUSB**, wybierz opcję **Składnik zostanie zainstalowany na lokalnym dysku twardym**.

4. Kliknij przycisk **Dalej**.

5. Postępuj zgodnie z instrukcjami Kreatora instalacji.

Włączanie i wyłączanie Ochrony przed atakami BadUSB

W celu włączenia lub wyłączenia Ochrony przed atakami BadUSB:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona przed atakami BadUSB**.

   W prawej części okna wyświetlone są ustawienia modułu Ochrona przed atakami BadUSB.

3. Wykonaj jedną z poniższych czynności:

   - Aby włączyć Ochronę przed atakami BadUSB, zaznacz pole **Włącz ochronę przed atakami BadUSB**.
   - Aby wyłączyć Ochronę przed atakami BadUSB, odznacz pole **Włącz ochronę przed atakami BadUSB**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zezwalanie na i blokowanie użycia Klawiatury ekranowej do autoryzacji

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. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ochrona antywirusowa** wybierz podsekcję **Ochrona przed atakami BadUSB**.

   W prawej części okna zostaną wyświetlone ustawienia komponentu.

3. Wykonaj jedną z poniższych czynności:

   - Aby zablokować użycie Klawiatury ekranowej do autoryzacji, zaznacz pole **Zabroń korzystania z Klawiatury ekranowej do autoryzacji**.
   - Aby zezwolić na użycie Klawiatury ekranowej do autoryzacji, odznacz pole **Zabroń korzystania z Klawiatury ekranowej do autoryzacji**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Autoryzacja klawiatury

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.

Aplikacja wymaga przeprowadzenia autoryzacji podłączonego urządzenia USB, które zostało rozpoznane przez system operacyjny jako klawiatura, tylko wtedy, gdy włączone jest wyświetlanie pytania o przeprowadzenie autoryzacji. Użytkownik może użyć niezautoryzowaną klawiaturę dopiero po jej zautoryzowaniu.

Jeśli wyświetlanie pytania o przeprowadzenie autoryzacji klawiatury USB jest wyłączone, użytkownik może używać wszystkich podłączonych klawiatur. Jak tylko wyświetlanie pytania o autoryzację klawiatury USB zostanie włączone, aplikacja wyświetli pytanie o przeprowadzenie autoryzacji każdej nieautoryzowanej klawiatury, która jest podłączona.

W celu zautoryzowania klawiatury:

1. Przy włączonej opcji autoryzacji klawiatury USB podłącz klawiaturę do portu USB.

   Zostanie otwarte okno **Autoryzacja klawiatury <nazwa klawiatury>** zawierające szczegółowe informacje o podłączonej klawiaturze oraz kod numeryczny do jej autoryzacji.

2. W oknie autoryzacji wprowadź losowo wygenerowany kod numeryczny z poziomu podłączonej klawiatury lub Klawiatury ekranowej (jeśli jest dostępna).

3. Kliknij **OK**.

   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. Można podjąć trzy próby wprowadzenia kodu numerycznego. Jeśli kod numeryczny zostanie wprowadzony niepoprawnie trzy razy z rzędu lub okno **Autoryzacja klawiatury <nazwa klawiatury>** zostanie zamknięte, aplikacja zablokuje możliwość wprowadzania danych z poziomu tej klawiatury. Po ponownym podłączeniu klawiatury lub ponownym uruchomieniu systemu operacyjnego, aplikacja ponownie wyświetli pytanie o przeprowadzenie autoryzacji klawiatury.

Kontrola uruchamiania aplikacji

Sekcja ta zawiera informacje o Kontroli uruchamiania aplikacji oraz instrukcje dotyczące konfiguracji ustawień tego modułu.

Informacje o module Kontrola uruchamiania aplikacji

Moduł Kontrola uruchamiania aplikacji monitoruje próby uruchamiania aplikacji przez użytkownika i kontroluje uruchamianie aplikacji przy użyciu *reguł Kontroli uruchamiania aplikacji*.

Uruchamianie aplikacji, których ustawienia nie odpowiadają żadnej z reguł Kontroli uruchamiania aplikacji, jest kontrolowane przez wybrany tryb działania modułu. Domyślnie wybrany jest *tryb Czarna lista*. Ten tryb pozwala każdemu użytkownikowi na uruchamianie dowolnej aplikacji.

Wszystkie próby użytkownika mające na celu uruchomienie aplikacji są zapisywane w raportach.

Włączanie i wyłączanie modułu Kontrola uruchamiania aplikacji

Domyślnie moduł Kontrola uruchamiania aplikacji jest wyłączony, ale w razie konieczności możesz go włączyć.

Istnieją dwa sposoby włączania i wyłączania komponentu:

- W oknie głównym aplikacji, na zakładce **Ochrona i kontrola**
- Z poziomu okna ustawień aplikacji

W celu włączenia lub wyłączenia modułu Kontrola uruchamiania aplikacji w oknie głównym aplikacji, na zakładce Ochrona i kontrola:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Kontrola węzła końcowego**.

   Zostanie otwarta sekcja **Kontrola węzła końcowego**.
4. Kliknij prawym przyciskiem myszy wiersz z informacjami o module Kontrola uruchamiania aplikacji.

   Zostanie otwarte menu wyboru działań.
5. Wykonaj jedną z poniższych czynności:

   - Aby włączyć moduł Kontrola uruchamiania aplikacji, wybierz z menu opcję **Włącz**.

     Ikona stanu modułu , wyświetlana w lewej części wiersza **Kontrola uruchamiania aplikacji**, zmieni się na ikonę .
   - Aby wyłączyć moduł Kontrola uruchamiania aplikacji, wybierz z menu opcję **Wyłącz**.

     Ikona stanu modułu , wyświetlana w lewej części wiersza **Kontrola uruchamiania aplikacji**, zmieni się na ikonę .

W celu włączenia lub wyłączenia modułu Kontrola uruchamiania aplikacji z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uruchamiania aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola uruchamiania aplikacji.
3. Wykonaj jedną z poniższych czynności:
   - Aby włączyć Kontrolę uruchamiania aplikacji, zaznacz pole **Włącz moduł Kontrola uruchamiania aplikacji**.
   - Aby wyłączyć Kontrolę uruchamiania aplikacji, usuń zaznaczenie z pola **Włącz moduł Kontrola uruchamiania aplikacji**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Ograniczenia funkcjonalności Kontroli uruchamiania aplikacji

Działanie komponentu Kontrola uruchamiania aplikacji jest ograniczone w następujących przypadkach:

- Jeśli wersja aplikacji zostanie zaktualizowana, importowanie ustawień komponentu Kontrola uruchamiania aplikacji nie będzie obsługiwane.

  Aby przywrócić funkcjonalność Kontroli uruchamiania aplikacji, należy ponownie skonfigurować ustawienia modułu.

- Jeśli nie ma połączenia z serwerami KSN, Kaspersky Endpoint Security pobiera informacje o reputacji aplikacji i ich modułach z lokalnych baz danych. Jeśli lokalne bazy danych nie zawierają informacji o aplikacji, aplikacja nie zostanie przydzielona do grupy zaufania.

  Kategoryzacja aplikacji, gdy jest połączenie z serwerami KSN, może różnić się od kategoryzacji, gdy nie ma połączenia z KSN.

- 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 uruchamiania aplikacji, komponent nie zablokuje uruchomienia skrypt z tego 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:

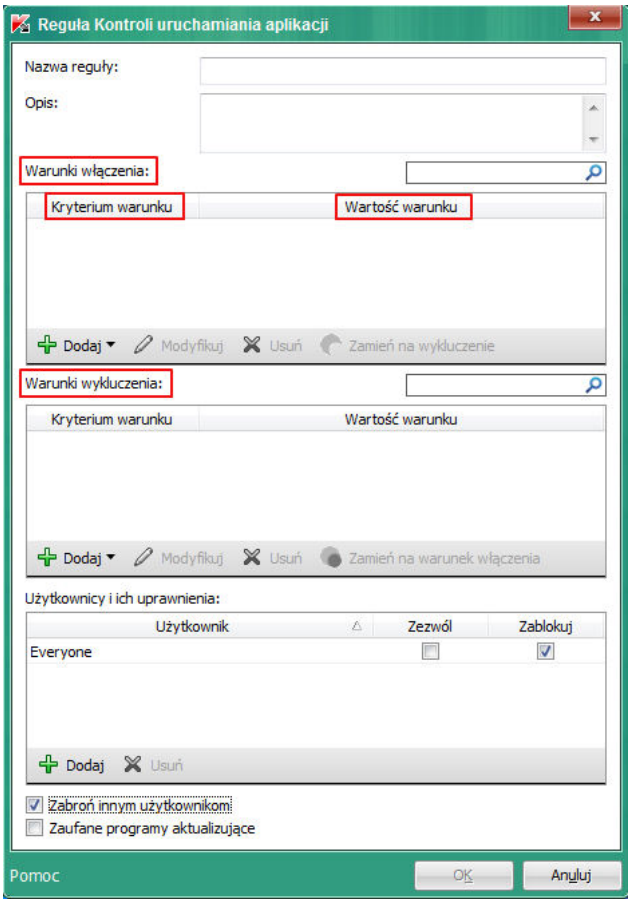
- { cCmdLineParser::itCmd, _T("%ComSpec%") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\system32\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\system32\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\system32\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\system32\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\system32\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\system32\\wwahost.exe") };
- { cCmdLineParser::itCmd, _T("%SystemRoot%\\syswow64\\cmd.exe") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\syswow64\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\syswow64\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\syswow64\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\syswow64\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\syswow64\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\syswow64\\wwahost.exe") }.

Informacje o regułach Kontroli uruchamiania aplikacji

Kaspersky Endpoint Security kontroluje uruchamianie aplikacji przez użytkownika przy użyciu reguł. Reguła Kontroli uruchamiania aplikacji określa warunki wyzwalania reguły oraz działanie wykonywane przez Kontrolę uruchamiania aplikacji, gdy reguła zostaje wyzwolona (zezwalanie na lub blokowanie uruchamianie aplikacji przez użytkowników).

Warunki wyzwalające regułę

Warunek wyzwalający regułę przedstawia następującą zależność: "typ warunku - kryterium warunku - wartość warunku" (zobacz poniższy rysunek). W oparciu o warunki wyzwalające regułę, Kaspersky Endpoint Security stosuje (lub nie stosuje) regułę do aplikacji.



Reguła Kontroli uruchamiania aplikacji. Parametry warunku wyzwalającego regułę

Reguły wykorzystują warunki włączenia oraz warunki wykluczenia:

- *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, użytkownik, 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 uruchamiania aplikacji wykona akcję określoną w regule. Jeśli parametry aplikacji odpowiadają wartościom kryteriów określonych w warunku wykluczenia, Kontrola uruchamiania aplikacji nie kontroluje uruchamiania aplikacji.

Decyzja podjęta przez komponent Kontrola uruchamiania aplikacji w momencie wyzwolenia reguły

Jeśli reguła zostanie wyzwolona, Kontrola uruchamiania aplikacji zezwala użytkownikom (lub grupom użytkowników) na uruchamianie aplikacji lub blokuje uruchomienie zgodnie z regułą. Możesz wybrać pojedynczych użytkownika lub grupę użytkowników, którzy mogą (lub nie mogą) uruchamiać aplikacje wyzwalające regułę.

Jeśli reguła nie określa tych użytkowników mogących uruchamiać aplikacje odpowiadające regule, reguła ta jest zwana regułą *blokującą*.

Jeśli reguła, która nie określa żadnych użytkowników, którzy nie mogą uruchamiać aplikacji odpowiadających regule, reguła ta jest zwana regułą *zezwalającą*.

Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Na przykład, jeśli reguła zezwalająca Kontroli uruchamiania 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 uruchamiania aplikacji mogą posiadać jeden z dwóch stanów działania:

- **Włączona.**

  Ten stan oznacza, że reguła jest włączona.

- **Wyłączona.**

  Ten stan oznacza, że reguła jest wyłączona.

Domyślne reguły Kontroli uruchamiania aplikacji

Domyślnie Kontrola uruchamiania aplikacji działa w trybie Czarnej listy. Ten komponent pozwala wszystkim użytkownikom na uruchamianie wszystkich aplikacji. Jeśli użytkownik spróbuje uruchomić aplikację, która jest zablokowana przez reguły Kontroli uruchamiania aplikacji, Kaspersky Endpoint Security zablokuje uruchomienie tej aplikacji (jeśli zaznaczone jest działanie **Zablokuj**) lub zapisze informacje o uruchomieniu aplikacji w raporcie (jeśli zaznaczone jest działanie **Powiadom**).

Zarządzanie regułami Kontroli uruchamiania aplikacji

Dla reguł Kontroli uruchamiania aplikacji możesz wykonać następujące czynności:

- Dodać nową regułę

- Utworzyć lub zmienić warunki wyzwalania reguły

- Zmodyfikować stan reguły

  Reguła Kontroli uruchamiania aplikacji może być włączona (pole obok reguły jest zaznaczone) lub wyłączona (pole obok reguły jest odznaczone). Po utworzeniu reguła Kontroli uruchamiania aplikacji jest włączona domyślnie.

- Usunąć regułę

Dodawanie i modyfikowanie reguły Kontroli uruchamiania aplikacji

W celu dodania lub zmodyfikowania reguły Kontroli uruchamiania aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uruchamiania aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola uruchamiania aplikacji.
3. Zaznacz opcję **Włącz moduł Kontrola uruchamiania aplikacji**, aby umożliwić modyfikację ustawień modułu.
4. 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 **Modyfikuj**.

   Zostanie otwarte okno **Reguła Kontroli uruchamiania aplikacji**.
5. Określ lub zmodyfikuj ustawienia reguły:

   a. W polu **Nazwa reguły** wprowadź lub zmodyfikuj nazwę reguły.

   b. W tabeli **Warunki włączenia**, utwórz lub zmodyfikuj listę warunków włączenia, które wywołają regułę, klikając przyciski **Dodaj**, **Modyfikuj**, **Usuń** i **Zamień na wykluczenie**.

   c. W tabeli **Warunki wykluczenia** utwórz lub zmodyfikuj listę warunków wykluczenia, które wywołają regułę, klikając przyciski **Dodaj**, **Modyfikuj**, **Usuń** i **Zamień na warunek włączenia**.

   d. Jeśli to konieczne, możesz zmienić typ warunku wyzwalającego regułę:

      - Aby zmienić typ warunku z włączenia na wykluczenie, wybierz warunek w tabeli **Warunki włączenia** i kliknij przycisk **Zamień na wykluczenie**.
      - Aby zmienić typ warunku z wykluczenia na włączenie, wybierz warunek w tabeli **Warunki wykluczenia** i kliknij przycisk **Zamień na warunek włączenia**.

   e. 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**.

      Zostanie otwarte okno **Wybierz Użytkowników lub Grupy** z Microsoft Windows. W tym oknie można wybrać użytkowników i / lub grupy użytkowników.

      Domyślnie wartość **Wszyscy** jest dodana do listy użytkowników. Reguła jest stosowana do wszystkich użytkowników.

Jeśli w w tabeli nie ma określonego użytkownika, reguła nie może zostać zapisana.

f. W tabeli **Użytkownicy i ich uprawnienia** wybierz pole **Zezwól** lub **Blokuj** obok użytkowników i/lub grup, aby określić ich uprawnienia uruchamiania aplikacji.

Pole, które jest domyślnie zaznaczone, zależy od trybu działania Kontroli uruchamiania aplikacji.

g. 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 uruchomienia 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 określeni w tabeli **Użytkownicy i ich uprawnienia** i nie należą do grup użytkowników określonych w tabeli **Użytkownicy i ich uprawnienia**.

h. Jeżeli chcesz, aby Kaspersky Endpoint Security uważał aplikacje spełniające warunki wyzwalające regułę za zaufane programy aktualizujące i zezwalał im na uruchamianie innych aplikacji, dla których nie określono reguły Kontroli uruchamiania aplikacji, zaznacz pole **Zaufane programy aktualizujące**.

6. Kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Dodawanie warunku wyzwalającego dla reguły Kontroli uruchamiania aplikacji

W celu dodania warunku wyzwalającego dla reguły Kontroli uruchamiania aplikacji:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uruchamiania aplikacji**.

W prawej części okna wyświetlone są ustawienia modułu Kontrola uruchamiania aplikacji.

3. Zaznacz opcję **Włącz moduł Kontrola uruchamiania aplikacji**, aby umożliwić modyfikację ustawień modułu.

4. Wykonaj jedną z poniższych czynności:

- Jeśli chcesz utworzyć nową regułę i dodać do niej warunek wyzwalający, kliknij przycisk **Dodaj**.
- Jeśli chcesz dodać warunek wyzwalający do istniejącej reguły, zaznacz na liście reguł żądaną regułę i kliknij przycisk **Modyfikuj**.

Zostanie otwarte okno **Reguła Kontroli uruchamiania aplikacji**.

5. W tabeli **Warunki włączenia** lub **Warunki wykluczenia** kliknij przycisk **Dodaj**.

Lista rozwijalna przycisku **Dodaj** umożliwia dodanie do reguły różnych warunków wyzwalających (patrz poniższa instrukcja).

W celu dodania warunku wyzwalającego regułę w oparciu o właściwości plików w określonym folderze:

1. Z listy rozwijalnej przycisku **Dodaj** wybierz **Warunek/warunki z właściwości plików w określonym folderze**.

   Zostanie otwarte standardowe okno **Wybierz folder** z Microsoft Windows.

2. W oknie **Wybierz folder** wybierz folder zawierający pliki wykonywalne aplikacji, których właściwości chcesz użyć jako podstawy dla jednego lub kilku warunków wyzwalających regułę.

3. Kliknij **OK**.

   Zostanie otwarte okno **Dodaj warunek**.

4. Z listy rozwijalnej **Pokaż kryterium** wybierz kryterium, w oparciu o które chcesz utworzyć jeden lub kilka warunków wyzwalających regułę: **Suma kontrolna pliku**, **Certyfikat**, **Kategoria KL**, **Metadane** lub **Ścieżka do folderu**.

   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.

5. Jeśli na liście rozwijalnej **Pokaż kryterium** wybrałeś **Metadane**, zaznacz pola obok właściwości pliku wykonywalnego, których chcesz użyć w warunku wyzwalającym regułę: **Nazwa pliku**, **Wersja pliku**, **Nazwa aplikacji**, **Wersja aplikacji** i **Producent**.

   Jeśli nie wybrano żadnych określonych właściwości, reguła nie może zostać zapisana.

6. Jeśli na liście rozwijalnej **Pokaż kryterium** wybrano **Certyfikat**, zaznacz pola obok ustawień, których chcesz użyć w warunku wyzwalającym regułę: **Wydawca**, **Użytkownik** i **Odcisk palca**.

   Jeśli nie wybrano żadnych określonych ustawień, reguła nie może zostać zapisana.

   Nie jest zalecane używanie tylko **Wydawca** i **Użytkownik** jako warunków wyzwalających regułę. Użycie tych kryteriów jest niemiarodajne.

7. Zaznacz pola obok nazw plików wykonywalnych aplikacji, których właściwości chcesz włączyć do warunków wyzwalających regułę.

8. Kliknij przycisk **Dalej**.

   Zostanie wyświetlona lista warunków wyzwalających regułę.

9. Na wyświetlonej liście zaznacz pola obok warunków wyzwalających regułę, które chcesz dodać do reguły Kontroli uruchamiania aplikacji.

10. Kliknij przycisk **Zakończ**.

W celu dodania warunku wyzwalającego regułę w oparciu o właściwości aplikacji uruchomionej na komputerze:

1. Z listy rozwijalnej przycisku **Dodaj** wybierz **Warunek/warunki z właściwości uruchomionych aplikacji**.

2. W oknie **Dodaj warunek**, z listy rozwijalnej **Pokaż kryterium** wybierz kryterium, w oparciu o które chcesz utworzyć jeden lub kilka warunków wyzwalających regułę: **Suma kontrolna pliku**, **Certyfikat**, **Kategoria KL**, **Metadane** lub **Ścieżka do folderu.**

3. Jeśli na liście rozwijalnej **Pokaż kryterium** wybrałeś **Metadane**, zaznacz pola obok właściwości pliku wykonywalnego, których chcesz użyć w warunku wyzwalającym regułę: **Nazwa pliku**, **Wersja pliku**, **Nazwa aplikacji**, **Wersja aplikacji** i **Producent**.

   Jeśli nie wybrano żadnych określonych właściwości, reguła nie może zostać zapisana.

4. Jeśli na liście rozwijalnej **Pokaż kryterium** wybrano **Certyfikat**, zaznacz pola obok ustawień, których chcesz użyć w warunku wyzwalającym regułę: **Wydawca**, **Użytkownik** i **Odcisk palca**.

   Jeśli nie wybrano żadnych określonych ustawień, reguła nie może zostać zapisana.

   > Nie jest zalecane używanie tylko **Wydawca** i **Użytkownik** jako warunków wyzwalających regułę. Użycie tych kryteriów jest niemiarodajne.

5. Zaznacz pola obok nazw plików wykonywalnych aplikacji, których właściwości chcesz włączyć do warunków wyzwalających regułę.

6. Kliknij przycisk **Dalej**.

   Zostanie wyświetlona lista warunków wyzwalających regułę.

7. Na wyświetlonej liście zaznacz pola obok warunków wyzwalających regułę, które chcesz dodać do reguły Kontroli uruchamiania aplikacji.

8. Kliknij przycisk **Zakończ**.

W celu dodania warunku wyzwalającego reguły w oparciu o kategorię KL:

1. Z listy rozwijalnej przycisku **Dodaj** wybierz **Warunek/warunki „Kategorii KL”**.

   Kategoria KL to lista aplikacji, które mają podobne atrybuty. Lista jest tworzona przez specjalistów z Kaspersky. Na przykład, kategoria "Aplikacje biurowe" zawiera aplikacje pakietu Microsoft Office, Adobe® Acrobat® i wiele innych.

2. W oknie **Warunek/warunki „Kategorii KL”** zaznacz pola obok nazw tych kategorii KL, w oparciu o które chcesz utworzyć warunki wyzwalające regułę.

3. Kliknij **OK**.

W celu dodania niestandardowego warunku wyzwalającego regułę:

1. Z listy rozwijalnej przycisku **Dodaj** wybierz **Warunek niestandardowy**.

2. W oknie **Warunek niestandardowy** kliknij przycisk **Wybierz** i określ ścieżkę dostępu do pliku wykonywalnego aplikacji.

3. Wybierz kryterium, w oparciu o które chcesz utworzyć warunek wyzwalający regułę: **Suma kontrolna pliku**, **Certyfikat**, **Metadane** lub **Ścieżka do pliku lub folderu**.

   > Jeśli używasz dowiązań symbolicznych, w polu **Ścieżka do pliku lub folderu** zalecane jest rozwiązanie dowiązań symbolicznych w celu poprawnego działania reguły Kontroli uruchamiania aplikacji. W tym celu kliknij przycisk **Rozwiąż dowiązanie symboliczne**.

4. Jeśli to konieczne, skonfiguruj ustawienia wybranego kryterium.

5. Kliknij **OK**.

W celu dodania warunku wyzwalającego regułę w oparciu o informacje o nośniku, na którym jest przechowywany plik wykonywalny aplikacji:

1. Z listy rozwijalnej przycisku **Dodaj** wybierz **Warunek według nośnika pliku**.

2. W oknie **Warunek według nośnika pliku**, z listy rozwijalnej **Dysk** wybierz typ dysku, z którego uruchamianie aplikacji będzie służyło jako warunek wyzwalający regułę.

3. Kliknij **OK**.

Zmienianie stanu reguły Kontroli uruchamiania aplikacji

W celu zmiany stanu reguły Kontroli uruchamiania aplikacji:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uruchamiania aplikacji**.
   W prawej części okna wyświetlone są ustawienia modułu Kontrola uruchamiania aplikacji.

3. Zaznacz opcję **Włącz moduł Kontrola uruchamiania aplikacji**, aby umożliwić modyfikację ustawień modułu.

4. Wybierz regułę, której stan chcesz zmienić.

5. W kolumnie **Stan** wykonaj następujące czynności:

   - Jeśli chcesz włączyć używanie reguły, zaznacz pole obok tej reguły.
   - Jeśli chcesz wyłączyć używanie reguły, odznacz pole obok tej reguły.

6. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Testowanie działania reguły Kontroli uruchamiania aplikacji

Aby upewnić się, że reguły Kontroli uruchamiania aplikacji nie będą blokowały aplikacji niezbędnych do pracy, zalecane jest przełączenie nowo utworzonych reguł do trybu testowego i sprawdzenie ich działania.

Analiza działania reguł Kontroli uruchamiania aplikacji obejmuje przejrzenie zdarzeń Kontroli uruchamiania aplikacji dostępnych w Kaspersky Security Center. Jeśli dozwolone jest uruchamianie wszystkich aplikacji niezbędnych do pracy użytkownika komputera, reguły zostały poprawnie utworzone. Jeśli jest inaczej, zalecane jest sprawdzenie ustawień utworzonych reguł.

Domyślnie, tryb testowy dla reguł Kontroli uruchamiania aplikacji jest wyłączony.

W celu sprawdzenia reguł Kontroli uruchamiania aplikacji:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uruchamiania aplikacji**.
   W prawej części okna wyświetlone są ustawienia modułu Kontrola uruchamiania aplikacji.

3. Zaznacz opcję **Włącz moduł Kontrola uruchamiania aplikacji**, aby umożliwić modyfikację ustawień modułu.

4. Z listy rozwijalnej **Tryb Kontroli uruchamiania aplikacji** wybierz jeden z następujących elementów:

- **Czarna lista**, jeśli chcesz zezwolić na uruchamianie wszystkich aplikacji, za wyjątkiem aplikacji określonych w regułach blokujących.
- **Biała lista**, jeśli chcesz zablokować uruchamianie wszystkich aplikacji, za wyjątkiem aplikacji określonych w regułach zezwalających.

5. Z listy rozwijalnej **Akcja** wybierz **Powiadom**.
6. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Kaspersky Endpoint Security nie zablokuje aplikacji, których uruchamianie jest zabronione przez reguły Kontroli uruchamiania aplikacji, ale wyśle informacje o ich uruchomieniu do Serwera administracyjnego.

Modyfikowanie szablonów wiadomości Kontroli uruchamiania aplikacji

Podczas próby uruchomienia aplikacji zablokowanej przez regułę Kontroli uruchamiania aplikacji program Kaspersky Endpoint Security wyświetli wiadomość informująca o zablokowaniu aplikacji przed uruchomieniem. 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. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uruchamiania aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola uruchamiania aplikacji.
3. Zaznacz opcję **Włącz moduł Kontrola uruchamiania aplikacji**, aby umożliwić modyfikację ustawień modułu.
4. Kliknij przycisk **Szablony**.

   Zostanie otwarte okno **Szablony wiadomości**.
5. Wykonaj jedną z poniższych czynności:
   - Jeśli chcesz zmodyfikować szablon wiadomości wyświetlanej podczas próby uruchamiania zablokowanej aplikacji, wybierz zakładkę **Blokada**.
   - Jeśli chcesz zmodyfikować szablon wiadomości wysyłanej do administratora sieci LAN, wybierz zakładkę **Wiadomość do administratora**.
6. Zmodyfikuj szablon wiadomości wyświetlanej, gdy zostaje zablokowane uruchomienie aplikacji, oraz wiadomości wysyłanej do administratora. W tym celu użyj przycisków **Domyślny** lub **Zmienna**.
7. Kliknij **OK**.
8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Informacje o trybach działania Kontroli uruchamiania aplikacji

Moduł Kontrola uruchamiania aplikacji działa w dwóch trybach:

- **Czarna lista**. W tym trybie Kontrola uruchamiania aplikacji zezwala wszystkim użytkownikom na uruchamianie wszystkich aplikacji, za wyjątkiem tych określonych w regułach blokujących Kontroli uruchamiania aplikacji.

  Ten tryb jest włączony domyślnie.

- **Biała lista**. W tym trybie Kontrola uruchamiania aplikacji blokuje wszystkim użytkownikom możliwość uruchamiania wszelkich aplikacji, za wyjątkiem tych określonych w regułach zezwalających Kontroli uruchamiania aplikacji.

  Jeżeli reguły zezwalające Kontroli uruchamiania 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.

Każdy tryb oferuje dwa działania, które można wykonać na uruchomionych aplikacjach: Kaspersky Endpoint Security może zablokować uruchomienie aplikacji lub powiadomić użytkownika o uruchomieniu aplikacji, która odpowiada warunkom reguł Kontroli uruchamiania aplikacji.

Moduł Kontrola uruchamiania 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:

- Tworzeni kategorii aplikacji.

  Reguły Kontroli uruchamiania 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.

- Zbierania informacji o aplikacjach zainstalowanych na komputerach w sieci LAN.

Dlatego zalecane jest korzystanie z Kaspersky Security Center podczas konfigurowania działania modułu Kontrola uruchamiania aplikacji.

Wybieranie trybu Kontroli uruchamiania aplikacji

W celu wybrania trybu Kontroli uruchamiania aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uruchamiania aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola uruchamiania aplikacji.
3. Zaznacz opcję **Włącz moduł Kontrola uruchamiania aplikacji**, aby umożliwić modyfikację ustawień modułu.
4. Z listy rozwijalnej **Tryb Kontroli uruchamiania aplikacji** wybierz jedną z następujących opcji:

   - **Czarna lista**, jeśli chcesz zezwolić na uruchamianie wszystkich aplikacji, za wyjątkiem aplikacji określonych w regułach blokujących.
   - **Biała lista**, jeśli chcesz zablokować uruchamianie wszystkich aplikacji, za wyjątkiem aplikacji określonych w regułach zezwalających.

Jeśli ten tryb zostanie wybrany, domyślnie tworzone są dwie reguły Kontroli uruchamiania aplikacji: **Obraz systemu** i **Zaufane programy aktualizujące**. Nie możesz usunąć tych reguł. Ustawienia dla tych reguł nie mogą być modyfikowane. Możesz włączyć lub wyłączyć te reguł, zaznaczając lub odznaczając pola znajdujące się obok ich nazw. 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 móc korzystać z tych reguł, należy jedynie wybrać odpowiedni tryb na liście **Tryb Kontroli uruchamiania aplikacji**.

5. Na liście rozwijanej **Akcja** wybierz akcję, jaka zostanie wykonana przez moduł, gdy użytkownik spróbuje uruchomić aplikację, która jest blokowana przez reguły Kontroli uruchamiania aplikacji.

6. Zaznacz pole **Monitoruj DLL i sterowniki**, 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.

   Jeśli pole jest zaznaczone, sterowniki i moduły DLL są monitorowane przed uruchomieniem Kaspersky Endpoint Security. Aby skonfigurować monitorowanie wszystkich sterowników i modułów DLL przed uruchomieniem aplikacji, po zaznaczeniu pola **Monitoruj DLL i sterowniki** uruchom ponownie komputer. Jeśli nie możesz uruchomić ponownie komputera, po zaznaczeniu pola **Monitoruj DLL i sterowniki** możesz załadować sterowniki i moduły DLL podczas działania Kaspersky Endpoint Security. W tej sytuacji monitorowane będą tylko sterowniki i moduły DLL, które są ładowane podczas działania Kaspersky Endpoint Security.

   Podczas monitorowania sterowników i modułów DLL nie jest zalecane korzystanie z reguł Kontroli uruchamiania aplikacji, które zostały utworzone w oparciu o kategorie KL. Określanie kategorii KL (w tym reguł "System operacyjny i jego składniki") dla sterowników i modułów DLL może działać niepoprawnie. Reguła "System operacyjny i jego składniki" została utworzona domyślnie i nie jest przydzielana podczas uruchamiania sterownika i modułu DLL. Podczas włączania tej funkcji konieczne jest utworzenie oddzielnych reguł zezwalających dla sterowników i modułów DLL. Korzystanie z funkcji **Monitoruj DLL i sterowniki**, gdy takie reguły zezwalające nie istnieją, mogłoby spowodować niestabilność systemu.

   Zalecamy włączenie ochrony hasłem dla konfiguracji ustawień programu, aby możliwe było wyłączenie reguł zezwalających blokujących uruchomienie krytycznie ważnych sterowników i modułów DLL przy nie wprowadzaniu zmian w ustawieniach profilu Kaspersky Security Center.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zarządzanie regułami Kontroli uruchamiania aplikacji przy użyciu Kaspersky Security Center

Ta sekcja zawiera informacje dotyczące używania Kaspersky Security Center do konfiguracji reguł Kontroli uruchamiania aplikacji oraz zalecenia dotyczące optymalnego wykorzystania Kontroli uruchamiania aplikacji.

Zbieranie informacji o aplikacjach zainstalowanych na komputerach użytkowników

Aby utworzyć optymalne reguły Kontroli uruchamiania aplikacji, najpierw należy zastanowić się, które aplikacje są używane na komputerach w sieci lokalnej. 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 na komputerach w firmowej sieci LAN są dostępne w folderze **Rejestr aplikacji** oraz w folderze **Pliki wykonywalne**. Foldery **Rejestr aplikacji** i **Pliki wykonywalne** znajdują się w folderze **Zarządzanie aplikacją**, 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**.

Tworzenie kategorii aplikacji

Aby tworzenie reguł było wygodniejsze, możesz utworzyć kategorie aplikacji i użyć ich podczas tworzenia reguł Kontroli uruchamiania 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 aplikacją** → **Kategorie aplikacji**.
3. W obszarze roboczym kliknij **Utwórz kategorię**.

   Zostanie uruchomiony Kreator tworzenia kategorii użytkownika.
4. Postępuj zgodnie z instrukcjami Kreatora tworzenia kategorii użytkownika.

Tworzenie reguł Kontroli uruchamiania aplikacji przy użyciu Kaspersky Security Center

W celu utworzenia reguł Kontroli uruchamiania 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 interesujący Cię profil.

5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:

   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.

   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.

6. W sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uruchamiania aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola uruchamiania aplikacji.

7. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Reguła Kontroli uruchamiania aplikacji**.

8. Z listy rozwijalnej **Kategoria** wybierz utworzoną kategorię aplikacji, w oparciu o którą chcesz utworzyć regułę.

9. Określ listę użytkowników i / lub grupy użytkowników, dla których chcesz skonfigurować uprawnienia uruchamiania aplikacji z wybranej kategorii. W tym celu, w tabeli **Użytkownicy i ich uprawnienia** kliknij przycisk **Dodaj**.

   Zostanie otwarte standardowe okno **Wybierz Użytkowników lub Grupy** z Microsoft Windows. W tym oknie można wybrać użytkowników i / lub grupy użytkowników.

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 tych użytkowników.

    - Jeśli chcesz zablokować użytkownikom i / lub grupom użytkowników możliwość uruchamiania aplikacji, które należą do wybranej kategorii, zaznacz pola **Blokuj** obok tych użytkowników.

11. Wybierz pole **Zabroń innym użytkownikom**, jeśli chcesz, aby dla wszystkich użytkowników, którzy nie pojawiają się w kolumnie **Użytkownicy** i nie są częścią grupy użytkowników określonej w kolumnie **Użytkownicy**, została zablokowana możliwość uruchamiania aplikacji, które należą do wybranej kategorii.

12. Jeżeli chcesz, aby Kaspersky Endpoint Security uważał aplikacje z kategorii określonej w regule za zaufane programy aktualizujące z prawem do uruchamiania innych aplikacji, dla których nie określono reguły Kontroli uruchamiania aplikacji, zaznacz pole **Zaufane programy aktualizujące**.

13. Kliknij **OK**.

14. W sekcji **Kontrola uruchamiania aplikacji** okna właściwości profilu kliknij przycisk **Zastosuj**.

Zmienianie stanu reguły Kontroli uruchamiania aplikacji przy użyciu Kaspersky Security Center

W celu zmiany stanu reguły Kontroli uruchamiania 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 interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uruchamiania aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola uruchamiania aplikacji.
7. Wybierz regułę Kontroli uruchamiania aplikacji, której stan chcesz zmienić.
8. W kolumnie **Stan** wykonaj jedną z następujących czynności:
   - Jeśli chcesz włączyć używanie reguły, zaznacz pole obok tej reguły.
   - Jeśli chcesz wyłączyć używanie reguły, odznacz pole obok tej reguły.
9. Kliknij przycisk **Zastosuj**.

Kontrola uprawnień aplikacji

Komponent jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów plików.

Sekcja ta zawiera informacje o Kontroli uprawnień aplikacji oraz instrukcje dotyczące konfiguracji ustawień tego modułu.

Informacje o module Kontrola uprawnień aplikacji

Kontrola uprawnień aplikacji uniemożliwia aplikacjom wykonywanie działań niebezpiecznych dla systemu operacyjnego i zapewnia kontrolę dostępu do zasobów systemu operacyjnego i danych tożsamości.

Moduł ten kontroluje aktywność aplikacji, łącznie z ich dostępem do chronionych zasobów (plików i folderów, kluczy rejestru), przy użyciu *reguł kontroli aplikacji*. Reguły kontroli aplikacji to zestaw ograniczeń, które są stosowane do różnych akcji wykonywanych przez aplikacje w systemie operacyjnym, oraz praw dostępu do zasobów komputera.

Aktywność sieciowa aplikacji jest monitorowana przez komponent Zapora sieciowa.

Podczas pierwszego uruchomienia aplikacji moduł Kontrola uprawnień aplikacji skanuje aplikację i umieszcza ją w grupie zaufania. Grupa zaufania określa reguły kontroli aplikacji, które są stosowane przez Kaspersky Endpoint Security podczas kontrolowania aktywności aplikacji.

Zalecane jest uczestniczenie w Kaspersky Security Network, aby Kontrola uprawnień aplikacji mogła działać efektywniej. Dane uzyskane przy pomocy Kaspersky Security Network umożliwią bardziej precyzyjne przydzielanie aplikacji do grup oraz zastosowanie optymalnych reguł kontroli aplikacji.

przy następnym uruchomieniu aplikacji moduł Kontrola uprawnień aplikacji zweryfikuje integralność aplikacji. Jeżeli aplikacja nie została zmieniona, moduł stosuje do niej bieżące reguły kontroli aplikacji. Jeżeli aplikacja została zmieniona, Kontrola uprawnień aplikacji skanuje ją tak, jakby była uruchamiana po raz pierwszy.

Ograniczenia kontroli urządzeń audio-wideo

Informacje o ochronie strumienia danych

W przypadku ochrony strumienia audio należy mieć na uwadze następujące kwestie:

- Aby ta funkcjonalność mogła działać, należy włączyć moduł Kontrola uprawnień aplikacji.
- Jeśli aplikacja zaczęła odbierać strumień audio przed uruchomieniem Kontroli uprawnień aplikacji, Kaspersky Endpoint Security zezwoli aplikacji na odbieranie strumienia audio i nie wyświetli żadnego komunikatu.
- Jeśli po rozpoczęciu odbierania przez aplikację strumienia audio przeniosłeś ją go grupy **Niezaufane** lub **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 w oknie ustawień Kontroli aplikacji, 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.

Kwestie specjalne dotyczące działania urządzeń audio-wideo podczas instalacji i aktualizacji Kaspersky Endpoint Security

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.

Informacje o dostępie aplikacji do kamer internetowych

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 kontroluje jedynie kamery podłączone do portów USB lub IEEE1394, które są wyświetlane w Menedżerze urządzeń systemu Windows jako **Urządzenia do obrazowania**.

Obsługiwane kamery internetowe

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.

Włączanie i wyłączanie modułu Kontrola uprawnień aplikacji

Domyślnie moduł Kontrola uprawnień aplikacji jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky. W razie konieczności możesz wyłączyć Kontrolę uprawnień aplikacji.

Istnieją dwa sposoby włączania i wyłączania komponentu:

- W oknie głównym aplikacji, na zakładce**Ochrona i kontrola**
- Z poziomu okna ustawień aplikacji

W celu włączenia lub wyłączenia modułu Kontrola uprawnień aplikacji w oknie głównym aplikacji, na zakładce Ochrona i kontrola:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Kontrola węzła końcowego**.
   Zostanie otwarta sekcja **Kontrola węzła końcowego**.
4. Kliknij prawym przyciskiem myszy wiersz z informacjami o module Kontrola uprawnień aplikacji.
   Zostanie otwarte menu wyboru działań.
5. Wykonaj jedną z poniższych czynności:
   - Aby włączyć moduł Kontrola uprawnień aplikacji, wybierz z menu opcję **Włącz**.
     Ikona stanu modułu , wyświetlana w lewej części wiersza Kontrola uprawnień aplikacji, zmieni się na ikonę .
   - Aby wyłączyć moduł Kontrola uprawnień aplikacji, wybierz z menu opcję **Wyłącz**.
     Ikona stanu modułu , wyświetlana w lewej części wiersza Kontrola uprawnień aplikacji, zmieni się na ikonę .

W celu włączenia lub wyłączenia modułu Kontrola uprawnień aplikacji z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uprawnień aplikacji**.
   W prawej części okna wyświetlone są ustawienia modułu Kontrola uprawnień aplikacji.
3. W prawej części okna wykonaj jedną z poniższych czynności:
   - Aby włączyć Kontrolę uprawnień aplikacji, zaznacz pole **Włącz moduł Kontrola uprawnień aplikacji**.
   - Aby wyłączyć Kontrolę uprawnień aplikacji, usuń zaznaczenie z pola **Włącz moduł Kontrola uprawnień aplikacji**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zarządzanie grupami zaufania aplikacji

Podczas pierwszego uruchomienia aplikacji moduł Kontrola uprawnień aplikacji 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 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 określić grupę zaufania, do której program Kaspersky Endpoint Security będzie automatycznie dodawał wszystkie nieznane aplikacje. Aplikacje, które zostały uruchomione przed Kaspersky Endpoint Security, są automatycznie przenoszone do grupy zaufania określonej w oknie **Wybierz grupę zaufania**.

Komponent kontroluje tylko aktywność sieciową aplikacji uruchomionych przed Kaspersky Endpoint Security w oparciu o reguły sieciowe zdefiniowane w ustawieniach Zapory sieciowej.

Konfigurowanie ustawień przydzielania aplikacji do grup 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 odpowiedź z KSN, aplikacja może zostać przeniesiona do grupy zaufania, która jest inna niż ta określona w ustawienia Kontroli uprawnień aplikacji.

W celu skonfigurowania ustawień dla umieszczania aplikacji w grupach zaufania:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uprawnień aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola uprawnień aplikacji.

3. Jeżeli chcesz, aby aplikacje podpisane cyfrowo przez zaufanych dostawców były automatycznie dodawane do grupy Zaufane, zaznacz pole **Ufaj aplikacjom posiadającym podpis cyfrowy**.

   Zaufani producenci to producenci oprogramowania, którzy zostali umieszczeni w grupie zaufania przez Kaspersky. Możesz także ręcznie dodać certyfikat producenta do zaufanych certyfikatów systemowych.

4. Wybierz sposób przydzielania nieznanych aplikacji do grup zaufania:

   - Aby używać analizy heurystycznej do przydzielania nieznanych aplikacji do grup zaufania, zaznacz opcję **Użyj analizy heurystycznej do określenia grupy** i w polu **Maksymalny czas na określenie grupy** określ czas przydzielony do skanowania uruchomionych aplikacji.

   - Jeśli chcesz przenieść wszystkie nieznane aplikacje do określonej grupy zaufania, wybierz **Automatycznie przenieś do grupy** i wybierz wymaganą grupę z listy rozwijalnej.

W celach zapewnienia bezpieczeństwa grupa **Zaufane** nie jest uwzględniona w wartościach ustawienia **Automatycznie przenieś do grupy**.

5. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Modyfikowanie grupy zaufania

Podczas pierwszego uruchomienia aplikacji Kaspersky Endpoint Security automatycznie umieszcza ją w grupie zaufania. W razie konieczności możesz ręcznie przenieść aplikację do innej grupy zaufania.

Specjaliści z Kaspersky nie zalecają przenoszenia aplikacji z automatycznie przydzielonej grupy zaufania do innej grupy zaufania. W zamian, możesz edytować reguły dla indywidualnej aplikacji.

W celu zmiany grupy zaufania, do której Kaspersky Endpoint Security automatycznie przydzielił aplikację po jej pierwszym uruchomieniu:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uprawnień aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola uprawnień aplikacji.
3. Kliknij przycisk **Aplikacje**.

   Okno **Aplikacje** zostanie otwarte na zakładce **Reguły kontroli aplikacji**.
4. Wybierz odpowiednią aplikację na zakładce **Reguły kontroli aplikacji**.
5. Wykonaj jedną z poniższych czynności:

   - Kliknij prawym klawiszem myszy, aby wyświetlić menu kontekstowe aplikacji. Z menu kontekstowego aplikacji wybierz **Przenieś do grupy** → <ναζωα γρυπψ>.
   - Aby otworzyć menu, kliknij odnośnik **Zaufane** / **Niski poziom ograniczeń** / **Wysoki poziom ograniczeń** / **Niezaufane**. Z menu kontekstowego wybierz żądaną grupę zaufania.
6. Kliknij **OK**.
7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Wybieranie grupy zaufania dla aplikacji uruchamianych przed Kaspersky Endpoint Security

Komponent kontroluje tylko aktywność sieciową aplikacji, które zostały uruchomione przed Kaspersky Endpoint Security. 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.

W celu wybrania grupy zaufania dla aplikacji uruchamianych przed Kaspersky Endpoint Security:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uprawnień aplikacji**.
   W prawej części okna wyświetlone są ustawienia modułu Kontrola uprawnień aplikacji.
3. Kliknij przycisk **Modyfikuj**.
   Zostanie otwarte okno **Wybierz grupę zaufania**.
4. Wybierz żądaną grupę zaufania.
5. Kliknij **OK**.
6. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zarządzanie regułami Kontroli aplikacji

Domyślnie aktywność aplikacji jest kontrolowana przez reguły kontroli aplikacji zdefiniowane dla grupy zaufania, do której Kaspersky Endpoint Security przypisał aplikację przy jej pierwszym uruchomieniu. Jeżeli jest to konieczne, możesz zmodyfikować reguły kontroli aplikacji dla całej grupy zaufania, dla pojedynczej aplikacji lub grupy aplikacji znajdujących się w grupie zaufania.

Reguły kontroli aplikacji zdefiniowane dla pojedynczej aplikacji lub grupy aplikacji znajdujących się w grupie zaufania mają wyższy priorytet niż reguły kontroli aplikacji zdefiniowane dla grupy zaufania. Innymi słowy, jeżeli ustawienia reguł kontroli aplikacji dla pojedynczej aplikacji lub grupy aplikacji znajdujących się w grupie zaufania różnią się od ustawień reguł kontroli aplikacji dla grupy zaufania, moduł Kontrola uprawnień aplikacji będzie kontrolował aktywność aplikacji lub grupy aplikacji znajdujących się w grupie zaufania zgodnie z regułami kontroli aplikacji, które zostały dla nich zdefiniowane.

Zmienianie reguł kontroli aplikacji dla grup zaufania i grup aplikacji

Optymalne reguły kontroli aplikacji dla różnych grup zaufania są tworzone domyślnie. Ustawienia reguł dla kontroli grupy aplikacji dziedziczą wartości z ustawień reguł kontroli grupy zaufania. Możesz zmodyfikować predefiniowane reguły kontroli grupy zaufania i reguły dla kontroli grupy aplikacji.

W celu zmodyfikowania reguł kontroli grupy zaufania lub reguł kontroli grupy aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uprawnień aplikacji**.
   W prawej części okna wyświetlone są ustawienia modułu Kontrola uprawnień aplikacji.
3. Kliknij przycisk **Aplikacje**.
   Zostanie otwarte okno **Kontrola uprawnień aplikacji** na zakładce **Reguły kontroli aplikacji**.
4. Wybierz żądaną grupę zaufania lub grupę aplikacji.
5. Z menu kontekstowe grupy zaufania lub grupy aplikacji wybierz **Reguły grupy**.
   Zostanie otwarte okno **Reguły kontroli aplikacji**.

6. W oknie **Reguły kontroli aplikacji** wykonaj jedną z poniższych czynności:

   - Aby zmodyfikować reguły kontroli grupy zaufania lub reguły kontroli grupy aplikacji zarządzające uprawnieniami dostępu grupy zaufania lub grupy aplikacji do rejestru systemu operacyjnego, plików użytkownika i ustawień aplikacji, wybierz zakładkę **Pliki i rejestr systemu**.

   - Aby zmodyfikować reguły kontroli grupy zaufania lub reguły kontroli grupy aplikacji zarządzające uprawnieniami dostępu grupy zaufania lub grupy aplikacji do procesów i obiektów systemu operacyjnego, wybierz zakładkę **Uprawnienia**.

7. Dla wymaganego zasobu kliknij prawym przyciskiem myszy odpowiadającą kolumnę akcji, aby otworzyć menu kontekstowe.

8. Z otwartego menu wybierz żądany element.

   - **Dziedzicz**
   - **Zezwól**
   - **Zablokuj**
   - **Zapisuj zdarzenia**

   Jeżeli modyfikujesz reguły kontroli grupy zaufania, element **Dziedzicz** nie jest dostępny.

9. Kliknij **OK**.

10. W oknie **Aplikacje** kliknij **OK**.

11. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Modyfikowanie reguły kontroli aplikacji

Domyślnie ustawienia reguł kontroli aplikacji dla aplikacji należących do grupy aplikacji lub grupy zaufania dziedziczą wartości ustawień reguł kontroli grupy zaufania. Możesz zmodyfikować ustawienia reguł kontroli aplikacji.

W celu zmiany reguły kontroli aplikacji:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uprawnień aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola uprawnień aplikacji.

3. Kliknij przycisk **Aplikacje**.

   Zostanie otwarte okno **Kontrola uprawnień aplikacji** na zakładce **Reguły kontroli aplikacji**.

4. Wybierz żądaną aplikację.

5. Wykonaj jedną z poniższych czynności:

   - Z menu kontekstowego aplikacji wybierz **Reguły aplikacji**.

- Kliknij przycisk **Dodatkowe** w prawym dolnym rogu zakładki **Reguły kontroli aplikacji**.

Zostanie otwarte okno **Reguły kontroli aplikacji**.

6. W oknie **Reguły kontroli aplikacji** wykonaj jedną z poniższych czynności:

   - Aby zmodyfikować reguły kontroli aplikacji zarządzające uprawnieniami aplikacji do dostępu do rejestru systemu operacyjnego, plików użytkownika i ustawień aplikacji, wybierz zakładkę **Pliki i rejestr systemu**.
   - Aby zmodyfikować reguły kontroli aplikacji zarządzające uprawnieniami aplikacji do dostępu do procesów i obiektów systemu, wybierz zakładkę **Uprawnienia**.

7. Dla wymaganego zasobu kliknij prawym przyciskiem myszy odpowiadającą kolumnę akcji, aby otworzyć menu kontekstowe.
8. Z otwartego menu wybierz żądany element.

   - **Dziedzicz**
   - **Zezwól**
   - **Zablokuj**
   - **Zapisuj zdarzenia**

9. Kliknij **OK**.
10. W oknie **Aplikacje** kliknij **OK**.
11. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Wyłączanie pobierania i aktualizacji reguł kontroli aplikacji z bazy danych Kaspersky Security Network

Domyślnie, jeśli nowe informacje o aplikacji zostaną wykryte w bazie danych Kaspersky Security Network, Kaspersky Endpoint Security zastosuje reguły kontroli pobrane z bazy danych KSN dla tej aplikacji. Następnie możesz ręcznie zmodyfikować reguły kontroli aplikacji.

Jeśli aplikacja nie została odnaleziona w bazie danych Kaspersky Security Network przy pierwszym uruchomieniu, a informacja o niej została dodana później, Kaspersky Endpoint Security domyślnie automatycznie zaktualizuje reguły kontroli dla tej aplikacji.

Możesz wyłączyć pobieranie reguł kontroli aplikacji z bazy danych Kaspersky Security Network i automatyczne aktualizacje reguł kontroli dla wcześniej nieznanych aplikacji.

W celu wyłączenia pobierania i aktualizacji reguł kontroli aplikacji z bazy danych Kaspersky Security Network:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uprawnień aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola uprawnień aplikacji.

3. Usuń zaznaczenie z pola **Uaktualnij reguły dla wcześniej nieznanych aplikacji z bazy danych KSN**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Wyłączanie dziedziczenia ograniczeń procesu nadrzędnego

Uruchomienie aplikacji może zostać zainicjowane przez użytkownika lub inną działającą w danym momencie aplikację. W przypadku uruchomienia aplikacji przez inną aplikację, zostaje utworzona procedura startowa zawierająca procesy nadrzędne i potomne.

Kiedy aplikacja próbuje uzyskać dostęp do chronionego zasobu, Kontrola uprawnień aplikacji analizuje wszystkie procesy nadrzędne aplikacji, aby określić, czy procesy te mają uprawnienia dostępu do chronionego zasobu. W procesie tym stosowana będzie reguła o minimalnym priorytecie: podczas porównywania uprawnień dostępu danej aplikacji z uprawnieniami procesu nadrzędnego, do aktywności aplikacji zastosowane będą uprawnienia dostępu o najniższym priorytecie.

Priorytet uprawnień dostępu może być następujący:

1. **Zezwól** To uprawnienie dostępu ma najwyższy priorytet.
2. **Zablokuj** To uprawnienie dostępu ma najniższy priorytet.

Mechanizm ten eliminuje wykorzystywanie zaufanych aplikacji przez niezaufane programy lub te z ograniczonymi uprawnieniami w celu wykonania działań wymagających określonych uprawnień.

Jeśli aktywność aplikacji została zablokowana w wyniku braku uprawnień nadawanych procesom nadrzędnym, możesz zmodyfikować te uprawnienia lub wyłączyć dziedziczenie ograniczeń od procesu nadrzędnego.

W celu wyłączenia dziedziczenia ograniczeń od procesów nadrzędnych:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uprawnień aplikacji**.
   W prawej części okna wyświetlone są ustawienia modułu Kontrola uprawnień aplikacji.
3. Kliknij przycisk **Aplikacje**.
   Zostanie otwarte okno **Kontrola uprawnień aplikacji** na zakładce **Reguły kontroli aplikacji**.
4. Wybierz żądaną aplikację.
5. Z menu kontekstowego aplikacji wybierz **Reguły aplikacji**.
   Zostanie otwarte okno **Reguły kontroli aplikacji**.
6. W oknie **Reguły kontroli aplikacji** wybierz zakładkę **Wykluczenia**.
7. Zaznacz pole **Nie dziedzicz ograniczeń nadrzędnego procesu (aplikacji)**.
8. Kliknij **OK**.
9. W oknie **Aplikacje** kliknij **OK**.
10. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Wykluczanie określonych akcji aplikacji z reguł kontroli aplikacji

W celu wykluczenia określonych akcji aplikacji z reguł kontroli aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uprawnień aplikacji**.
   W prawej części okna wyświetlone są ustawienia modułu Kontrola uprawnień aplikacji.
3. Kliknij przycisk **Aplikacje**.
   Zostanie otwarte okno **Kontrola uprawnień aplikacji** na zakładce **Reguły kontroli aplikacji**.
4. Wybierz żądaną aplikację.
5. Z menu kontekstowego aplikacji wybierz **Reguły aplikacji**.
   Zostanie otwarte okno **Reguły kontroli aplikacji**.
6. Przejdź na zakładkę **Wykluczenia**.
7. Zaznacz pola obok akcji aplikacji, które nie muszą być monitorowane.
8. Kliknij **OK**.
9. W oknie **Aplikacje** kliknij **OK**.
10. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Usuwanie przestarzałych reguł kontroli aplikacji

Domyślnie automatycznie usuwane są reguły kontroli dla aplikacji, które nie były uruchamiane dłużej niż 60 dni. Możesz zmienić czas przechowywania reguł kontroli dla nieużywanych aplikacji lub wyłączyć automatyczne usuwanie tych reguł.

W celu usunięcia przestarzałych reguł kontroli aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uprawnień aplikacji**.
   W prawej części okna wyświetlone są ustawienia modułu Kontrola uprawnień aplikacji.
3. Wykonaj jedną z poniższych czynności:
   - Jeżeli chcesz, aby Kaspersky Endpoint Security usuwał reguły kontroli dla nieużywanych aplikacji, zaznacz pole **Usuń reguły dla aplikacji nieaktywnych dłużej niż** i określ żądaną liczbę dni.
   - Aby wyłączyć automatyczne usuwanie reguł kontroli dla nieużywanych aplikacji, usuń zaznaczenie z pola **Usuń reguły dla aplikacji nieaktywnych dłużej niż**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Ochrona zasobów systemu operacyjnego i danych tożsamości

Moduł Kontrola uprawnień aplikacji zarządza uprawnieniami aplikacji do wykonywania akcji na różnych kategoriach zasobów systemu operacyjnego i danych tożsamości.

Specjaliści z Kaspersky utworzyli listę predefiniowanych kategorii chronionych zasobów. Nie możesz zmieniać ani usuwać predefiniowanych kategorii chronionych zasobów ani chronionych zasobów znajdujących się w tych kategoriach.

Możesz także wykonać następujące akcje:

- Dodać nową kategorię chronionych zasobów.
- Dodać nowy chroniony zasób.
- Wyłączyć ochronę zasobu.

Dodawanie kategorii chronionych zasobów

W celu dodania nowej kategorii chronionych zasobów:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uprawnień aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola uprawnień aplikacji.
3. Kliknij przycisk **Zasoby**.

   Zostanie otwarte okno **Kontrola uprawnień aplikacji** na zakładce **Chronione zasoby**.
4. W lewej części zakładki **Chronione zasoby** wybierz sekcję lub kategorię chronionych zasobów, do której chcesz dodać nową kategorię chronionych zasobów.
5. Kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz **Kategoria**.

   Zostanie otwarte okno **Kategoria chronionych zasobów**.
6. W otwartym oknie **Kategoria chronionych zasobów** wprowadź nazwę nowej kategorii chronionych zasobów.
7. Kliknij **OK**.

   Na liście kategorii chronionych zasobów pojawi się nowy element.
8. Kliknij **OK** w oknie **Kontrola uprawnień aplikacji**.
9. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Po dodaniu kategorii chronionych zasobów, możesz ją zmodyfikować lub usunąć, klikając przyciski **Modyfikuj** lub **Usuń** w lewej górnej części zakładki **Chronione zasoby**.

Dodawanie chronionego zasobu

W celu dodania chronionego zasobu:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uprawnień aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola uprawnień aplikacji.
3. Kliknij przycisk **Zasoby**.

   Zostanie otwarte okno **Kontrola uprawnień aplikacji** na zakładce **Chronione zasoby**.
4. W lewej części zakładki **Chronione zasoby** wybierz kategorię chronionych zasobów, do której chcesz dodać nowy chroniony zasób.
5. Kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz typ zasobu, który chcesz dodać:

   - **Plik lub folder**.
   - **Klucz rejestru**.

   Zostanie otwarte okno **Chroniony zasób**.
6. W oknie **Chroniony zasób** wprowadź nazwę chronionego zasobu w polu **Nazwa**.
7. Kliknij przycisk **Przeglądaj**.
8. W otwartym oknie określ żądane ustawienia w zależności od typu chronionego zasobu, który chcesz dodać, i kliknij **OK**.
9. W oknie **Chroniony zasób** kliknij **OK**.

   Nowy element pojawi się na liście chronionych zasobów wybranej kategorii, na zakładce **Chronione zasoby**.
10. Kliknij **OK** w oknie **Kontrola uprawnień aplikacji**.
11. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Po dodaniu chronionego zasobu możesz go zmodyfikować lub usunąć, klikając przyciski **Modyfikuj** lub **Usuń** w lewej górnej części zakładki **Chronione zasoby**.

Wyłączanie ochrony zasobu

W celu wyłączenia ochrony zasobu:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola uprawnień aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola uprawnień aplikacji.

3. W prawej części okna kliknij przycisk **Zasoby**.

   Zostanie otwarte okno **Kontrola uprawnień aplikacji** na zakładce **Chronione zasoby**.

4. Wykonaj jedną z poniższych czynności:

   - W lewej części zakładki, na liście chronionych zasobów wybierz zasób, dla którego chcesz wyłączyć ochronę i usuń zaznaczenie z pola obok jego nazwy.

   - Kliknij **Wykluczenia** i wykonaj następujące czynności:

     a. W oknie **Wykluczenia** kliknij przycisk **Dodaj**. Z listy rozwijalnej wybierz typ zasobu, który chcesz dodać do listy wykluczeń z ochrony przez moduł Kontrola uprawnień aplikacji: **Plik lub folder** lub **Klucz rejestru**.

     Zostanie otwarte okno **Chroniony zasób**.

     b. W oknie **Chroniony zasób** wprowadź nazwę chronionego zasobu w polu **Nazwa**.

     c. Kliknij przycisk **Przeglądaj**.

     d. W oknie, które zostanie otwarte, określ wymagane ustawienia w zależności od typu chronionego zasobu, który chcesz dodać do listy wykluczeń z ochrony modułu Kontrola uprawnień aplikacji.

     e. Kliknij **OK**.

     f. W oknie **Chroniony zasób** kliknij **OK**.

     Nowy element pojawi się na liście zasobów wykluczonych z ochrony modułu Kontrola uprawnień aplikacji.

     > Po dodaniu zasobu do listy wykluczeń z ochrony modułu Kontrola uprawnień aplikacji, możesz go zmienić lub usunąć, klikając przycisk **Modyfikuj** lub **Usuń** w górnej części okna **Wykluczenia**.

     g. W oknie **Wykluczenia** kliknij **OK**.

5. Kliknij **OK** w oknie **Kontrola uprawnień aplikacji**.

6. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Monitor wykrywania luk

Komponent jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów plików.

Ta sekcja zawiera informacje o Monitorze wykrywania luk oraz instrukcje dotyczące włączania i wyłączania modułu.

Informacje o module Monitor wykrywania luk

Moduł Monitor wykrywania luk wykonuje w czasie rzeczywistym zadanie wykrywania luk w uruchamianych aplikacjach i w aplikacjach już działających na komputerze użytkownika. Jeżeli moduł Monitor wykrywania luk jest włączony, nie musisz uruchamiać zadania Wykrywanie luk. To zadanie jest przydatne wtedy, gdy zadanie Wykrywanie luk nigdy nie zostało uruchomione lub było uruchomione jakiś czas temu.

Włączanie i wyłączanie modułu Monitor wykrywania luk

Domyślnie komponent Monitor wykrywania luk jest wyłączony. W razie konieczności możesz włączyć Monitor wykrywania luk.

Istnieją dwa sposoby włączania i wyłączania komponentu:

- W oknie głównym aplikacji, na zakładce**Ochrona i kontrola**
- Z poziomu okna ustawień aplikacji

W celu włączenia lub wyłączenia modułu Monitor wykrywania luk w oknie głównym aplikacji, na zakładce Ochrona i kontrola:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Kontrola węzła końcowego**.

   Zostanie otwarta sekcja **Kontrola węzła końcowego**.
4. Kliknij prawym przyciskiem myszy wiersz z informacjami o module Monitor wykrywania luk, aby otworzyć menu kontekstowe.

   Zostanie otwarte menu wyboru działań.
5. Wykonaj jedną z poniższych czynności:

   - Aby włączyć Monitor wykrywania luk, wybierz **Włącz**.

     Ikona stanu modułu , wyświetlana w lewej części wiersza **Monitor wykrywania luk**, zmieni się na ikonę .
   - Aby wyłączyć Monitor wykrywania luk, wybierz **Wyłącz**.

     Ikona stanu modułu , wyświetlana w lewej części wiersza **Monitor wykrywania luk**, zmieni się na ikonę .

W celu włączenia lub wyłączenia modułu Monitor wykrywania luk z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz **Monitor wykrywania luk**.

   W prawej części okna wyświetlone są ustawienia modułu Monitor wykrywania luk.
3. W prawej części okna wykonaj jedną z poniższych czynności:

   - Jeżeli chcesz, aby Kaspersky Endpoint Security uruchamiał wykrywanie luk w aplikacjach uruchomionych na komputerze użytkownika lub uruchomionych przez użytkownika, zaznacz pole **Włącz Monitor wykrywania luk**.
   - Jeżeli nie chcesz, aby Kaspersky Endpoint Security uruchamiał wykrywanie luk w aplikacjach uruchomionych na komputerze użytkownika lub uruchomionych przez użytkownika, usuń zaznaczenie z pola **Włącz Monitor wykrywania luk**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Kontrola urządzeń

Komponent jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów plików.

Sekcja ta zawiera informacje o Kontroli urządzeń oraz instrukcje dotyczące konfiguracji ustawień modułu.

Informacje o module Kontrola urządzeń

Kontrola urządzeń zapewnia bezpieczeństwo poufnych danych, ograniczając dostęp użytkownika do urządzeń zainstalowanych na komputerze lub podłączonych do niego, w tym:

- Urządzeń przechowujących dane (dyski twarde, dyski wymienne, napędy taśmowe, płyty CD/DVD)
- Urządzeń przesyłających dane (modemów, zewnętrznych kart sieciowych)
- Urządzeń tworzących kopie danych (drukarki)
- Magistral połączeń (zwanych również "magistralami") odpowiadających interfejsom służącym do podłączania urządzeń do komputera (takich jak USB, FireWire i podczerwień)

Kontrola urządzeń zarządza dostępem użytkownika do urządzeń, stosując *reguły dostępu do urządzeń* (zwane również "regułami dostępu") i *reguły dostępu do magistral połączeń* (zwane również "regułami dostępu do magistral").

Włączanie i wyłączanie modułu Kontrola urządzeń

Domyślnie Kontrola urządzeń jest włączona. W razie konieczności możesz wyłączyć Kontrolę urządzeń.

Istnieją dwa sposoby włączania i wyłączania komponentu:

- W oknie głównym aplikacji, na zakładce**Ochrona i kontrola**
- Z poziomu okna ustawień aplikacji

*W celu włączenia lub wyłączenia modułu Kontrola urządzeń w oknie głównym aplikacji, na zakładce **Ochrona i kontrola**:*

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Kontrola węzła końcowego**.

   Zostanie otwarta sekcja **Kontrola węzła końcowego**.
4. Kliknij prawym przyciskiem myszy wiersz z informacjami o module Kontrola urządzeń.

   Zostanie otwarte menu wyboru działań.

5. Wykonaj jedną z poniższych czynności:

   - Aby włączyć moduł Kontrola urządzeń, wybierz z menu opcję **Włącz**.
   - Aby wyłączyć moduł Kontrola urządzeń, wybierz z menu opcję **Wyłącz**.

W celu włączenia lub wyłączenia modułu Kontrola urządzeń z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola urządzeń**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola urządzeń.
3. Wykonaj jedną z poniższych czynności:

   - Jeżeli chcesz włączyć Kontrolę urządzeń, zaznacz pole **Włącz moduł Kontrola urządzeń**.
   - Jeżeli chcesz wyłączyć Kontrolę urządzeń, usuń zaznaczenie z pola **Włącz moduł Kontrola urządzeń**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Informacje o regułach dostępu do urządzeń i magistral połączeń

Reguła dostępu do urządzenia to kombinacja parametrów, które definiują następujące funkcje modułu Kontrola urządzeń:

- Zezwalanie wybranym użytkownikom i / lub grupie użytkowników na dostęp do określonych typów urządzeń w zdefiniowanych przedziałach czasu.

  Możesz wybrać użytkownika i / lub grupę użytkowników, a także utworzyć dla nich terminarz dostępu do urządzenia.
- Ustawianie prawa do odczytu zawartości pamięci urządzeń.
- Ustawianie prawa do modyfikacji zawartości pamięci urządzeń.

Domyślnie reguły dostępu są tworzone dla wszystkich typów urządzeń znajdujących się w klasyfikacji modułu Kontrola urządzeń. Takie reguły nadają wszystkim użytkownikom pełne prawa dostępu do urządzeń przez cały czas, jeżeli dozwolony jest dostęp do magistral połączeń odpowiednich typów urządzeń.

Reguła dostępu do magistral połączeń blokuje lub zezwala na dostęp do magistral połączeń.

Reguły zezwalające na dostęp do magistral domyślnie są tworzone dla wszystkich magistral połączeń, które znajdują się w klasyfikacji modułu Kontrola urządzeń.

Nie możesz tworzyć i usuwać reguł dostępu do urządzenia lub magistral połączeń, a jedynie je modyfikować.

Informacje o zaufanych urządzeniach

Zaufane urządzenia są urządzeniami, do których użytkownicy, określeni w ustawieniach zaufanego urządzenia, mają przez cały czas pełne prawa dostępu.

Podczas pracy z zaufanymi urządzeniami można:

- Dodawać urządzenia do listy zaufanych urządzeń.
- Zmieniać użytkowników i / lub grupę użytkowników, którzy mają prawa dostępu do zaufanego urządzenia.
- Usuwać urządzenia z listy zaufanych urządzeń.

Jeżeli dodałeś urządzenie do listy zaufanych i utworzyłeś dla tego typu urządzenia regułę dostępu, która blokuje lub zezwala na dostęp, program Kaspersky Endpoint Security będzie decydował, czy nadać prawo dostępu do urządzenia w oparciu o jego obecność na liście zaufanych urządzeń. Obecność na liście zaufanych urządzeń ma wyższy priorytet niż reguła dostępu.

Standardowe decyzje dotyczące dostępu do urządzeń

Kaspersky Endpoint Security podejmuje decyzję dotyczącą zezwolenia na dostęp do urządzenia po podłączeniu urządzenia do komputera przez użytkownika.

Standardowe decyzje dotyczące dostępu do urządzeń

Nr	Początkowe warunki	Zastępcze kroki wykonywane zanim podjęta zostanie decyzja dotycząca dostępu do urządzenia			Decyzja dotycząca dostępu do urządzenia
		Sprawdzanie, czy urządzenie znajduje się na liście zaufanych urządzeń	Testowanie dostępu do urządzenia w oparciu o regułę dostępu	Testowanie dostępu do magistrali w oparciu o regułę dostępu do magistrali	
1	Urządzenie nie znajduje się w klasyfikacji urządzeń modułu Kontrola urządzeń.	Nie znajduje się na liście zaufanych urządzeń.	Brak reguły dostępu.	Nie jest skanowane.	Dostęp dozwolony.
2	Urządzenie jest zaufane.	Znajduje się na liście zaufanych urządzeń.	Nie jest skanowane.	Nie jest skanowane.	Dostęp dozwolony.
3	Dostęp do urządzenia jest dozwolony.	Nie znajduje się na liście zaufanych urządzeń.	Dostęp dozwolony.	Nie jest skanowane.	Dostęp dozwolony.
4	Dostęp do urządzenia zależy od magistrali.	Nie znajduje się na liście zaufanych urządzeń.	Dostęp zależy od magistrali.	Dostęp dozwolony.	Dostęp dozwolony.
5	Dostęp do urządzenia zależy od magistrali.	Nie znajduje się na liście zaufanych urządzeń.	Dostęp zależy od magistrali.	Dostęp zablokowany.	Dostęp zablokowany.
6	Dostęp do	Nie znajduje się na	Dostęp	Brak reguły dostępu	Dostęp

	urządzenia jest dozwolony. Brak reguły dostępu do magistrali.	liście zaufanych urządzeń.	dozwolony.	do magistrali.	dozwolony.
7	Dostęp do urządzenia jest zablokowany.	Nie znajduje się na liście zaufanych urządzeń.	Dostęp zablokowany.	Nie jest skanowane.	Dostęp zablokowany.
8	Brak reguły dostępu do urządzenia lub brak reguły dostępu do magistrali.	Nie znajduje się na liście zaufanych urządzeń.	Brak reguły dostępu.	Brak reguły dostępu do magistrali.	Dostęp dozwolony.
9	Brak reguły dostępu do urządzenia.	Nie znajduje się na liście zaufanych urządzeń.	Brak reguły dostępu.	Dostęp dozwolony.	Dostęp dozwolony.
10	Brak reguły dostępu do urządzenia.	Nie znajduje się na liście zaufanych urządzeń.	Brak reguły dostępu.	Dostęp zablokowany.	Dostęp zablokowany.

Możesz zmodyfikować regułę dostępu do urządzenia po podłączeniu urządzenia. Jeśli urządzenie jest podłączone i reguła dostępu zezwala na dostęp do niego, a później zmienisz regułę dostępu i zablokujesz dostęp, Kaspersky Endpoint Security zablokuje dostęp przy następnym żądaniu operacji na plikach urządzenia (przeglądanie drzewa folderów, odczyt, zapis). 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.

Modyfikowanie reguły dostępu do urządzenia

W zależności od typu urządzenia, możesz modyfikować różne ustawienia dostępu takie jak listę użytkowników otrzymujących dostęp do urządzenia, terminarz dostępu i dozwolony/zablokowany dostęp.

W celu zmodyfikowania reguły dostępu do urządzenia:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola urządzeń**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola urządzeń.
3. W prawej części okna wybierz zakładkę **Rodzaje urządzeń**.

   Zakładka **Rodzaje urządzeń** zawiera reguły dostępu dla wszystkich urządzeń uwzględnionych w klasyfikacji modułu Kontrola urządzeń.
4. Wybierz regułę dostępu, którą chcesz zmienić.
5. Kliknij przycisk **Modyfikuj**. Przycisk jest dostępny jedynie dla typów urządzeń posiadających system plików.

   Zostanie otwarte okno **Konfiguracja reguły dostępu do urządzenia**.

Domyślnie reguła dostępu dla urządzenia nadaje wszystkim użytkownikom pełny dostęp do określonego typu urządzeń w dowolnym momencie. Na liście **Użytkownicy i / lub grupy użytkowników** ta reguła dostępu zawiera grupę **Wszystkie**. W tabeli **Uprawnienia wybranej grupy użytkowników według terminarza dostępu** ta reguła dostępu do urządzeń posiada **Domyślny terminarz** dostępu do urządzeń z uprawnieniami do wykonywania każdego działania na urządzeniach.

6. Zmodyfikuj ustawienia reguły dostępu do urządzenia:

   a. Wybierz użytkownika i / lub grupę użytkowników z listy **Użytkownicy i / lub grupy użytkowników**.

   Aby zmodyfikować listę **Użytkownicy i / lub grupy użytkowników**, użyj przycisków **Dodaj**, **Modyfikuj** i **Usuń**.

   b. W tabeli **Uprawnienia wybranej grupy użytkowników według terminarza dostępu** skonfiguruj terminarz dostępu do urządzeń dla wybranego użytkownika i / lub grupy użytkowników. W tym celu zaznacz pola obok nazw terminarzy dostępu dla urządzeń, których chcesz użyć w modyfikowanej regule dostępu do urządzenia.

   Aby zmodyfikować listę terminarzy dostępu do urządzeń, użyj przycisków **Utwórz**, **Modyfikuj**, **Kopiuj** i **Usuń**, dostępnych w tabeli **Uprawnienia wybranej grupy użytkowników według terminarza dostępu**.

   c. Dla każdego terminarza dostępu do urządzeń używanych w modyfikowanej regule określ działania, które są dozwolone podczas pracy z urządzeniami. W tym celu, w tabeli **Uprawnienia wybranej grupy użytkowników według terminarza dostępu** zaznacz pola w kolumnach z nazwami żądanych działań.

   d. Kliknij **OK**.

   Po zmodyfikowaniu domyślnych ustawień reguły dostępu do urządzenia, ustawienie dostępu do typu urządzenia w kolumnie **Dostęp** w tabeli na zakładce **Rodzaje urządzeń** jest zmieniana na wartość *Ograniczone regułami*.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Dodawanie lub wykluczanie wpisów do/z raportu zdarzeń

Logowanie zdarzeń jest dostępne tylko dla działań na plikach znajdujących się na nośnikach wymiennych.

W celu włączenia lub wyłączenia zapisywania zdarzeń:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola urządzeń**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola urządzeń.

3. W prawej części okna wybierz zakładkę **Rodzaje urządzeń**.

   Zakładka **Rodzaje urządzeń** zawiera reguły dostępu dla wszystkich urządzeń uwzględnionych w klasyfikacji modułu Kontrola urządzeń.

4. W tabeli urządzeń wybierz **Nośniki wymienne**.

   Przycisk **Logowanie** jest dostępny w górnej części tabeli.

5. Kliknij przycisk **Logowanie**.

   Zostanie otwarte okno **Ustawienia logowania**.

6. Wykonaj jedną z poniższych czynności:

- Jeśli chcesz włączyć logowanie działań zapisu i usuwania plików na nośnikach wymiennych, zaznacz pole **Włącz logowanie**.

  Kaspersky Endpoint Security zapisze zdarzenie do pliku raportu i wyśle wiadomość na Serwer administracyjny Kaspersky Security Center za każdym razem, gdy użytkownik wykona działania zapisu lub usunięcia plików na nośnikach wymiennych.

- W innym przypadku usuń zaznaczenie z pola **Włącz logowanie**.

7. Określ, które działania mają być rejestrowane. W tym celu wykonaj jedną z następujących czynności:

   - Jeśli chcesz, żeby Kaspersky Endpoint Security zapisywał wszystkie zdarzenia, zaznacz pole **Zapisz informacje dotyczące wszystkich plików**.

   - Jeśli chcesz, żeby Kaspersky Endpoint Security zapisywał tylko informacje o plikach określonego formatu, w sekcji **Filtr formatów pliku** zaznacz pola obok odpowiednich formatów plików.

8. Określ, które działania użytkowników Kaspersky Endpoint Security mają być rejestrowane jako zdarzenia. W tym celu:

   a. W sekcji **Użytkownicy** kliknij przycisk **Wybierz**.

      Zostanie otwarte standardowe okno **Wybierz Użytkowników lub Grupy** z Microsoft Windows.

   b. Określ lub zmodyfikuj listę użytkowników i / lub grup użytkowników.

   Jeśli użytkownicy określeni w sekcji **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 wiadomość do Serwera administracyjnego Kaspersky Security Center.

9. W oknie **Ustawienia logowania** kliknij **OK**.

10. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

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**.

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. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola urządzeń**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola urządzeń.

3. W prawej części okna wybierz zakładkę **Rodzaje urządzeń**.

   Zakładka **Rodzaje urządzeń** zawiera reguły dostępu dla wszystkich urządzeń uwzględnionych w klasyfikacji modułu Kontrola urządzeń.

4. W kolumnie **Dostęp**, obok urządzenia **Wi-Fi** kliknij prawym klawiszem myszy, aby otworzyć menu kontekstowe.
5. Wybierz opcję **Blokuj z wyjątkami**.
6. Na liście urządzeń wybierz **Wi-Fi** i kliknij **Modyfikuj**.

   Zostanie otwarte okno **Zaufana sieć Wi-Fi**.
7. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Zaufana sieć Wi-Fi**.
8. W oknie **Zaufana sieć Wi-Fi**:

   - W polu **Nazwa sieci** określ nazwę sieci Wi-Fi, którą chcesz dodać do listy zaufanych.
   - Z listy rozwijalnej **Typ autoryzacji** wybierz typ autoryzacji używanej podczas nawiązywania połączenia z zaufaną siecią Wi-Fi.
   - Z listy rozwijalnej **Rodzaj szyfrowania** wybierz rodzaj szyfrowania używanego podczas zabezpieczania ruchu zaufanej sieci Wi-Fi.
   - 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.
9. W oknie **Zaufana sieć Wi-Fi** kliknij **OK**.
10. W oknie **Zaufane sieci Wi-Fi** kliknij **OK**.

Modyfikowanie reguły dostępu do magistrali połączeń

W celu zmodyfikowania reguły dostępu do magistrali połączeń:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola urządzeń**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola urządzeń.
3. Wybierz zakładkę **Magistrale**.

   Zakładka **Magistrale** wyświetla reguły dostępu dla wszystkich magistrali połączeń sklasyfikowanych w module Kontrola urządzeń.
4. Wybierz magistralę połączenia, którą chcesz zmienić.
5. Zmień wartość parametru dostępu.

   - Aby zezwolić na dostęp do magistrali połączenia, kliknij kolumnę **Dostęp**, aby otworzyć menu kontekstowe, z którego wybierz **Zezwól**.
   - Aby zablokować dostęp do magistrali połączenia, kliknij kolumnę **Dostęp**, aby otworzyć menu kontekstowe, z którego wybierz **Zablokuj**.

6. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Działania podejmowane na zaufanych urządzeniach

Sekcja ta zawiera informacje dotyczące działań podejmowanych na zaufanych urządzeniach.

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. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola urządzeń**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola urządzeń.
3. W prawej części okna wybierz zakładkę **Zaufane urządzenia**.
4. Kliknij przycisk **Wybierz**.

   Zostanie otwarte okno **Wybierz zaufane urządzenia**.
5. Zaznacz pole obok nazwy urządzenia, które chcesz dodać do listy zaufanych urządzeń.

   Lista w kolumnie **Urządzenia** zależy od wartości wybranej z listy rozwijalnej **Wyświetl podłączone urządzenia**.
6. Kliknij przycisk **Wybierz**.

   Zostanie otwarte okno **Wybierz Użytkowników lub Grupy** z Microsoft Windows.
7. W oknie **Wybierz Użytkowników lub Grupy** określ użytkowników i / lub grupy użytkowników, dla których Kaspersky Endpoint Security rozpoznaje wybrane urządzenia jako zaufane.

   Nazwy użytkowników i / lub grup użytkowników, określone w oknie **Wybierz użytkowników i / lub grupy użytkowników**, są wyświetlane w polu **Zezwól użytkownikom i / lub grupom użytkowników**.
8. Kliknij **OK** w oknie **Wybierz zaufane urządzenia**.

   W tabeli, na zakładce **Zaufane urządzenia** okna ustawień modułu **Kontrola urządzeń**, pojawi się wiersz wyświetlający parametry dodanego zaufanego urządzenia.
9. Powtórz kroki 4–7 dla każdego urządzenia, które chcesz dodać do listy zaufanych urządzeń dla określonych użytkowników i / lub grup użytkowników.
10. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Dodawanie urządzeń do listy Zaufane na podstawie modelu lub numeru ID urządzenia

Domyślnie podczas dodawania urządzenia do listy zaufanych urządzeń dostęp do niego jest dozwolony dla wszystkich użytkowników (grupa użytkowników Wszyscy).

W celu dodania urządzeń do listy Zaufane na podstawie modelu lub numeru ID urządzenia:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz utworzyć listę zaufanych urządzeń.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola urządzeń**.
7. W prawej części okna wybierz zakładkę **Zaufane urządzenia**.
8. Kliknij przycisk **Dodaj**.

   Zostanie otwarte menu kontekstowe przycisku.
9. W otwartym menu kontekstowym przycisku **Dodaj** wykonaj jedną z następujących czynności:
   - Kliknij przycisk **Urządzenia według ID**, jeśli chcesz wybrać urządzenia ze znanymi unikatowymi numerami ID, które zostaną dodane do listy zaufanych urządzeń.
   - Wybierz element **Urządzenia według modelu**, aby dodać do listy te zaufane urządzenia, których numery VID (ID producenta) i PID (ID produktu) chcesz znać.
10. W otwartym oknie, z listy rozwijalnej **Rodzaj urządzenia** wybierz typ urządzeń, jakie mają być wyświetlane w tabeli poniżej.
11. Kliknij przycisk **Odśwież**.

    Tabela wyświetla listę urządzeń, dla których znane są numery ID i / lub modele oraz które należą do typu wybranego na liście rozwijalnej **Rodzaj urządzenia**.
12. Zaznacz pola obok nazw urządzeń, które chcesz dodać do listy zaufanych urządzeń.
13. Kliknij przycisk **Wybierz**.

    Zostanie otwarte okno **Wybierz Użytkowników lub Grupy** z Microsoft Windows.
14. W oknie **Wybierz Użytkowników lub Grupy** określ użytkowników i / lub grupy użytkowników, dla których Kaspersky Endpoint Security rozpoznaje wybrane urządzenia jako zaufane.

    Nazwy użytkowników i / lub grup użytkowników, określone w oknie **Wybierz użytkowników i / lub grupy użytkowników**, są wyświetlane w polu **Zezwól użytkownikom i / lub grupom użytkowników**.
15. Kliknij **OK**.

    W tabeli, na zakładce **Zaufane urządzenia** pojawią się wiersze z parametrami dodanych zaufanych urządzeń.

16. W celu zapisania zmian kliknij **OK** lub **Zastosuj**.

Dodawanie urządzeń do listy Zaufane w oparciu o maskę numeru ID urządzenia

Domyślnie podczas dodawania urządzenia do listy zaufanych urządzeń dostęp do niego jest dozwolony dla wszystkich użytkowników (grupa użytkowników Wszyscy).

Urządzenia mogą zostać dodane do listy Zaufane w oparciu o maskę ich numeru ID tylko w Konsoli administracyjnej Kaspersky Security Center.

W celu dodania urządzeń do listy Zaufane w oparciu o maskę ich numeru ID:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz utworzyć listę zaufanych urządzeń.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola urządzeń**.
7. W prawej części okna wybierz zakładkę **Zaufane urządzenia**.
8. Kliknij przycisk **Dodaj**.

   Zostanie otwarte menu kontekstowe przycisku.
9. Z menu kontekstowego przycisku **Dodaj** wybierz element **Urządzenia według maski ID**.

   Zostanie otwarte okno **Dodaj zaufane urządzenia według maski ID**.
10. W oknie **Dodaj zaufane urządzenia według maski ID**, w polu **Maska** wprowadź maskę numerów ID urządzenia.
11. Kliknij przycisk **Wybierz**.

    Zostanie otwarte okno **Wybierz Użytkowników lub Grupy** z Microsoft Windows.
12. W oknie **Wybierz Użytkowników lub Grupy** określ użytkowników i / lub grupy użytkowników, dla których Kaspersky Endpoint Security rozpoznaje jako zaufane te urządzenia, których modele lub numery ID odpowiadają określonej masce.

    Nazwy użytkowników i / lub grup użytkowników, określone w oknie **Wybierz użytkowników i / lub grupy użytkowników**, są wyświetlane w polu **Zezwól użytkownikom i / lub grupom użytkowników**.
13. Kliknij **OK**.

W tabeli na zakładce **Zaufane urządzenia** okna ustawień komponentu **Kontrola urządzeń** pojawi się wiersz z ustawieniami reguły dodawania urządzeń do listy zaufanych urządzeń według maski ich numerów.

14. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Konfigurowanie dostępu użytkownika do zaufanego urządzenia

Domyślnie podczas dodawania urządzenia do listy zaufanych urządzeń dostęp do niego jest dozwolony dla wszystkich użytkowników (grupa użytkowników Wszyscy). Możesz skonfigurować dostęp użytkowników (lub grup użytkowników) do zaufanego urządzenia.

W celu skonfigurowania dostępu użytkownika do zaufanego urządzenia:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola urządzeń**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola urządzeń.
3. W prawej części okna wybierz zakładkę **Zaufane urządzenia**.
4. Na liście zaufanych urządzeń wybierz urządzenie, dla którego chcesz zmodyfikować reguły dostępu.
5. Kliknij przycisk **Modyfikuj**.

   Zostanie otwarte okno **Konfiguracja reguły dostępu do zaufanego urządzenia**.
6. Kliknij przycisk **Wybierz**.

   Zostanie otwarte okno **Wybierz Użytkowników lub Grupy** z Microsoft Windows.
7. W oknie **Wybierz Użytkowników lub Grupy** określ użytkowników i / lub grupy użytkowników, dla których Kaspersky Endpoint Security rozpoznaje wybrane urządzenia jako zaufane.
8. Kliknij **OK**.

   Nazwy użytkowników i / lub grup użytkowników, określone w oknie **Wybierz użytkowników i / lub grupy użytkowników**, są wyświetlane w polu **Zezwól użytkownikom i / lub grupom użytkowników** okna **Konfiguracja reguły dostępu do zaufanego urządzenia**.
9. Kliknij **OK**.
10. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Usuwanie urządzenia z listy zaufanych urządzeń

W celu usunięcia urządzenia z listy zaufanych urządzeń:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola urządzeń**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola urządzeń.

3. W prawej części okna wybierz zakładkę **Zaufane urządzenia**.
4. Wybierz urządzenie, które chcesz usunąć z listy zaufanych urządzeń.
5. Kliknij przycisk **Usuń**.
6. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Decyzja o dostępie do urządzenia, które usunąłeś z listy zaufanych, jest podejmowana przez Kaspersky Endpoint Security w oparciu o regułę dostępu do urządzenia i magistral połączeń.

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. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola urządzeń**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola urządzeń.
3. W prawej części okna kliknij przycisk **Szablony**.

   Zostanie otwarte okno **Szablony wiadomości**.
4. Wykonaj jedną z poniższych czynności:
   - Aby zmodyfikować szablon wiadomości dotyczącej zablokowanego dostępu do urządzenia lub niedozwolonej operacji na zawartości urządzenia, wybierz zakładkę **Blokada**.
   - Aby zmodyfikować szablon wiadomości wysyłanej do administratora sieci LAN, wybierz zakładkę **Wiadomość do administratora**.
5. Zmodyfikuj szablon wiadomości. Możesz również skorzystać z następujących przycisków: **Zmienna**, **Domyślny** i **Odnośnik** (ten przycisk jest dostępny tylko na zakładce **Blokada**).
6. Kliknij **OK**.
7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Uzyskiwanie dostępu do zablokowanego urządzenia

Instrukcje te są przeznaczone dla użytkowników komputerów klienckich z zainstalowanym Kaspersky Endpoint Security.

Funkcja z Kaspersky Endpoint Security nadająca tymczasowy dostęp do urządzenia jest dostępna jedynie, gdy Kaspersky Endpoint Security działa w ramach profilu Kaspersky Security Center, a funkcja ta jest włączona w ustawieniach profilu (patrz *Podręcznik administratora Kaspersky Security Center*).

W celu uzyskania dostępu do zablokowanego urządzenia z poziomu okna ustawień modułu Kontrola urządzeń:

1. W oknie głównym aplikacji wybierz zakładkę **Ochrona i kontrola**.
2. Kliknij sekcję **Kontrola węzła końcowego**.

   Zostanie otwarta sekcja **Kontrola węzła końcowego**.
3. Kliknij prawym przyciskiem myszy wiersz z informacjami o module Kontrola urządzeń.

   Zostanie otwarte menu wyboru działań.
4. Kliknij przycisk **Dostęp do urządzenia**.

   Zostanie otwarte okno **Żądanie dostępu do urządzenia**.
5. Z listy podłączonych urządzeń wybierz urządzenie, do którego chcesz uzyskać dostęp.
6. Kliknij przycisk **Uzyskaj plik żądania dostępu**.

   Zostanie otwarte okno **Tworzenie pliku żądania dostępu**.
7. W polu **Czas dostępu** określ przedział czasu, podczas którego chcesz mieć dostęp do urządzenia.
8. Kliknij przycisk **Zapisz**.

   Zostanie otwarte standardowe okno **Zapisz plik żądania dostępu** z Microsoft Windows.
9. W oknie **Zapisz plik żądania dostępu** wybierz folder, w którym chcesz zapisać plik żądania dostępu do urządzenia, i kliknij przycisk **Zapisz**.
10. Wyślij plik żądania dostępu do urządzenia administratorowi sieci LAN.
11. Odbierz plik klucza dostępu do urządzenia od administratora sieci LAN.
12. W oknie **Żądanie dostępu do urządzenia** kliknij przycisk **Aktywuj klucz dostępu**.

    Zostanie otwarte standardowe okno **Otwórz klucz dostępu** z Microsoft Windows.
13. W oknie **Otwórz klucz dostępu** wybierz plik klucza dostępu do urządzenia, który uzyskałeś od administratora sieci LAN, i kliknij **Otwórz**.

    Zostanie otwarte okno **Aktywacja klucza dostępu do urządzenia** wyświetlające informacje o uzyskanym dostępie.
14. Kliknij **OK** w oknie **Aktywacja klucza dostępu do urządzenia**.

W celu uzyskania dostępu do zablokowanego urządzenia poprzez kliknięcie odnośnika w wiadomości informującej o zablokowaniu urządzenia:

1. W oknie z wiadomością informującą o zablokowaniu urządzenia lub magistrali połączenia kliknij odnośnik **Poproś o dostęp**.

Zostanie otwarte okno **Tworzenie pliku żądania dostępu**.

2. W polu **Czas dostępu** określ przedział czasu, podczas którego chcesz mieć dostęp do urządzenia.

3. Kliknij przycisk **Zapisz**.

   Zostanie otwarte standardowe okno **Zapisz plik żądania dostępu** z Microsoft Windows.

4. W oknie **Zapisz plik żądania dostępu** wybierz folder, w którym chcesz zapisać plik żądania dostępu do urządzenia, i kliknij przycisk **Zapisz**.

5. Wyślij plik żądania dostępu do urządzenia administratorowi sieci LAN.

6. Odbierz plik klucza dostępu do urządzenia od administratora sieci LAN.

7. W oknie **Żądanie dostępu do urządzenia** kliknij przycisk **Aktywuj klucz dostępu**.

   Zostanie otwarte standardowe okno **Otwórz klucz dostępu** z Microsoft Windows.

8. W oknie **Otwórz klucz dostępu** wybierz plik klucza dostępu do urządzenia, który uzyskałeś od administratora sieci LAN, i kliknij **Otwórz**.

   Zostanie otwarte okno **Aktywacja klucza dostępu do urządzenia** wyświetlające informacje o uzyskanym dostępie.

9. Kliknij **OK** w oknie **Aktywacja klucza dostępu do urządzenia**.

Przedział czasu, dla którego nadano uprawnienia dostępu do urządzenia, może różnić się od przedziału czasu, o który prosiłeś. Dostęp do urządzenia jest nadawany na czas określony przez administratora sieci lokalnej w trakcie generowania klucza dostępu do urządzenia.

Tworzenie klucza dostępu do zablokowanego urządzenia przy użyciu Kaspersky Security Center

Aby nadać użytkownikowi tymczasowy dostęp do zablokowanego urządzenia, potrzebny jest klucz dostępu do urządzenia. Klucz dostępu możesz utworzyć przy użyciu Kaspersky Security Center.

W celu utworzenia klucza dostępu dla zablokowanego urządzenia:

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 do urządzeń oraz danych w trybie offline**.

   Zostanie otwarte okno **Przydziel dostęp do urządzeń oraz danych w trybie offline**.

6. Wybierz zakładkę **Kontrola urządzeń**.

7. Na zakładce **Kontrola urządzeń** kliknij przycisk **Przeglądaj**.

   Zostanie otwarte standardowe okno **Wybierz plik żądania dostępu** z Microsoft Windows.

8. W oknie **Wybierz plik żądania dostępu** wybierz plik zgłoszenia dostępu, który otrzymałeś od użytkownika, i kliknij przycisk **Otwórz**.

   Kontrola urządzeń wyświetla szczegółowe informacje dotyczące zablokowanego urządzenia, o dostęp do którego prosił użytkownik.

9. Określ wartość ustawienia **Czas dostępu**.

   Ustawienie to definiuje czas, przez jaki użytkownik będzie miał dostęp do zablokowanego urządzenia. Domyślna wartość to wartość określona przez użytkownika podczas tworzenia pliku zgłoszenia dostępu.

10. Określ wartość ustawienia **Okres aktywacji**.

    Ustawienie to definiuje przedział czasu, podczas którego użytkownik może aktywować dostęp do zablokowanego urządzenia przy pomocy klucza dostępu.

11. Kliknij przycisk **Zapisz**.

    Zostanie otwarte standardowe okno **Zapisz klucz dostępu** z Microsoft Windows.

12. Wybierz folder docelowy, w którym chcesz zapisać plik z kluczem dostępu do zablokowanego urządzenia.

13. Kliknij przycisk **Zapisz**.

Kontrola sieci

Komponent jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów plików.

Sekcja ta zawiera informacje o Kontroli sieci oraz instrukcje dotyczące konfiguracji ustawień modułu.

Informacje o module Kontrola sieci

Kontrola sieci umożliwia nadzorowanie akcji użytkownika wykonywanych w obrębie sieci LAN poprzez ograniczanie lub blokowanie dostępu do zasobów sieciowych.

Zasób sieciowy jest pojedynczą stroną internetową lub kilkoma stronami internetowymi, bądź też stroną lub kilkoma stronami posiadającymi wspólną cechę.

Kontrola sieci udostępnia następujące opcje:

- Oszczędzanie ruchu sieciowego.

  Ruch jest kontrolowany poprzez ograniczanie lub blokowanie plików multimedialnych, bądź przez ograniczanie lub blokowanie dostępu do zasobów sieciowych niezwiązanych z obowiązkami użytkowników.

- Ograniczanie dostępu według kategorii zawartości zasobów sieciowych.

  Aby oszczędzić ruch sieciowy i ograniczyć potencjalne straty finansowe związane z niewłaściwym wykorzystaniem czasu pracowników, możesz ograniczyć lub zablokować dostęp do określonych kategorii zasobów sieciowych (na przykład, zablokować dostęp do zasobów internetowych należących do kategorii "Media komunikacji internetowej").

- Scentralizowana kontrola dostępu do zasobów sieciowych.

  Korzystając z Kaspersky Security Center, masz kontrolę nad indywidualnymi i grupowymi ustawieniami dostępu do zasobów sieciowych.

Wszystkie ograniczenia i blokady nałożone na dostęp do zasobów sieciowych są realizowane jako reguły dostępu do zasobów sieciowych.

Włączanie i wyłączanie modułu Kontrola sieci

Domyślnie Kontrola sieci jest włączona. W razie konieczności możesz wyłączyć Kontrolę sieci.

Istnieją dwa sposoby włączania i wyłączania komponentu:

- W oknie głównym aplikacji, na zakładce**Ochrona i kontrola**
- Z poziomu okna ustawień aplikacji

*W celu włączenia lub wyłączenia modułu Kontrola sieci w oknie głównym aplikacji, na zakładce **Ochrona i kontrola**:*

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Kontrola węzła końcowego**.
   Zostanie otwarta sekcja **Kontrola węzła końcowego**.
4. Kliknij prawym przyciskiem myszy wiersz z informacjami o module Kontrola sieci.
   Zostanie otwarte menu wyboru działań.
5. Wykonaj jedną z poniższych czynności:
   - Aby włączyć moduł Kontrola sieci, wybierz z menu opcję **Włącz**.
   - Aby wyłączyć moduł Kontrola sieci, wybierz z menu opcję **Wyłącz**.

W celu włączenia lub wyłączenia modułu Kontrola sieci z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola sieci**.
   W prawej części okna wyświetlone są ustawienia modułu Kontrola sieci.
3. Wykonaj jedną z poniższych czynności:
   - Jeżeli chcesz włączyć Kontrolę sieci, zaznacz pole **Włącz moduł Kontrola sieci**.
   - Jeżeli chcesz wyłączyć Kontrolę sieci, usuń zaznaczenie z pola **Włącz moduł Kontrola sieci**.

   Jeżeli Kontrola sieci jest wyłączona, Kaspersky Endpoint Security nie kontroluje dostępu do zasobów sieciowych.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Kategorie zawartości zasobów sieciowych

Kategorie zawartości zasobów sieciowych (zwane dalej także "kategorie"), znajdujące się poniżej, zostały wybrane tak, aby w pełni odzwierciedlać dane dostępne w zasobach sieciowych, biorąc pod uwagę ich przeznaczenie i tematykę. Kolejność, w jakiej kategorie pojawiają się na liście, nie reprezentuje ich ważności ani częstotliwości występowania w internecie. Nazwy kategorii są prowizoryczne i są używane wyłącznie na stronach internetowych i w produktach firmy Kaspersky. Ich nazwy niekoniecznie muszą odzwierciedlać znaczenie określone przez prawo. Jeden zasób sieciowy może należeć do kilku kategorii jednocześnie.

Treści dla dorosłych

Ta kategoria zawiera następujące typy zasobów sieciowych:

- Zasoby internetowe zawierające zdjęcia oraz materiały wideo obrazujące narządy płciowe, stosunek płciowy lub masturbację ludzi lub stworzeń humanoidalnych.

- Zasoby internetowe o treści (łącznie z dziełami literatury i artystycznymi) zawierającej opisy narządów płciowych ludzi lub stworzeń humanoidalnych, stosunku płciowego lub masturbacji ludzi lub stworzeń humanoidalnych.
- Zasoby internetowe poświęcone dyskusjom na temat aspektów seksualnych w związkach międzyludzkich.

  Pokrywa się z kategorią "Media komunikacji internetowej".

- Zasoby internetowe zawierające materiały erotyczne, dzieła przedstawiające w sposób realistyczny seksualne zachowania ludzi lub dzieła sztuki przeznaczone do wzbudzania podniecenia seksualnego.
- Zasoby internetowe oficjalnych mediów lub społeczności internetowych skierowane do docelowej grupy odbiorców i zawierające specjalne działy i/lub pojedyncze artykuły traktujące o aspektach seksualnych w związkach międzyludzkich.
- Zasoby sieciowe poświęcone perwersjom seksualnym.
- Zasoby internetowe reklamujące i sprzedające przedmioty służące do wzbudzania podniecenia seksualnego i wykorzystywane podczas stosunku płciowego, usługi seksualne i randki, w tym usługi online, takie jak wideo czaty o tematyce erotycznej, seks przez telefon, seks wirtualny.
- Zasoby internetowe z następującą zawartością:
  - Artykuły i blogi poruszające popularne i naukowe tematy dotyczące edukacji seksualnej.
  - Encyklopedie medyczne, zwłaszcza ich sekcje poświęcone rozmnażaniu płciowemu.
  - Zasoby zakładów leczniczych, zwłaszcza ich sekcje dotyczące narządów płciowych.

Oprogramowanie, audio, wideo

Ta kategoria obejmuje następujące podkategorie, które możesz wybrać indywidualnie:

- **Audio i wideo**.

  Ta podkategoria obejmuje zasoby internetowe, z których można pobrać materiały audio i wideo: filmy, nagrania wydarzeń sportowych lub koncertów, piosenki, teledyski, wideoklipy, pliki dźwiękowe lub filmowe z materiałami szkoleniowymi itd.

- **Torrenty**.

  Ta podkategoria obejmuje strony internetowe trackerów torrentowych przeznaczonych do udostępniania plików o nieograniczonej wielkości.

- **Udostępnianie plików**.

  Ta podkategoria obejmuje udostępnianie plików stron internetowych niezależnie od fizycznej lokalizacji udostępnianych plików.

Alkohol, tytoń, narkotyki

Ta kategoria obejmuje strony odnoszące się bezpośrednio lub pośrednio do alkoholu bądź produktów zawierających alkohol, tytoniu, narkotyków, substancji psychotropowych i odurzających.

- Zasoby internetowe reklamujące i sprzedające tego typu substancje oraz przyrządy do ich zażywania.

Pokrywa się z kategorią "Handel elektroniczny".

- Zasoby internetowe z instrukcjami dotyczącymi spożywania lub wytwarzania narkotyków, substancji psychotropowych i/lub substancji odurzających.

Ta kategoria obejmuje zasoby sieciowe dotyczące tematów naukowych i medycznych.

Przemoc

Ta kategoria uwzględnia zasoby internetowe zawierające zdjęcia, filmy, treści obrazujące przemoc fizyczną lub psychiczną stosowaną wobec ludzi i zwierząt.

- Zasoby internetowe przedstawiające lub opisujące sceny egzekucji, tortury lub znęcanie się, a także narzędzia przeznaczone do takich praktyk.

  Pokrywa się z kategorią "Broń, materiały wybuchowe i pirotechniczne".

- Zasoby internetowe pokazujące lub opisujące sceny morderstw, walk, pobić lub gwałtów, a także sceny, w których ludzie, zwierzęta lub stworzenia humanoidalne są molestowane lub poniżane.
- Zasoby internetowe zachęcające do wykonania czynności, które zagrażają życiu i/lub zdrowiu, na przykład samookaleczenia lub samobójstwo.
- Zasoby internetowe zawierające informacje uzasadniające i usprawiedliwiające dopuszczalność przemocy i/lub okrucieństwa lub zachęcające do aktów przemocy wobec ludzi lub zwierząt.
- Zasoby internetowe zawierające rzeczywiste opisy lub obrazy ofiar i okrucieństw wojny, konfliktów zbrojnych i starć zbrojnych, wypadków, katastrof, katastrof naturalnych, kataklizmów społecznych i przemysłowych lub cierpienia ludzkiego.
- Gry przeglądarkowe ze scenami przemocy i okrucieństwa, łącznie z tak zwanymi "strzelankami", "bijatykami", "slasherami" itd.

  Pokrywa się z kategorią "Gry komputerowe".

Broń, materiały wybuchowe i pirotechniczne

Ta kategoria obejmuje zasoby sieciowe zawierające informacje o broniach, materiałach wybuchowych i pirotechnicznych:

- Strony internetowe producentów i sklepów sprzedających broń, materiały wybuchowe i pirotechniczne.

  Pokrywa się z kategorią "Handel elektroniczny".

- Zasoby internetowe poświęcone produkcji lub wykorzystaniu broni, materiałów wybuchowych i pirotechnicznych.

- Zasoby internetowe zawierające materiały analityczne, historyczne, produkcyjne i encyklopedyczne na temat broni, materiałów wybuchowych i pirotechnicznych.

Pojęcie "bronie" oznacza urządzenia, elementy i środki, których przeznaczeniem jest zagrażanie życiu lub zdrowiu ludzi i zwierząt i/lub uszkodzenie sprzętów i budynków.

Wulgaryzmy

Ta kategoria obejmuje zasoby sieciowe, na których zostały wykryte wulgaryzmy.

Pokrywa się z kategorią "Treści dla dorosłych".

Ta kategoria uwzględnia także zasoby internetowe z materiałami lingwistycznymi i filologicznymi, w których wulgaryzmy i nieprzyzwoitości używane są jako temat badań.

Hazard, loterie, zakłady bukmacherskie

Ta kategoria obejmuje zasoby sieciowe, które oferują odpłatne uczestniczenie w grach, nawet jeśli nie jest to warunkiem koniecznym do uzyskania dostępu do strony. Ta kategoria zawiera zasoby sieciowe oferujące:

- Gry hazardowe, w które uczestnicy muszą wnieść wkład pieniężny.

  Pokrywa się z kategorią "Gry komputerowe".

- Zakłady bukmacherskie, w których obstawianie zakładów odbywa się z użyciem pieniędzy.
- Loterie, które wymagają zakupu losów lub numerów.
- Informacje, które mogą wywołać chęć uczestniczenia w grach hazardowych, zakładach bukmacherskich lub loteriach.

Pokrywa się z kategorią "Handel elektroniczny".

Ta kategoria obejmuje gry, które jako oddzielną opcję oferują darmowe uczestnictwo, a także zasoby sieciowe, które aktywnie reklamują zasoby sieciowe podpadające pod tę kategorię.

Komunikacja w sieci

Ta kategoria zawiera zasoby sieciowe, które umożliwiają użytkownikom (zarejestrowanym lub nie) wysyłanie osobistych wiadomości do innych użytkowników odpowiednich zasobów sieciowych lub innych usług online i/lub dodawanie zawartości (dostępnej publicznie lub nie) do odpowiednich zasobów sieciowych o określonej tematyce. Możesz indywidualnie wybrać następujące podkategorie:

- **Czaty i fora**.

Ta podkategoria obejmuje zasoby sieciowe przeznaczone do publicznej dyskusji na różne tematy dzięki specjalnym aplikacjom internetowym jak również zasoby sieciowe przeznaczone do dystrybucji lub obsługi komunikatorów internetowych, które umożliwiają komunikację w czasie rzeczywistym.

- **Blogi**.

  Ta podkategoria obejmuje platformy blogowe, które są stronami internetowymi dostarczającymi płatne lub bezpłatne usługi dla tworzenia i prowadzenia blogów.

- **Sieci społecznościowe**.

  Ta podkategoria obejmuje strony internetowe przeznaczone do tworzenia, wyświetlania i zarządzania kontaktami z innymi osobami, organizacjami i organizacjami rządowymi. Warunkiem korzystania z tej możliwości jest zarejestrowanie konta użytkownika.

- **Portale randkowe**.

  Ta podkategoria obejmuje zasoby internetowe oferujące rodzaj płatnego lub bezpłatnego serwisu społecznościowego.

  Pokrywa się z kategoriami "Treści dla dorosłych" i "Handel elektroniczny".

- **Poczta przez WWW**.

  Ta podkategoria obejmuje strony logowania w usłudze poczty elektronicznej oraz strony skrzynek pocztowych zawierające wiadomości e-mail i powiązane dane (na przykład kontakty osobiste). Ta kategoria nie obejmuje innych stron internetowych dostawców usługi internetowej, którzy także oferują usługi poczty elektronicznej.

Sklepy internetowe, banki i systemy płatności

Ta kategoria uwzględnia zasoby internetowe przeznaczone do przeprowadzania wszelakich bezgotówkowych transakcji online z wykorzystaniem specjalnie zaprojektowanych do tego celu aplikacji internetowych. Możesz indywidualnie wybrać następujące podkategorie:

- **Sklepy i aukcje**.

  Ta podkategoria obejmuje sklepy internetowe i aukcje internetowe sprzedające różne towary, pracę lub usługi pojedynczym osobom i/lub osobom prawnym, łącznie ze stronami internetowymi sklepów, które prowadzą sprzedaż tylko przez internet, oraz profilami internetowymi fizycznych sklepów, które akceptują płatności online.

- **Banki**.

  Ta podkategoria obejmuje specjalistyczne strony internetowe banków z funkcją banku internetowego, a także możliwością dokonywania elektronicznych przelewów między kontami bankowymi, tworzenia lokat bankowych, zmianą waluty, dokonywania płatności za usługi firm trzecich itd.

- **Systemy płatności**.

  Ta podkategoria obejmuje strony internetowe systemów płatności elektronicznych, które zapewniają dostęp do osobistego konta użytkownika.

Jeśli jest to możliwe technicznie, opłaty mogą być dokonywane z użyciem kart płatniczych wszelkiego rodzaju (plastikowych lub wirtualnych, debetowych lub kredytowych, lokalnych lub międzynarodowych) i systemów płatności elektronicznych. Zasoby internetowe mogą być uwzględniane w tej kategorii bez względu na to, czy posiadają takie aspekty techniczne, jak przesyłanie danych poprzez protokół SSL, użycie autoryzacji trzydomenowej 3D Secure itd.

Oferty pracy

Ta kategoria obejmuje zasoby internetowe, które skupiają pracodawców i poszukujących pracy:

- Strony internetowe agencji rekrutujących (agencje pracy i/lub agencje łowców głów).
- Strony internetowe pracodawców z opisami stanowisk, na które jest nabór.
- Niezależne portale z ofertami pracy zamieszczane przez pracodawców i agencje rekrutujące.
- Profesjonalne sieci społecznościowe umożliwiające opublikowanie lub wyszukanie informacji o specjalistach, którzy nie poszukują aktywnie pracy.

> Pokrywa się z kategorią "Media komunikacji internetowej".

Anonimowe systemy dostępu

Ta kategoria obejmuje zasoby internetowe pełniące funkcję pośrednika w pobieraniu zawartości innych zasobów internetowych z użyciem specjalnych aplikacji internetowych, których celem jest:

- Omijanie ograniczeń na dostęp do adresów internetowych lub adresów IP, które zostały nałożone przez administratora sieci LAN;
- Anonimowy dostęp do zasobów internetowych, w tym stron internetowych, które w szczególności odrzucają żądania HTTP z pewnych adresów IP lub ich grup (na przykład adresów IP pogrupowanych według kraju pochodzenia).

Ta kategoria uwzględnia zasoby internetowe przeznaczone do wyżej opisanych celów ("anonimizery"), jak również zasoby internetowe, które mają podobną funkcjonalność techniczną.

Gry komputerowe

Ta kategoria obejmuje zasoby sieciowe poświęcone grom komputerowym różnych gatunków:

- Strony internetowe twórców gier komputerowych.
- Zasoby sieciowe przeznaczone do dyskusji na temat gier komputerowych.

> Pokrywa się z kategorią "Media komunikacji internetowej".

- Zasoby internetowe zapewniające możliwość grania w gry online z innymi uczestnikami lub w pojedynkę po przeprowadzeniu lokalnej instalacji aplikacji lub bez przeprowadzenia takiej instalacji ("gry przeglądarkowe").
- Zasoby internetowe reklamujące, dystrybuujące i obsługujące gry.

> Pokrywa się z kategorią "Handel elektroniczny".

Religie, związki wyznaniowe

Ta kategoria obejmuje zasoby internetowe zawierające materiały dotyczące ruchów, związków i organizacji państwowych reprezentujących ideologie religijne i/lub wyznające jakikolwiek kult.

- Strony oficjalnych organizacji religijnych o rożnym zasięgu, od międzynarodowych religii do lokalnych wspólnot religijnych.
- Strony nieoficjalnych grup i organizacji religijnych, które powstały w przeszłości w wyniku oddzielenia od dominującego związku wyznaniowego lub społeczności.
- Strony internetowe związków wyznaniowych i wspólnot religijnych, które powstały niezależnie od tradycyjnych ruchów religijnych, także jako inicjatywa określonego założyciela.
- Strony internetowe organizacji międzyreligijnych dążące do nawiązania współpracy przedstawicieli różnych religii tradycyjnych.
- Zasoby internetowe zawierające materiały naukowe, historyczne i encyklopedyczne na temat religii.
- Zasoby internetowe zawierające szczegółowe obrazy i opisy okazywania czci i uwielbienia jako części kultów religijnych, łącznie z obrzędami i rytuałami mającymi na celu okazanie czci Bogu, istotom i/lub przedmiotom, które według ich wyznawców posiadają nadnaturalne moce.

Media informacyjne

Ta kategoria obejmuje zasoby zawierające informacje publiczne utworzone przez mass media lub publikacje online, które umożliwiają użytkownikom dodawanie własnych relacji z wydarzeń.

- Strony internetowe oficjalnych mediów.
- Strony internetowe oferujące umieszczanie informacji z przypisaniem oficjalnych źródeł informacji.
- Strony internetowe oferujące zebranie w jednym miejscu wiadomości informacyjnych z różnych oficjalnych i nieoficjalnych źródeł.
- Strony internetowe, na których wiadomości informacyjne są tworzone przez samych użytkowników ("platformy social news").

  Pokrywa się z kategorią "Media komunikacji internetowej".

Banery

Ta kategoria zawiera zasoby sieciowe z banerami. Informacje reklamowe znajdujące się na banerach mogą rozpraszać podczas pracy, a samo pobieranie banerów zwiększa ilość ruchu sieciowego.

Informacje o regułach dostępu do zasobów sieciowych

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 typem danych należących do określonej kategorii. 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", która nadaje wszystkim użytkownikom uprawnienia dostępu do dowolnych zasobów w dowolnym czasie.

Działania podejmowane na regułach dostępu do zasobów sieciowych

Możesz wykonać następujące działania na regułach dostępu do zasobów sieciowych:

- Dodać nową regułę

- Zmodyfikować regułę

- Przypisać priorytet do reguły

  Priorytet reguły jest określany przez pozycję wiersza zawierającego krótki opis tej reguły w tabeli reguł dostępu, w oknie ustawień komponentu Kontrola sieci. Oznacza to, że reguła znajdująca się wyżej w tabeli reguł dostępu posiada wyższy priorytet, niż reguła znajdująca się pod nią.

  Jeżeli zasób sieciowy, do którego użytkownik próbuje uzyskać dostęp, odpowiada parametrom kilku reguł, Kaspersky Endpoint Security wykonuje akcję zgodnie z regułą o najwyższym priorytecie.

- Przetestować regułę.

  Możesz sprawdzić logikę zachowania reguł, korzystając z funkcji Diagnostyka reguł.

- Włączyć i wyłączyć regułę.

Reguła dostępu do zasobu sieciowego może być włączona (stan działania: *Włączona*) lub wyłączona (Stan działania: *Wyłączona*). Domyślnie, po utworzeniu reguła jest włączona (stan działania: *Włączona*). Możesz wyłączyć regułę.

- Usunąć regułę

Dodawanie i modyfikowanie reguły dostępu do zasobu sieciowego

W celu dodania lub zmodyfikowania reguły dostępu do zasobu sieciowego:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola sieci**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola sieci.
3. Wykonaj jedną z poniższych czynności:
   - W celu dodania reguły kliknij przycisk **Dodaj**.
   - Jeżeli chcesz zmodyfikować regułę, wybierz ją w tabeli i kliknij przycisk **Modyfikuj**.

   Zostanie otwarte okno **Reguła dostępu do zasobów sieciowych**.
4. Określ lub zmodyfikuj ustawienia reguły. W tym celu:
   a. W polu **Nazwa** wprowadź lub zmodyfikuj nazwę reguły.
   b. Z listy rozwijalnej **Filtruj zawartość** wybierz żądaną opcję:
      - **Dowolna zawartość**.
      - **Według kategorii zawartości**.
      - **Według typu danych**.
      - **Według kategorii zawartości i typu danych**.
   c. Jeśli jest wybrana inna opcja niż **Dowolna zawartość**, zostaną otwarte sekcje wyboru kategorii zawartości i/lub typów danych. 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.
   d. Z listy rozwijalnej **Zastosuj dla adresów** wybierz żądaną opcję:
      - **Dla wszystkich adresów**.
      - **Dla określonych adresów**.
   e. Jeżeli wybrano opcję **Dla określonych adresów**, otwarta zostanie sekcja, w której można utworzyć listę zasobów sieciowych. Możesz dodać i zmodyfikować adresy zasobów sieciowych, korzystając z przycisków **Dodaj**, **Modyfikuj** i **Usuń**.

f. Zaznacz pole **Określ użytkowników i / lub grupy**.

g. Kliknij przycisk **Wybierz**.

Zostanie otwarte okno **Wybierz Użytkowników lub Grupy** z Microsoft Windows.

h. Określ lub zmodyfikuj listę użytkowników i / lub grupy użytkowników, dla których dostęp do zasobów sieciowych opisanych przez regułę jest dozwolony lub zablokowany.

i. Z listy rozwijalnej **Akcja** wybierz żądaną opcję:

- **Zezwól** Jeśli wybrano tę wartość, Kaspersky Endpoint Security zezwala na dostęp do zasobu sieciowego odpowiadającego ustawieniom reguły.
- **Zablokuj** 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.

j. Z otwartej listy rozwijalnej **Terminarz reguły** wybierz żądany terminarz lub utwórz nowy oparty na wybranym terminarzu reguły. W tym celu:

1. Obok listy rozwijalnej **Terminarz reguły** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Terminarz reguły**.

2. Aby do terminarza reguły dodać przedział czasu, podczas którego reguła nie będzie stosowana, w tabeli wyświetlającej terminarz reguły kliknij komórki tabeli odpowiadające czasowi i dniom tygodnia, które chcesz wybrać.

   Komórka tabeli zmieni kolor na szary.

3. Aby dodać okres, w którym reguła będzie stosowana, i okres, w którym nie będzie stosowana, kliknij szare komórki tabeli odpowiadające czasowi i dniom tygodnia, które chcesz wybrać.

   Komórka tabeli zmieni kolor na zielony.

4. Kliknij przycisk **Zapisz jako**.

   Zostanie otwarte okno **Nazwa terminarza reguły**.

5. Wprowadź nazwę terminarza reguły lub pozostaw sugerowaną nazwę domyślną.

6. Kliknij **OK**.

5. W oknie **Reguła dostępu do zasobów sieciowych** kliknij **OK**.

6. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

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. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola sieci**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola sieci.
3. W prawej części okna wybierz regułę, dla której chcesz zmienić priorytet.
4. Użyj przycisków **W górę** i **W dół** w celu przesunięcia reguły na żądaną pozycję na liście.
5. Powtórz kroki 3–4 dla reguł, których priorytet chcesz zmienić.
6. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

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. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola sieci**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola sieci.
3. W prawej części okna kliknij przycisk **Diagnostyka**.

   Zostanie otwarte okno **Diagnostyka reguł**.
4. Wypełnij pola w sekcji **Warunki**:

   a. 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.

   b. 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.

   c. Jeśli chcesz przetestować reguły wykorzystywane przez Kaspersky Endpoint Security do kontrolowania dostępu do zasobów sieciowych o określonych kategoriach zawartości i / lub kategoriach typu danych, z listy rozwijalnej **Filtruj zawartość** wybierz żądaną opcję (**Według kategorii zawartości**, **Według typu danych** lub **Według kategorii zawartości i typu danych**).

   d. 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.
5. Kliknij przycisk **Sprawdź**.

Po zakończeniu testu wyświetlana jest wiadomość o akcji podjętej przez Kaspersky Endpoint Security, zgodnej z pierwszą regułą wyzwoloną przy próbie dostępu do określonego zasobu sieciowego (akceptuj, zablokuj lub ostrzegaj). 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 **Sprawdź**. Następująca tabela wyświetla pozostałe wyzwolone reguły, określając akcję wykonaną przez Kaspersky Endpoint Security. Reguły uszeregowane są malejąco według priorytetu.

Włączanie i wyłączanie reguły dostępu do zasobu sieciowego

W celu włączenia lub wyłączenia reguły dostępu do zasobu sieciowego:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola sieci**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola sieci.
3. W prawej części okna wybierz regułę, którą chcesz włączyć lub wyłączyć.
4. W kolumnie **Stan** wykonaj następujące czynności:
   - Jeżeli chcesz włączyć regułę, wybierz wartość *Włącz*.
   - Jeżeli chcesz wyłączyć regułę, wybierz wartość *Wyłącz*.
5. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Przenoszenie reguł dostępu do zasobów sieciowych z poprzedniej wersji aplikacji

Jeśli Service Pack 1 Maintenance Release 1 lub poprzednia wersja aplikacji jest aktualizowana do Kaspersky Endpoint Security 10 Service Pack 2 for Windows, 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 internetowa" i "Sieci społecznościowe" zostają przeniesione do kategorii "Media komunikacji internetowej".
- 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 "Handel elektroniczny".
- 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.

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 wyeksportowania listy adresów zasobów sieciowych do pliku:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola sieci**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola sieci.
3. Wybierz regułę, której listę adresów zasobów sieciowych chcesz wyeksportować do pliku.
4. Kliknij przycisk **Modyfikuj**.

   Zostanie otwarte okno **Reguła dostępu do zasobów sieciowych**.
5. Jeżeli nie chcesz eksportować całej listy, ale tylko jej część, wybierz żądane adresy zasobów sieciowych.
6. Kliknij przycisk znajdujący się z prawej strony pola z listą adresów zasobów sieciowych.

   Zostanie otwarte okno potwierdzenia wykonania akcji.
7. Wykonaj jedną z poniższych czynności:

   - Jeżeli chcesz wyeksportować tylko wybrane pozycje z listy adresów zasobów sieciowych, w oknie potwierdzenia wykonania akcji kliknij przycisk **Tak**.
   - Jeżeli chcesz wyeksportować wszystkie pozycje z listy adresów zasobów sieciowych, w oknie potwierdzenia wykonania akcji kliknij przycisk **Nie**.

     Zostanie otwarte standardowe okno **Zapisz jako** z Microsoft Windows.
8. W oknie **Zapisz jako** wybierz plik, do którego chcesz wyeksportować listę adresów zasobów sieciowych. Kliknij przycisk **Zapisz**.

W celu zaimportowania listy adresów zasobów sieciowych z pliku do reguły:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola sieci**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola sieci.
3. Wykonaj jedną z poniższych czynności:

   - Jeżeli chcesz utworzyć nową regułę dostępu do zasobu sieciowego, kliknij przycisk **Dodaj**.
   - Wybierz regułę dostępu do zasobu sieciowego, którą chcesz zmienić. Następnie kliknij przycisk **Modyfikuj**.

   Zostanie otwarte okno **Reguła dostępu do zasobów sieciowych**.

4. Wykonaj jedną z poniższych czynności:

   - Jeżeli tworzysz nową regułę dostępu do zasobu sieciowego, wybierz z listy rozwijalnej **Zastosuj dla adresów** opcję **Dla określonych adresów**.
   - Jeżeli modyfikujesz regułę dostępu do zasobu sieciowego, przejdź do kroku 5 niniejszej instrukcji.

5. Kliknij przycisk znajdujący się z prawej strony pola z listą adresów zasobów sieciowych.

   Jeżeli tworzysz nową regułę, zostanie otwarte standardowe okno **Otwórz plik** z Microsoft Windows.

   Jeżeli modyfikujesz regułę, zostanie otwarte okno żądające potwierdzenia akcji.

6. Wykonaj jedną z poniższych czynności:

   - Jeżeli modyfikujesz nową regułę dostępu do zasobu sieciowego, przejdź do kroku 7 niniejszej instrukcji.
   - Jeżeli modyfikujesz regułę dostępu do zasobu sieciowego, w oknie potwierdzenia wykonania akcji wykonaj jedną z następujących czynności:
     - Jeżeli pozycje importowane z listy adresów zasobów sieciowych mają zostać dodane do już istniejącej listy, kliknij przycisk **Tak**.
     - Jeżeli chcesz usunąć pozycje z listy adresów zasobów sieciowych i dodać te importowane, kliknij przycisk **Nie**.

   Zostanie otwarte okno **Otwórz plik** z Microsoft Windows.

7. W oknie **Otwórz plik** wybierz plik z listą adresów zasobów sieciowych, która ma zostać zaimportowana.

8. Kliknij przycisk **Otwórz**.

9. W oknie **Reguła dostępu do zasobów sieciowych** kliknij **OK**.

Modyfikowanie masek adresów zasobów sieciowych

Korzystanie z *maski adresu zasobu sieciowego* (nazywanej również "maską adresu") może być użyteczne, gdy podczas tworzenia reguły dostępu do zasobu sieciowego wprowadzasz kilka podobnych adresów zasobów sieciowych. Jedna maska adresu może odpowiadać większej liczbie adresów zasobów sieciowych.

Podczas tworzenia maski adresu postępuj zgodnie z następującymi regułami:

1. Symbol `*` zastępuje dowolną sekwencję zawierającą zero lub więcej znaków.

   Na przykład, gdy wprowadzisz maskę adresu *abc*, reguła dostępu będzie stosowana do wszystkich zasobów sieciowych zawierających sekwencję znaków abc. Na przykład: http://www.example.com/page_0-9abcdef.html.

   Aby uwzględnić znak `*` w masce adresu, wprowadź dwa znaki `*`.

2. Sekwencja znaków `www.` na początku maski adresu jest interpretowana jako sekwencja `*.`.

   Przykład: maska adresu www.example.com jest traktowana jako *.example.com.

3. Jeżeli maska adresu nie rozpoczyna się od znaku `*`, wówczas zawartość maski adresu będzie odpowiadała tej samej zawartości z przedrostkiem `*.`.

4. Sekwencja znaków `*.` na początku maski adresu jest interpretowana jako `*.` lub pusty ciąg znaków.

Na przykład: maska adresu http://www.*.example.com odpowiada adresowi http://www2.example.com.

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.

     Na przykład: maska adresu example.com odpowiada adresowi http://example.com i https://example.com.

   - Jeżeli maska adresu zawiera protokół sieciowy, będzie ona odpowiadała tylko adresowi z tym samym protokołem sieciowym.

     Na przykład: maska adresu http://*.example.com odpowiada adresowi http://www.example.com, ale nie adresowi https://www.example.com.

9. Maska adresu podana w podwójnych cudzysłowach jest przetwarzana bez brania pod uwagę dodatkowych zamienników, za wyjątkiem znaku `*`, jeśli został włączony w skład maski adresu. Reguły 5 i 7 nie są stosowane do masek adresów umieszczonych w podwójnym cudzysłowie (przykłady 14 – 18 w tabeli poniżej).

10. Podczas porównywania z maską adresu zasobu sieciowego nie jest brana pod uwagę nazwa użytkownika i hasło, port połączenia oraz wielkość znaków.

Przykłady użycia reguł tworzenia masek adresów

Nr	Maska adresu	Sprawdzany adres zasobu sieciowego	Zastępowanie adresu przez maskę adresu	Komentarz
1	*.example.com	http://www.123example.com	Nie	Patrz reguła 1.
2	*.example.com	http://www.123.example.com	Tak	Patrz reguła 1.
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 2, 1.
7	www.example.com	https://www.example.com	Tak	Patrz reguły 2, 1.
8	http://www.*.example.com	http://123.example.com	Tak	Patrz reguły 2, 4, 1.
9	www.example.com	http://www.example.com/abc	Tak	Patrz reguły 2, 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.

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 wysyłanego do administratora sieci LAN. Możesz zmodyfikować ich zawartość.

W celu zmodyfikowania szablonu dla wiadomości Kontroli sieci:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Kontrola węzła końcowego** wybierz podsekcję **Kontrola sieci**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola sieci.
3. W prawej części okna kliknij przycisk **Szablony**.

   Zostanie otwarte okno **Szablony wiadomości**.
4. Wykonaj jedną z poniższych czynności:

- Jeśli chcesz zmodyfikować szablon wiadomości ostrzegającej użytkownika, że zasób sieciowy może być niepożądany, wybierz zakładkę **Ostrzeżenie**.

- Jeśli chcesz zmodyfikować szablon wiadomości informującej użytkownika o zablokowanym dostępie do zasobu sieciowego, wybierz zakładkę **Blokada**.

- Aby zmodyfikować szablon wiadomości wysyłanej do administratora, wybierz zakładkę **Wiadomość do administratora**.

5. Zmodyfikuj szablon wiadomości. Możesz także skorzystać z listy rozwijalnej **Zmienna**, a także przycisków **Domyślny** i **Odnośnik** (ten przycisk nie jest dostępny na zakładce **Wiadomość do administratora**).

6. Kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

KATA Endpoint Sensor

Ustawienia komponentu KATA Endpoint Sensor są dostępne tylko w Konsoli administracyjnej Kaspersky Security Center. Aby korzystać z tego komponentu, należy zainstalować wtyczkę zarządzającą.

Ta sekcja zawiera informacje o KATA Endpoint Sensor oraz instrukcje dotyczące włączania i wyłączania tego komponentu.

Informacje o KATA Endpoint Sensor

KATA Endpoint Sensor to komponent Kaspersky Anti Targeted Attack Platform. To rozwiązanie jest przeznaczone do szybkiego wykrywania zagrożeń takich jak ataki ukierunkowane.

Ten komponent jest zainstalowany na komputerach klienckich. Na tych komputerach komponent cały czas monitoruje procesy, aktywne połączenia sieciowe oraz pliki, które są modyfikowane, i przesyła te informacje do Kaspersky Anti Targeted Attack Platform.

Funkcjonalność komponentu jest dostępna w następujących systemach operacyjnych:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1.
- Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition.
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition.
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1.
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition.
- Microsoft Windows Server 2016

Dodatkowe informacje o platformie Kaspersky Anti Targeted Attack Platform można znaleźć w systemie pomocy platformy Kaspersky Anti Targeted Attack Platform.

Połączenia przychodzące na komputery z komponentem KATA Endpoint Sensor powinny zostać zaakceptowane bezpośrednio z serwera Kaspersky Anti Targeted Attack Platform, bez użycia serwera proxy.

Włączanie i wyłączanie komponentu KATA Endpoint Sensor

W celu włączenia lub wyłączenia komponentu KATA Endpoint Sensor:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder odpowiedniej grupy administracyjnej, dla której chcesz zmodyfikować ustawienia profilu.

3. W obszarze roboczym wybierz zakładkę **Profile**.

4. Wybierz interesujący Cię profil.

5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:

   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.

6. W sekcji **Ustawienia zaawansowane** wybierz podsekcję **KATA Endpoint Sensor**.

7. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz włączyć KATA Endpoint Sensor, zaznacz pole **KATA Endpoint Sensor**.
   - Jeśli chcesz wyłączyć KATA Endpoint Sensor, odznacz pole **KATA Endpoint Sensor**.

8. Jeśli w poprzednim kroku zaznaczyłeś opcję **KATA Endpoint Sensor**, w polu **Adres serwera** określ adres serwera Kaspersky Anti Targeted Attack Platform zawierający następujące elementy:

   a. Nazwa protokołu

   b. Adres IP lub w pełni kwalifikowana nazwa domeny (FQDN) serwera

   c. Ścieżka do Kolektora zdarzeń systemu Windows na serwerze

9. Kliknij **OK**.

10. Zastosuj profil.

    Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

Szyfrowanie danych

Jeśli program Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla stacji roboczych, funkcja szyfrowania danych jest w pełni dostępna. Jeśli program Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów plików, dostępne jest tylko szyfrowanie dysków twardych przy użyciu technologii Szyfrowanie dysków funkcją BitLocker.

Ta sekcja zawiera informacje o szyfrowaniu i deszyfrowaniu dysków twardych, nośników wymiennych oraz plików i folderów na lokalnych dyskach komputera i zawiera instrukcje dotyczące sposobu konfiguracji i przeprowadzania szyfrowania i deszyfrowania danych z użyciem Kaspersky Endpoint Security oraz wtyczki zarządzającej Kaspersky Endpoint Security.

Jeśli nie ma dostępu do zaszyfrowanych danych, zapoznaj się ze specjalnymi instrukcjami opisującymi sposób pracy z zaszyfrowanymi danymi (Praca z zaszyfrowanymi plikami w przypadku ograniczonej funkcjonalności szyfrowania plików, Praca z zaszyfrowanymi urządzeniami, gdy nie ma dostępu do nich).

Włączanie wyświetlania ustawień szyfrowania w profilu Kaspersky Security Center

W celu włączenia wyświetlania ustawień szyfrowania w profilu Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. Z menu kontekstowego węzła **Serwer administracyjny – <Nazwa komputera>** wybierz **Widok → Ustawienia interfejsu**.

   Zostanie otwarte okno **Ustawienia interfejsu**.
3. W oknie **Ustawienia interfejsu** zaznacz pole **Pokaż ochronę danych i szyfrowania**.
4. Kliknij **OK**.

Informacje o szyfrowaniu danych

Kaspersky Endpoint Security umożliwia szyfrowanie plików i folderów przechowywanych na dyskach lokalnych i nośnikach wymiennych lub wszystkich nośnikach wymiennych i dyskach twardych. Szyfrowanie danych minimalizuje ryzyko wycieku informacji, co może mieć miejsce, gdy komputer przenośny, nośnik wymienny lub dysk twardy zostanie zgubiony bądź skradziony lub gdy dostęp do danych jest uzyskiwany przez nieautoryzowanych użytkowników lub aplikacje.

Jeśli licencja wygasła, aplikacja nie szyfruje nowych danych, a stare zaszyfrowane dane pozostają zaszyfrowane i nie można ich używać. W tej sytuacji szyfrowanie nowych danych wymaga aktywacji programu z nową licencją zezwalającą na korzystanie z szyfrowania.

Jeśli licencja utraciła ważność, postanowienia Umowy licencyjnej zostały naruszone lub klucz, 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 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 profilu Kaspersky Security Center, 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.

  Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

- **Szyfrowanie nośników 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.

  Aplikacja wykonuje akcję określoną w regule szyfrowania po zastosowaniu profilu Kaspersky Security Center.

- **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 archiwów**. 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 dysków twardych**. 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 dysków twardych oraz utworzyć listę dysków twardych wykluczonych z szyfrowania. Po zastosowaniu profilu Kaspersky Security Center, program Kaspersky Endpoint Security szyfruje dyski twarde sektor po sektorze. Aplikacja szyfruje wszystkie logiczne partycje dysków twardych jednocześnie. Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

  Po zaszyfrowaniu dysków twardych, przy kolejnym uruchomieniu komputera użytkownik musi przejść proces autoryzacji przy użyciu Agenta autoryzacji przed uzyskaniem dostępu do dysków twardych i załadowaniem systemu operacyjnego. Wymaga to wprowadzenia hasła do tokena lub karty inteligentnej podłączonej do komputera, bądź wpisania nazwy użytkownika i hasła konta Agenta autoryzacji utworzonego przez administratora lokalnej sieci firmowej przy użyciu zadań zarządzania kontem Agenta autoryzacji. Konta te są oparte na kontach systemu Microsoft Windows, z poziomu których użytkownik loguje się do systemu operacyjnego. Można zarządzać kontami Agenta autoryzacji i używać technologii Single Sign-On (SSO), która umożliwia automatyczne zalogowanie się do systemu operacyjnego, używając nazwy użytkownika i hasła konta Agenta autoryzacji.

  > Jeśli utworzysz kopie zapasowe danych komputera, a następnie zaszyfrujesz dane komputera, po czym przywrócisz kopie zapasowe danych komputera i ponownie zaszyfrujesz dane komputera, Kaspersky Endpoint Security utworzy kopie kont Agenta autoryzacji. Aby usunąć kopie kont, użyj narzędzia klmover z parametrem `dupfix`. Narzędzie klmover jest dostępne z programem Kaspersky Security Center. Więcej na temat działania tego narzędzia można znaleźć w *Podręczniku administratora dla Kaspersky Security Center*.

  > Podczas aktualizacji z poprzedniej wersji aplikacji do Kaspersky Endpoint Security 10 Service Pack 2 for Windows nie jest zapisywana lista kont Agenta autoryzacji.

  Dostęp do zaszyfrowanych dysków twardych jest możliwy tylko z poziomu komputerów, na których zainstalowany jest program Kaspersky Endpoint Security z funkcją szyfrowania dysków twardych. 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, jak tylko nowe pliki zostaną zapisane na nowym urządzeniu podczas uruchamiania regularnego szyfrowania z użyciem funkcji **Zaszyfruj tylko używaną przestrzeń dyskową**, po pewnym czasie wszystkie sektory zostaną zaszyfrowane.

Dane potrzebne do odszyfrowania plików są udostępniane przez Serwer administracyjny Kaspersky Security Center, który kontrolował komputer w momencie szyfrowania. Jeśli z jakiegoś powodu komputer z zaszyfrowanymi plikami będzie pod kontrolą innego Serwera administracyjnego oraz nie podjęto żadnej próby otwarcia zaszyfrowanych plików, dostęp do tych plików będzie można uzyskać na jeden z następujących sposobów:

- Poprzez wysłanie prośby do administratora sieci LAN o dostęp do zaszyfrowanych obiektów;
- Przywracając dane na zaszyfrowanych urządzeniach przy użyciu Narzędzia przywracania;
- Przywracając z kopii zapasowej konfigurację Serwera administracyjnego Kaspersky Security Center kontrolującego komputer w momencie szyfrowania i używając tej konfiguracji na Serwerze administracyjnym obecnie kontrolującym komputer z zaszyfrowanymi obiektami.

Podczas szyfrowania aplikacja tworzy pliki usługi. Do ich przechowywania potrzeba około 2-3% 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.

Kompatybilność funkcji szyfrowania Kaspersky Endpoint Security z Kaspersky Anti-Virus dla UEFI nie jest obsługiwana. Szyfrowanie dysków twardych komputerów, na których zainstalowany jest Kaspersky Anti-Virus dla platformy UEFI, powoduje problemy z działaniem Kaspersky Anti-Virus dla UEFI.

Ograniczenia funkcji szyfrowania

Tworzenie nowych partycji na zaszyfrowanych dyskach twardych, a także formatowanie istniejących partycji zaszyfrowanych dysków twardych może spowodować utratę danych na tych dyskach.

Szyfrowanie dysku twardego przy użyciu technologii Kaspersky Disk Encryption jest niedostępne dla dysków twardych, które nie spełniają wymagań sprzętowych i programowych.

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.
- Intel® Rapid Start Technology i dyski, które posiadają partycję hibernacji nawet wtedy, gdy Intel® Rapid Start Technology jest wyłączony.

- Dyski w formacie MBR z więcej niż czterema partycjami rozszerzonymi.
- 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 2% wolnej niepofragmentowanej przestrzeni.
- Dyski posiadające sektor o rozmiarze innym niż 512 bajtów lub 4096 bajtów, który emuluje 512 bajtów.
- Dyski hybrydowe.

Zmienianie algorytmu szyfrowania

Algorytm szyfrowania używany przez Kaspersky Endpoint Security do szyfrowania danych zależy od bibliotek szyfrowania zawartych w pakiecie dystrybucyjnym.

W celu zmiany algorytmu szyfrowania:

1. Przed zmianą algorytmu szyfrowania odszyfruj obiekty, które Kaspersky Endpoint Security zaszyfrował.

   Po zmianie algorytmu szyfrowania, obiekty, które zostały wcześniej zaszyfrowane, staną się niedostępne.

2. Usuń Kaspersky Endpoint Security.
3. Zainstaluj Kaspersky Endpoint Security z pakietu dystrybucyjnego zawierającego biblioteki szyfrowania dla innej liczby bitów.

Włączanie technologii Single Sign-On (SSO)

Technologia Single Sign-On (SSO) jest niekompatybilna z innymi dostawcami danych uwierzytelniających kont.

W celu włączenia technologii Single Sign-On (SSO):

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz włączyć technologię Single Sign-On (SSO).
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:

- Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
- Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.

6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Ogólne ustawienia szyfrowania**.
7. W podsekcji **Ogólne ustawienia szyfrowania**, w sekcji **Ustawienia hasła** kliknij przycisk **Konfiguruj**.

   Zostanie otwarta zakładka **Agent autoryzacji** okna **Ustawienia hasła szyfrowania**.
8. Zaznacz pole **Użyj technologii Single Sign-On (SSO)**.
9. Kliknij **OK**.
10. Aby zapisać zmiany, w oknie **Właściwości: <Nazwa profilu>** kliknij **OK**.
11. Zastosuj profil.

    Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

Uwagi dotyczące szyfrowania plików

Podczas korzystania z funkcji szyfrowania plików należy pamiętać, że:

- Profil Kaspersky Security Center z predefiniowanymi ustawieniami szyfrowania dysku wymiennego zostanie utworzony dla określonej grupy zarządzanych komputerów. Z tego powodu, rezultat zastosowania profilu szyfrowania / deszyfrowania danych na dyskach wymiennych zależy od komputera, do którego podłączony został dysk wymienny.
- Kaspersky Endpoint Security nie szyfruje / deszyfruje plików ze stanem "tylko do odczytu", które są przechowywane na nośnikach wymiennych.
- 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 wstępnie określonych folderach profili użytkownika mobilnego, obowiązkowych profili użytkownika, tymczasowych profili użytkownika oraz folderach przekierowanych. Lista standardowych folderów, które specjaliści z Kaspersky zalecają zaszyfrować, obejmuje następujące foldery:
  - Moje Dokumenty.
  - Ulubione.
  - Cookies.
  - Pulpit.
  - Pliki tymczasowe programu Internet Explorer
  - Folder plików tymczasowych.
  - Pliki programu Outlook.
- Kaspersky Endpoint Security nie szyfruje pewnych plików i folderów, gdyż może to doprowadzić do uszkodzenia systemu operacyjnego i zainstalowanych na nim aplikacji. Na przykład, na liście wykluczeń szyfrowania znajdują

się następujące pliki i foldery ze wszystkimi osadzonymi folderami:

- %WINDIR%.
- %PROGRAMFILES%, %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 zadania szyfrowania plików i folderów.

- Następujące rodzaje urządzeń są obsługiwane jako nośniki wymienne:
  - Nośniki danych podłączane poprzez magistralę USB
  - Dyski twarde podłączane poprzez magistrale USB i FireWire
  - Dyski SSD podłączane poprzez magistrale USB i FireWire

Szyfrowanie plików na lokalnych dyskach komputera

Szyfrowanie plików na lokalnych dyskach komputera jest dostępne, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla stacji roboczych. Szyfrowanie plików na lokalnych dyskach komputera jest niedostępne, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów plików.

Ta sekcja opisuje szyfrowanie plików na lokalnych dyskach komputera i zawiera instrukcje dotyczące sposobu konfiguracji i przeprowadzania szyfrowania plików na lokalnych dyskach komputera z zainstalowanym programem Kaspersky Endpoint Security oraz Wtyczką konsoli Kaspersky Endpoint Security.

Szyfrowanie plików na lokalnych dyskach komputera

W celu zaszyfrowania plików na dyskach lokalnych:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz skonfigurować szyfrowanie plików na dyskach lokalnych.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.

6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie plików i folderów**.

7. W prawej części okna wybierz zakładkę **Szyfrowanie**.

8. Z listy rozwijalnej **Tryb szyfrowania** wybierz element **Domyślne reguły**.

9. 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.

   Zostanie otwarte okno **Wybierz wstępnie określone foldery**.

   b. Wybierz element **Folder niestandardowy**, aby dodać ręcznie wprowadzoną ścieżkę folderu do reguły szyfrowania.

   Zostanie otwarte okno **Dodaj folder niestandardowy**.

   c. Wybierz element **Pliki według rozszerzenia**, aby dodać rozszerzenia plików do reguły szyfrowania. Kaspersky Endpoint Security zaszyfruje pliki z określonymi rozszerzeniami na wszystkich lokalnych dyskach komputera.

   Zostanie otwarte okno **Dodaj / modyfikuj listę rozszerzeń plików**.

   d. Wybierz element **Pliki według grup(y) rozszerzeń**, aby dodać grupy rozszerzeń plików do reguły szyfrowania. Kaspersky Endpoint Security szyfruje pliki, które mają rozszerzenia znajdujące się na liście grup rozszerzeń na wszystkich lokalnych dyskach komputera.

   Zostanie otwarte okno **Wybierz grupy rozszerzeń plików**.

10. Aby zapisać zmiany, w oknie **Właściwości: <Nazwa profilu>** kliknij **OK**.

11. Zastosuj profil.

    Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

Natychmiast po zastosowaniu profilu program Kaspersky Endpoint Security szyfruje te pliki, które znajdują się w regule szyfrowania, a nie znajdują się w regule deszyfrowania.

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.

Kaspersky Endpoint Security zaszyfruje niezaszyfrowane pliki, jeśli ich właściwości (ścieżka pliku / nazwa pliku / rozszerzenie pliku) wciąż spełniają kryteria reguły szyfrowania po modyfikacji.

Kaspersky Endpoint Security odracza szyfrowanie otwartych plików, aż do ich zamknięcia.

Jeśli użytkownik tworzy nowy pik, którego właściwości spełniają kryteria reguły szyfrowania, Kaspersky Endpoint Security szyfruje plik, gdy tylko zostanie on otwarty.

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.

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 drzewie Konsoli administracyjnej, w folderze **Zarządzane urządzenia** otwórz folder z nazwą odpowiedniej grupy administracyjnej, dla której chcesz skonfigurować reguły dostępu do zaszyfrowanego pliku dla aplikacji.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie plików i folderów**.
7. Z listy rozwijalnej **Tryb szyfrowania** wybierz element **Domyślne reguły**.

   Reguły dostępu są stosowane tylko w trybie **Domyślne reguły**. Po zastosowaniu reguł dostępu w trybie **Domyślne reguły**, jeśli zmienisz na tryb **Pozostaw niezmienione**, Kaspersky Endpoint Security będzie ignorował 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**.

   Zostanie otwarte okno **Dodaj aplikacje z listy Kaspersky Security Center**.

   Wykonaj następujące czynności:

   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, dla których chcesz utworzyć reguły dostępu do zaszyfrowanych plików.

   d. Z listy rozwijalnej **Reguły dla aplikacji** wybierz regułę, która będzie determinować dostęp aplikacji do zaszyfrowanych plików.

   e. 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.

   f. Kliknij **OK**.

   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**.

    Zostanie otwarte okno **Dodaj / modyfikuj nazwy plików wykonywalnych aplikacji**.

Wykonaj następujące czynności:

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 **Reguły dla aplikacji** wybierz regułę, która będzie determinować dostęp aplikacji do zaszyfrowanych plików.

d. Kliknij **OK**.

Szczegółowe informacje o regule dostępu do zaszyfrowanego pliku dla aplikacji pojawią się w tabeli, na zakładce **Reguły dla aplikacji**.

11. W celu zapisania zmian kliknij **OK**.

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** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz skonfigurować szyfrowanie plików utworzonych przez określone aplikacje.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie plików i folderów**.
7. Z listy rozwijalnej **Tryb szyfrowania** wybierz element **Domyślne reguły**.

Reguły szyfrowania są stosowane tylko w trybie **Domyślne reguły**. Po zastosowaniu reguł szyfrowania w trybie **Domyślne reguły**, jeśli zmienisz na tryb **Pozostaw niezmienione**, 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**.

   Zostanie otwarte okno **Dodaj aplikacje z listy Kaspersky Security Center**.

   Wykonaj następujące czynności:

   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 **Aplikacja** zaznacz pola obok aplikacji, których utworzone pliki mają być zaszyfrowane.

   d. Z listy rozwijalnej **Reguły 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.

   f. Kliknij **OK**.

   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**.

    Zostanie otwarte okno **Dodaj / modyfikuj nazwy plików wykonywalnych aplikacji**.

    Wykonaj następujące czynności:

    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 **Reguły dla aplikacji** wybierz **Zaszyfruj wszystkie utworzone pliki**.

    d. Kliknij **OK**.

    Informacje o regule szyfrowania dla plików utworzonych lub zmodyfikowanych przez wybrane aplikacje pojawią się w tabeli na zakładce **Reguły dla aplikacji**.

11. W celu zapisania zmian kliknij **OK**.

Tworzenie reguły deszyfrowania

W celu wygenerowania reguły deszyfrowania:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej, w folderze **Zarządzane urządzenia** otwórz folder z nazwą grupy administracyjnej, dla której chcesz wygenerować listę plików przeznaczonych do odszyfrowania.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie plików i folderów**.
7. W prawej części okna wybierz zakładkę **Deszyfrowanie**.
8. Z listy rozwijalnej **Tryb szyfrowania** wybierz element **Domyślne reguły**.
9. Na zakładce **Deszyfrowanie** 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.

      Zostanie otwarte okno **Wybierz wstępnie określone foldery**.

   b. Wybierz element **Folder niestandardowy**, aby dodać ręcznie wprowadzoną ścieżkę folderu do reguły deszyfrowania.

      Zostanie otwarte okno **Dodaj folder niestandardowy**.

   c. Wybierz element **Pliki według rozszerzenia**, aby dodać rozszerzenia plików do reguły deszyfrowania. Kaspersky Endpoint Security nie szyfruje plików z określonymi rozszerzeniami na wszystkich lokalnych dyskach komputera.

      Zostanie otwarte okno **Dodaj / modyfikuj listę rozszerzeń plików**.

   d. Wybierz element **Pliki według grup(y) rozszerzeń**, aby dodać grupy rozszerzeń plików do reguły deszyfrowania. Kaspersky Endpoint Security nie szyfruje plików, które mają rozszerzenia znajdujące się na liście grup rozszerzeń na wszystkich lokalnych dyskach komputera.

      Zostanie otwarte okno **Wybierz grupy rozszerzeń plików**.

10. Aby zapisać zmiany, w oknie **Właściwości: <Nazwa profilu>** kliknij **OK**.
11. Zastosuj profil.

    Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

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** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz skonfigurować deszyfrowanie plików na dyskach lokalnych.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie plików i folderów**.
7. W prawej części okna wybierz zakładkę **Szyfrowanie**.
8. 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.
9. Utwórz listę deszyfrowanych plików.
10. Aby zapisać zmiany, w oknie **Właściwości: <Nazwa profilu>** kliknij **OK**.
11. Zastosuj profil.

Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

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

Podczas tworzenia zaszyfrowanego pakietu Kaspersky Endpoint Security nie przeprowadza kompresji plików.

W celu utworzenia zaszyfrowanego pakietu:

1. Na komputerze z zainstalowanym programem Kaspersky Endpoint Security i włączoną funkcją szyfrowania użyj dowolnego menedżera plików, aby wybrać pliki i/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 **Dodaj do pakietu zaszyfrowanego**.

   Zostanie otwarte standardowe okno **Określ ścieżkę do zapisu zaszyfrowanego pakietu** w Microsoft Windows.

3. W standardowym oknie **Określ ścieżkę do zapisu zaszyfrowanego pakietu** w Microsoft Windows wybierz miejsce zapisu szyfrowanego pakietu na dysku wymiennym. Kliknij przycisk **Zapisz**.

   Zostanie otwarte okno **Dodaj do pakietu zaszyfrowanego**.

4. W oknie **Dodaj do pakietu zaszyfrowanego** wprowadź i potwierdź hasło.

5. Kliknij przycisk **Utwórz**.

   Zostanie uruchomiony proces tworzenia zaszyfrowanego pakietu. Po zakończeniu procesu, w wybranym folderze docelowym na nośniku wymiennym zostanie utworzony samorozpakowujący się, chroniony hasłem zaszyfrowany pakiet.

Jeśli anulujesz tworzenie zaszyfrowanego pakietu, Kaspersky Endpoint Security wykona następujące działania:

1. Zakończy procesy kopiowania plików do pakietu oraz zakończy wszystkie trwające operacje mające na celu zaszyfrowanie pakietu.

2. Usunie wszystkie pliki tymczasowe, które zostały utworzone w procesie tworzenia i szyfrowania pakietu, a także sam plik szyfrowanego pakietu.

3. Powiadomi użytkownika o wymuszonym zakończeniu procesu tworzenia szyfrowanego pakietu.

Rozpakowywanie zaszyfrowanych pakietów

W celu rozpakowania zaszyfrowanego pakietu:

1. Wybierz zaszyfrowany pakiet w dowolnym menedżerze plików. Kliknij go w celu uruchomienia Kreatora rozpakowywania.

   Zostanie otwarte okno **Wprowadź hasło**.

2. Wprowadź hasło chroniące zaszyfrowany pakiet.

3. W oknie **Wprowadź hasło** kliknij **OK**.

   Jeśli hasło zostało wpisane poprawnie, zostanie otwarte standardowe okno dialogowe **Przeglądaj** systemu Microsoft Windows.

4. W oknie dialogowym **Przeglądaj** systemu Microsoft Windows wybierz folder docelowy dla rozpakowywania zaszyfrowanego pakietu i kliknij **OK**.

   Proces rozpakowywania zaszyfrowanego pakietu do folderu docelowego zostanie rozpoczęty.

Jeśli zaszyfrowany pakiet został wcześniej wypakowany do określonego folderu docelowego, istniejące w folderze pliki zostaną nadpisane plikami z zaszyfrowanego pakietu.

Jeśli anulujesz rozpakowywanie zaszyfrowanego pakietu, Kaspersky Endpoint Security wykona następujące działania:

1. Zatrzyma proces deszyfrowania pakietu i zakończy wszystkie operacje kopiowania plików z zaszyfrowanego archiwum, jeśli takie operacje trwają.

2. Usunie wszystkie pliki tymczasowe utworzone w trakcie deszyfrowania i rozpakowywania zaszyfrowanego pakietu, oraz pliki, które zostały już skopiowane z zaszyfrowanego pakietu do folderu docelowego.

3. Powiadomi użytkownika o wymuszonym zakończeniu procesu wypakowywania szyfrowanego pakietu.

Szyfrowanie nośników wymiennych

Szyfrowanie nośników wymiennych jest dostępne, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla stacji roboczych. Szyfrowanie nośników wymiennych nie jest dostępne, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów plików.

Ta sekcja zawiera informacje o szyfrowaniu nośników wymiennych oraz instrukcje dotyczące konfiguracji i przeprowadzania szyfrowania dysków przy użyciu Kaspersky Endpoint Security i wtyczki zarządzającej Kaspersky Endpoint Security.

Uruchamianie szyfrowania nośników wymiennych

W celu zaszyfrowania dysków wymiennych:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz skonfigurować szyfrowanie nośników wymiennych.

3. W obszarze roboczym wybierz zakładkę **Profile**.

4. Wybierz interesujący Cię profil.

5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:

   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.

   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.

6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie nośników wymiennych**.

7. Z listy rozwijalnej **Tryb szyfrowania** wybierz domyślne działanie wykonywane przez Kaspersky Endpoint Security na wszystkich dyskach wymiennych podłączonych do komputerów w wybranej grupie administracyjnej:

   - **Zaszyfruj cały nośnik wymienny**. Jeśli wybrano tę opcję, podczas stosowania profilu Kaspersky Security Center z określonymi ustawieniami szyfrowania dla dysków wymiennych, Kaspersky Endpoint Security szyfruje zawartość dysków wymiennych sektor po sektorze. W wyniku tego, aplikacja szyfruje nie tylko pliki przechowywane na dyskach wymiennych, ale także systemy plików dysków wymiennych, włączając w to nazwy plików i struktury folderów. Kaspersky Endpoint Security nie szyfruje ponownie nośników wymiennych, które zostały już zaszyfrowane.

     Ten scenariusz szyfrowania jest możliwy dzięki funkcji szyfrowania dysków twardych, dostępnej w Kaspersky Endpoint Security.

   - **Zaszyfruj wszystkie pliki**. Jeśli wybrano tę opcję, podczas stosowania profilu Kaspersky Security Center z określonymi ustawieniami szyfrowania dla dysków wymiennych, Kaspersky Endpoint Security szyfruje wszystkie pliki przechowywane na nośnikach wymiennych. Kaspersky Endpoint Security nie szyfruje ponownie już zaszyfrowanych plików. Aplikacja nie skanuje systemów plików dysków wymiennych, łącznie z nazwami zaszyfrowanych plików i strukturami folderów.

   - **Zaszyfruj tylko nowe pliki**. Jeśli wybrano tę opcję, podczas stosowania profilu Kaspersky Security Center z określonymi ustawieniami szyfrowania dla dysków wymiennych, Kaspersky Endpoint Security szyfruje tylko te pliki, które zostały dodane do dysków wymiennych lub były przechowywane na dyskach wymiennych i zostały zmodyfikowane po ostatnim zastosowaniu profilu Kaspersky Security Center.

   - **Odszyfruj cały nośnik wymienny**. Jeśli wybrano tę opcję, podczas stosowania profilu Kaspersky Security Center 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.

     Scenariusz szyfrowania jest możliwy dzięki funkcji szyfrowania plików oraz funkcji szyfrowania dysków twardych, które są dostępne w Kaspersky Endpoint Security.

   - **Pozostaw niezmienione**. Jeśli wybrano tę opcję, podczas stosowania profilu Kaspersky Security Center z określonymi ustawieniami szyfrowania dla dysków wymiennych, Kaspersky Endpoint Security nie szyfruje ani nie deszyfruje plików przechowywanych na nośnikach wymiennych.

8. Utwórz reguły szyfrowania dla plików na dyskach wymiennych, których zawartość chcesz zaszyfrować.

9. Zastosuj profil.

Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

Natychmiast po zastosowaniu profilu, gdy użytkownik podłączy dysk wymienny lub gdy nośnik jest już podłączony, Kaspersky Endpoint Security powiadomi użytkownika o tym, że dysk wymienny znajduje się pod działaniem reguły szyfrowania, dzięki czemu dane przechowywane na dysku wymiennym zostaną zaszyfrowane.

Jeśli dla szyfrowania danych na dysku wymiennym określono regułę *Pozostaw niezmienione*, aplikacja nie wyświetla żadnych powiadomień.

Aplikacja ostrzega użytkownika, że proces szyfrowania może zająć trochę czasu.

Aplikacja zażąda potwierdzenia szyfrowania i wykona następujące czynności:

- Zaszyfruje dane zgodnie z ustawieniami profilu, jeśli użytkownik wyrazi na to zgodę.
- Pozostawi dane niezaszyfrowane, jeśli użytkownik anuluje szyfrowanie, i ograniczy dostęp do plików nośnika wymiennego jako tylko do odczytu.
- Pozostawi dane niezaszyfrowane, jeśli użytkownik zignoruje pytanie o zaszyfrowanie, ograniczy dostęp do plików tylko do odczytu na dysku wymiennym i ponownie zażąda potwierdzenia zaszyfrowania danych przy kolejnym zastosowaniu profilu Kaspersky Security Center lub podłączeniu dysku wymiennego.

Profil Kaspersky Security Center z predefiniowanymi ustawieniami szyfrowania danych na dyskach wymiennych zostanie utworzony dla określonej grupy zarządzanych komputerów. Dlatego też wynik szyfrowania danych na dyskach wymiennych zależy od komputera, do którego podłączony został dysk wymienny.

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.

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.

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** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz dodać reguły szyfrowania nośników wymiennych.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie nośników wymiennych**.
7. Kliknij przycisk **Dodaj** lewym klawiszem myszy 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 tym profilu**.

     Zostanie otwarte okno **Dodaj urządzenia z listy zaufanych urządzeń**.

- Jeśli chcesz dodać regułę szyfrowania dla nośników wymiennych, które znajdują się na liście Kaspersky Security Center, wybierz **Z listy urządzeń Kaspersky Security Center**.

  Zostanie otwarte okno **Dodaj urządzenia z listy Kaspersky Security Center**.

8. Jeśli w poprzednim kroku wybrałeś opcję **Z listy urządzeń Kaspersky Security Center**, określ filtry wyświetlania urządzeń w tabeli. W tym celu:

   a. Określ wartości następujących parametrów: **Wyświetl w tabeli urządzenia, dla których określono**, **Rodzaj urządzenia**, **Nazwa**, **Komputer** i **Kaspersky Disk Encryption**.

   b. Kliknij przycisk **Odśwież**.

9. W kolumnie **Rodzaj urządzenia** zaznacz pola obok nazw dysków wymiennych, dla których chcesz utworzyć reguły szyfrowania.

10. Z listy rozwijalnej **Tryb szyfrowania dla wybranych urządzeń** wybierz akcję, jaka zostanie wykonana przez Kaspersky Endpoint Security na plikach przechowywanych na wybranych dyskach wymiennych.

11. 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.

12. 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 nośnik wymienny**, sektory, które nie są zajęte przez pliki, będą wciąż niezaszyfrowane.

13. 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**.

14. Kliknij **OK**.

    Wiersze z parametrami utworzonych reguł szyfrowania pojawią się w tabeli **Reguły niestandardowe**.

15. W celu zapisania zmian kliknij **OK**.

Dodane reguły szyfrowania dysku wymiennego są stosowane do dysków wymiennych, które są podłączone do dowolnych komputerów kontrolowanych przez zmodyfikowany profil Kaspersky Security Center.

Modyfikowanie reguły szyfrowania dla nośników wymiennych

W celu zmodyfikowania reguły szyfrowania dla nośnika wymiennego:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz zmodyfikować regułę szyfrowania nośnika wymiennego.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie nośników wymiennych**.
7. Na liście nośników wymiennych, dla których skonfigurowano reguły szyfrowania, wybierz wpis odpowiadający żądanemu nośnikowi wymiennemu.
8. Kliknij przycisk **Określ regułę**, aby zmodyfikować regułę szyfrowania dla wybranego dysku wymiennego.
   Zostanie otwarte menu kontekstowe przycisku **Określ regułę**.
9. Z menu kontekstowego przycisku **Określ regułę** wybierz akcję wykonywaną przez Kaspersky Endpoint Security na plikach przechowywanych na wybranym dysku wymiennym.
10. W celu zapisania zmian kliknij **OK**.

Zmodyfikowane reguły szyfrowania dysku wymiennego są stosowane do dysków wymiennych, które są podłączone do dowolnych komputerów kontrolowanych przez zmodyfikowany profil Kaspersky Security Center.

Włączanie trybu przenośnego dla uzyskiwania dostępu do zaszyfrowanych plików na dyskach wymiennych

W celu włączenia trybu przenośnego dla uzyskiwania dostępu do zaszyfrowanych plików na dyskach wymiennych:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli, w folderze **Zarządzane urządzenia** otwórz folder z nazwą grupy administracyjnej, dla której chcesz włączyć tryb przenośny dla uzyskiwania dostępu do zaszyfrowanych plików na nośnikach wymiennych.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie nośników wymiennych**.

7. Zaznacz pole **Tryb przenośny**.

   Tryb przenośny jest dostępny dla szyfrowania wszystkich plików lub tylko nowych plików.

8. Kliknij **OK**.

9. Zastosuj profil.

   Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

10. Podłącz nośnik wymienny do urządzenia, na którym zastosowano profil Kaspersky Security Center.

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. Kliknij **OK**.

    Kaspersky Endpoint Security szyfruje pliki na nośniku wymiennym zgodnie z regułami szyfrowania, zdefiniowanymi w profilu Kaspersky Security Center. Przenośny Menedżer plików używany do pracy z zaszyfrowanymi plikami także zostanie zapisany na nośniku wymiennym.

Po włączeniu trybu przenośnego, użytkownik może uzyskać dostęp do zaszyfrowanych plików na dyskach wymiennych podłączonych do komputera bez funkcji szyfrowania.

Deszyfrowanie nośników wymiennych

W celu odszyfrowania dysków wymiennych:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz skonfigurować deszyfrowanie nośników wymiennych.

3. W obszarze roboczym wybierz zakładkę **Profile**.

4. Wybierz interesujący Cię profil.

5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:

   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.

6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie nośników wymiennych**.

7. Jeśli chcesz odszyfrować wszystkie zaszyfrowane pliki przechowywane na dyskach wymiennych, z listy rozwijalnej **Tryb szyfrowania** wybierz **Odszyfruj cały nośnik wymienny**.

8. Aby odszyfrować dane przechowywane na pojedynczych dyskach wymiennych, zmodyfikuj reguły szyfrowania dla dysków wymiennych, których dane chcesz odszyfrować. W tym celu:

a. Na liście nośników wymiennych, dla których skonfigurowano reguły szyfrowania, wybierz wpis odpowiadający żądanemu nośnikowi wymiennemu.

b. Kliknij przycisk **Określ regułę**, aby zmodyfikować regułę szyfrowania dla wybranego dysku wymiennego.

Zostanie otwarte menu kontekstowe przycisku **Określ regułę**.

c. Wybierz element **Odszyfruj wszystkie pliki** z menu kontekstowego przycisk **Określ regułę**.

9. W celu zapisania zmian kliknij **OK**.

10. Zastosuj profil.

Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

Po zastosowaniu profilu, gdy użytkownik podłączy dysk wymienny lub gdy nośnik jest już podłączony, Kaspersky Endpoint Security powiadomi użytkownika o tym, że dysk wymienny znajduje się pod działaniem reguły szyfrowania, dzięki czemu zaszyfrowane pliki przechowywane na dysku wymiennym oraz system plików dysku wymiennego (jeśli jest zaszyfrowany) zostaną odszyfrowane. Aplikacja ostrzega użytkownika, że proces deszyfrowania może zająć trochę czasu.

Profil Kaspersky Security Center z predefiniowanymi ustawieniami szyfrowania danych na dyskach wymiennych zostanie utworzony dla określonej grupy zarządzanych komputerów. Dlatego też wynik deszyfrowania danych na dyskach wymiennych zależy od komputera, do którego podłączony został dysk wymienny.

Jeśli użytkownik zainicjuje bezpieczne usuwanie dysku wymiennego w trakcie deszyfrowania danych, Kaspersky Endpoint Security przerwie proces deszyfrowania i pozwoli na usunięcie dysku wymiennego przed zakończeniem procesu deszyfrowania.

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.

Szyfrowanie dysków twardych

Jeśli program Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla stacji roboczych, technologie Szyfrowanie dysków funkcją BitLocker i Kaspersky Disk Encryption będą dostępne do szyfrowania. Jeśli program Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów plików, dostępne jest tylko technologia Szyfrowanie dysków funkcją BitLocker.

Ta sekcja zawiera informacje o szyfrowaniu dysków twardych oraz instrukcje dotyczące konfiguracji i przeprowadzania szyfrowania dysków twardych z Kaspersky Endpoint Security i Wtyczką konsoli Kaspersky Endpoint Security.

Informacje o szyfrowaniu dysków twardych

Przed rozpoczęciem szyfrowania dysku twardego aplikacja wykonuje kilka 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 dysku twardego 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 dysków twardych 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 dysku twardego, w wierszu polecenia wpisz `avp pbatestreset`. Jeśli system operacyjny nie załaduje się po sprawdzeniu dysku twardego na kompatybilność z Agentem autoryzacji, usuń obiekty i dane pozostałe po testowym działaniu Agenta autoryzacji, korzystając z Narzędzia przywracania zaszyfrowanego urządzenia. Następnie uruchom Kaspersky Endpoint Security i ponownie wykonaj polecenie `avp pbatestreset`.

Po uruchomieniu szyfrowania dysku twardego, Kaspersky Endpoint Security zaszyfruje wszystkie dane zapisane na dyskach twardych.

Jeśli podczas deszyfrowania dysku twardego użytkownik zamknie lub uruchomi ponownie komputer, Agent autoryzacji załaduje się przed kolejnym uruchomieniem systemu operacyjnego. Kaspersky Endpoint Security wznawia szyfrowanie dysków twardych po pomyślnej autoryzacji w Agencie autoryzacji i uruchomieniu systemu operacyjnego.

Jeśli podczas szyfrowania dysków twardych system operacyjny przełączy się w tryb hibernacji, Agent autoryzacji zostanie załadowany po wyjściu systemu operacyjnego z trybu hibernacji. Kaspersky Endpoint Security wznawia szyfrowanie dysków twardych po pomyślnej autoryzacji w Agencie autoryzacji i uruchomieniu systemu operacyjnego.

Jeśli podczas szyfrowania dysku twardego system operacyjny przejdzie w tryb uśpienia, Kaspersky Endpoint Security wznowi szyfrowanie dysków twardych 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.

Agent autoryzacji obsługuje układy klawiatury dla następujących języków:

- Angielski (UK)
- Angielski (USA)
- Arabski (Algieria, Maroko, Tunis; układ AZERTY)
- Hiszpański (Ameryka Łacińska)
- Włoski
- Niemiecki (Niemcy i Austria)

- Niemiecki (Szwajcaria)
- Portugalski (Brazylia, układ ABNT2)
- Rosyjski (dla klawiatury o 105 klawiszach odpowiadającej układowi QWERTY systemu IBM / Windows)
- Turecki (układ QWERTY)
- Francuski (Francja)
- Francuski (Szwajcaria)
- Francuski (Belgia, układ AZERTY)
- Japoński (dla klawiatury o 106 klawiszach z układem QWERTY)

Układ klawiatury staje się dostępny w Agencie autoryzacji, jeśli ten układ został dodany w ustawieniach języka i standardów regionalnych systemu operacyjnego oraz stał się dostępny na ekranie powitalnym Microsoft Windows.

Jeśli nazwa konta Agenta autoryzacji zawiera symbole, których nie można wprowadzić przy użyciu układów klawiatury dostępnych w Agencie autoryzacji, dostęp do zaszyfrowanych dysków twardych można uzyskać tylko po ich przywróceniu przy pomocy Narzędzia przywracania zaszyfrowanego urządzenia lub po odzyskaniu nazwy i hasła kona Agenta autoryzacji.

Kaspersky Endpoint Security obsługuje następujące tokeny, czytniki kart inteligentnych oraz karty inteligentne:

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (karta inteligentna)
- SafeNet eToken 4100 72K Java (karta inteligentna)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB)
- Rutoken EDS (USB)
- Rutoken EDS (Flash)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (karta inteligentna)
- Athena IDProtect Laser (USB)

- Gemalto IDBridge CT40 (czytnik)
- Gemalto IDPrime .NET 511

Szyfrowanie dysków twardych przy użyciu technologii Kaspersky Disk Encryption

Przed zaszyfrowaniem dysków twardych na komputerze zalecamy upewnić się, że komputer nie jest zainfekowany. W tym celu uruchom zadanie Pełne skanowanie lub Skanowanie obszarów krytycznych. Szyfrowanie dysku twardego komputera, który został zainfekowany rootkitem, może spowodować problemy z jego działaniem (a nawet jego awarię).

W celu zaszyfrowania dysków twardych przy użyciu technologii Kaspersky Disk Encryption:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz skonfigurować szyfrowanie dysków twardych.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie dysków twardych**.
7. 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.

8. Z listy rozwijalnej **Tryb szyfrowania** wybierz **Zaszyfruj wszystkie dyski twarde**.

   Jeśli chcesz wykluczyć niektóre dyski twarde z szyfrowania, utwórz listę tych dysków twardych.

9. 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**.

  Ta funkcja jest stosowana tylko na niezaszyfrowanych urządzeniach. Jeśli urządzenie zostało wcześniej zaszyfrowane przy użyciu funkcji **Zaszyfruj tylko używaną przestrzeń dyskową**, po zastosowaniu profilu w trybie **Zaszyfruj wszystkie dyski twarde**, sektory, które nie są zajęte przez pliki, będą wciąż niezaszyfrowane.

10. W celu zapisania zmian kliknij **OK**.

11. Zastosuj profil.

    Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

Szyfrowanie dysków twardych przy pomocy technologii Szyfrowanie dysków funkcją BitLocker

Przed zaszyfrowaniem dysków twardych na komputerze zalecamy upewnić się, że komputer nie jest zainfekowany. W tym celu uruchom zadanie Pełne skanowanie lub Skanowanie obszarów krytycznych. Szyfrowanie dysku twardego komputera, który został zainfekowany rootkitem, może spowodować problemy z jego działaniem (a nawet jego awarię).

Użycie technologii Szyfrowanie dysków funkcją BitLocker na komputerach z serwerowym systemem operacyjnym może wymagać zainstalowania komponentu **Szyfrowanie dysków funkcją BitLocker** przy pomocy Kreatora dodawania ról i komponentów.

W celu zaszyfrowania dysków twardych przy pomocy technologii Szyfrowanie dysków funkcją BitLocker:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz skonfigurować szyfrowanie dysków twardych.

3. W obszarze roboczym wybierz zakładkę **Profile**.

4. Wybierz interesujący Cię profil.

5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:

   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.

   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.

6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie dysków twardych**.

7. Z listy rozwijalnej **Technologia szyfrowania** wybierz opcję **Szyfrowanie dysków funkcją BitLocker**.

8. Z listy rozwijalnej **Tryb szyfrowania** wybierz opcję **Zaszyfruj wszystkie dyski twarde**.

9. Jeśli do wprowadzania informacji w środowisku wykonawczym przed uruchomieniem systemu chcesz używać klawiatury dotykowej, zaznacz pole **Zezwól na korzystanie na tabletach z uwierzytelniania wymagającego autoryzacji klawiatury przed rozruchem**.

   Zalecane jest korzystanie z tego ustawienia tylko na urządzeniach, na których znajdują się alternatywne narzędzia do wprowadzania danych przed rozruchem, na przykład klawiatura USB.

10. Wybierz jeden z następujących rodzajów szyfrowania:

    - Jeśli chcesz używać szyfrowania sprzętowego, zaznacz pole **Użyj szyfrowania sprzętowego**.
    - Jeśli chcesz używać szyfrowania programowego, odznacz pole **Użyj szyfrowania sprzętowego**.

11. 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 szyfrowanie chcesz zastosować do całego dysku twardego, odznacz opcję **Zaszyfruj tylko używaną przestrzeń dyskową**.

      Ta funkcja jest stosowana tylko na niezaszyfrowanych urządzeniach. Jeśli urządzenie zostało wcześniej zaszyfrowane przy użyciu funkcji **Zaszyfruj tylko używaną przestrzeń dyskową**, po zastosowaniu profilu w trybie **Zaszyfruj wszystkie dyski twarde**, sektory, które nie są zajęte przez pliki, będą wciąż niezaszyfrowane.

12. Wybierz metodę dostępu do dysków twardych zaszyfrowanych funkcją BitLocker.

    - Jeśli chcesz używać Trusted Platform Module (TPM) do przechowywania kluczy szyfrowania, zaznacz opcję **Używaj modułu TPM (Trusted Platform Module)**.
    - Jeśli do szyfrowania dysków twardych nie używasz modułu TPM, zaznacz opcję **Użyj hasła** i w polu **Minimalna długość hasła** określ minimalną liczbę znaków, jaką hasło musi zawierać.

    Dostępność Trusted Platform Module (TPM) jest obowiązkowa dla systemów operacyjnych Windows 7 i Windows 2008 R2, a także dla wcześniejszych wersji.

13. Jeśli w poprzednim kroku wybrałeś opcję **Używaj modułu TPM (Trusted Platform Module)**:

    - Jeśli chcesz ustawić kod PIN, który będzie wymagany, gdy użytkownik spróbuje uzyskać dostęp do klucza szyfrowania, zaznacz pole **Użyj kodu PIN** i w polu **Minimalna długość kodu PIN** określ minimalną liczbę cyfr, jaką kod PIN musi zawierać.
    - Jeśli chcesz uzyskać dostęp do zaszyfrowanych dysków twardych bez użycia modułu TPM na komputerze, korzystając z hasła, zaznacz pole **Używaj hasła, jeśli moduł TPM jest niedostępny** i w polu **Minimalna długość hasła** określ minimalną liczbę znaków, jaką hasło powinno zawierać.

      W tym przypadku dostęp do kluczy szyfrowania będzie możliwy po podaniu określonego hasła, jeśli pole **Użyj hasła** jest zaznaczone.

      Jeśli pole **Używaj hasła, jeśli moduł TPM jest niedostępny** nie jest zaznaczone, a moduł TPM jest niedostępny, szyfrowanie dysku twardego nie zostanie uruchomione.

14. W celu zapisania zmian kliknij **OK**.

15. Zastosuj profil.

    Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

Po zastosowaniu profilu na komputerze klienckim z zainstalowanym programem Kaspersky Endpoint Security, wprowadzone zostaną następujące procedury:

- Jeśli profil szyfrowania jest stosowany do dysku twardego, w przypadku korzystania z modułu TPM zostanie wyświetlone okno do wpisania kodu PIN, a gdy moduł TPM nie jest używany, zostanie wyświetlone okno do podania 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 nowszym będzie wyświetlane okno z żądaniem podłączenia urządzenia USB w celu zapisania pliku klucza odzyskiwania.

Jeśli nie ma dostępu do kluczy szyfrowania, użytkownik może poprosić administratora sieci lokalnej o dostarczenie klucza odzyskiwania (klucz odzyskiwania nie może być kodem, który był wcześniej zapiany na urządzeniu USB lub został utracony).

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 drzewie Konsoli administracyjnej, w folderze **Zarządzane urządzenia** otwórz folder z nazwą grupy administracyjnej, dla której chcesz utworzyć listę dysków twardych, które będą wykluczone z szyfrowania.

3. W obszarze roboczym wybierz zakładkę **Profile**.

4. Wybierz interesujący Cię profil.

5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:

   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.

   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.

6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie dysków twardych**.

7. 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.

8. W celu dodania dysków twardych do listy dysków twardych wykluczonych z szyfrowania:

   a. Kliknij przycisk **Dodaj**.

Zostanie otwarte okno **Dodaj urządzenia z listy Kaspersky Security Center**.

b. W oknie **Dodaj urządzenia z listy Kaspersky Security Center** określ wartości następujących parametrów: **Nazwa**, **Komputer**, **Typ dysku** i **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**.

9. 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**.

10. W celu zapisania zmian kliknij **OK**.

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** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz skonfigurować deszyfrowanie dysków twardych.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Szyfrowanie dysków twardych**.
7. Z listy rozwijalnej **Technologia szyfrowania** wybierz technologię, za pomocą której zostały zaszyfrowane dyski twarde.
8. 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.

9. W celu zapisania zmian kliknij **OK**.
10. Zastosuj profil.

    Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

Jeśli podczas deszyfrowania dysków twardych, zaszyfrowanych za pomocą technologii Kaspersky Disk Encryption, użytkownik zamknie lub uruchomi ponownie komputer, Agent autoryzacji załaduje się przed kolejnym uruchomieniem systemu operacyjnego. Kaspersky Endpoint Security wznawia deszyfrowanie dysku twardego po pomyślnej autoryzacji w Agencie autoryzacji i uruchomieniu systemu operacyjnego.

Jeśli podczas deszyfrowania dysków twardych, zaszyfrowanych za pomocą technologii Kaspersky Disk Encryption, system operacyjny przełączy się w tryb hibernacji, Agent autoryzacji załaduje się po wyjściu systemu operacyjnego z trybu hibernacji. Kaspersky Endpoint Security wznawia deszyfrowanie dysku twardego po pomyślnej autoryzacji w Agencie autoryzacji i uruchomieniu systemu operacyjnego. Po odszyfrowaniu dysku twardego, tryb hibernacji jest niedostępny, aż do pierwszego ponownego uruchomienia systemu operacyjnego.

Jeśli podczas deszyfrowania dysku twardego system operacyjny przejdzie w tryb uśpienia, Kaspersky Endpoint Security wznowi deszyfrowanie dysku twardego po wyjściu systemu operacyjnego z trybu uśpienia, bez wczytywania Agenta autoryzacji.

Zarządzanie Agentem autoryzacji

Jeśli dyski twarde są zaszyfrowane, Agent autoryzacji ładuje się przed uruchomieniem systemu operacyjnego. Użyj Agenta autoryzacji do zakończenia procesu autoryzacji, aby uzyskać dostęp do zaszyfrowanych dysków twardych i załadować system operacyjny.

Po pomyślnym zakończeniu procedury autoryzacji, system operacyjny zostanie załadowany. Proces autoryzacji jest powtarzany przy każdym ponownym uruchomieniu systemu operacyjnego.

W niektórych przypadkach użytkownik może nie przejść procedury autoryzacji. Na przykład, autoryzacja jest niemożliwa, gdy użytkownik zapomniał dane uwierzytelniające konta Agenta autoryzacji, hasło do tokena lub karty inteligentnej, bądź też zgubił token lub kartę inteligentną.

Jeśli użytkownik zapomniał dane uwierzytelniające konta Agenta autoryzacji lub hasło do tokena lub karty inteligentnej, może skontaktować się z administratorem korporacyjnej sieci LAN w celu odzyskania ich.

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 danych na zaszyfrowanych urządzeniach.

Używanie tokenów i kart inteligentnych z Agentem autoryzacji

Token lub karta inteligentna mogą zostać użyte do autoryzacji podczas dostępu do zaszyfrowanych dysków twardych. W tym celu należy dodać plik certyfikatu elektronicznego tokena lub karty inteligentnej do polecenia tworzenia konta 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.

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.

  Jeśli certyfikat elektroniczny tokena lub karty inteligentnej nie spełnia tego wymagania, wtyczka zarządzająca nie załaduje pliku tego certyfikatu do polecenia tworzenia konta Agenta autoryzacji i wyświetli wiadomość o błędzie.

- Parametr `KeyUsage`, definiujący przeznaczenie certyfikatu, musi posiadać wartość `keyEncipherment` lub `dataEncipherment`.

  Jeśli certyfikat elektroniczny tokena lub karty inteligentnej nie spełnia tego wymagania, wtyczka zarządzająca załaduje plik tego certyfikatu do polecenia tworzenia konta Agenta autoryzacji i wyświetli ostrzeżenie.

- Certyfikat zawiera klucz RSA o długości minimum 1024 bitów.

  Jeśli certyfikat elektroniczny tokena lub karty inteligentnej nie spełnia tego wymagania, wtyczka zarządzająca nie załaduje pliku tego certyfikatu do polecenia tworzenia konta Agenta autoryzacji i wyświetli wiadomość o błędzie.

Modyfikowanie komunikaty pomocy Agenta Autoryzacji

Przed zmodyfikowaniem komunikaty pomocy Agenta Autoryzacji należy przejrzeć listę znaków obsługiwanych w środowisku wykonawczym przed uruchomieniem systemu.

W celu zmodyfikowania komunikaty pomocy Agenta Autoryzacji:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz zmodyfikować komunikaty pomocy Agenta Autoryzacji.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.

6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Ogólne ustawienia szyfrowania**.
7. W sekcji **Szablony** kliknij przycisk **Pomoc**.

   Zostanie otwarte okno **Komunikaty pomocy Agenta Autoryzacji**.
8. 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.
9. Zmodyfikuj treść pomocy.

   Jeśli chcesz przywrócić oryginalny tekst, kliknij przycisk **Domyślny**.
10. Kliknij **OK**.
11. Aby zapisać zmiany, w oknie **Właściwości: <Nazwa profilu>** kliknij **OK**.

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.

Wybieranie poziomu śledzenia Agenta autoryzacji

Aplikacja zapisuje w pliku śledzenia informacje serwisowe o działaniu Agenta autoryzacji oraz informacje o działaniach użytkownika dotyczących Agenta autoryzacji. Plik śledzenia Agenta autoryzacji może być pomocny podczas przywracania danych na zaszyfrowanych dyskach twardych.

W celu wybrania poziomu śledzenia Agenta autoryzacji:

1. Jak tylko uruchomi się komputer z zaszyfrowanymi dyskami twardymi, wciśnij klawisz **F3**, aby wywołać okno konfiguracji ustawień Agenta autoryzacji.
2. W oknie ustawień Agenta 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 znajdują się zaszyfrowane dyski twarde lub podczas szyfrowania dysków twardych.

W przeciwieństwie do innych plików śledzenia aplikacji, plik śledzenia Agenta autoryzacji nie jest wysyłany na serwer Kaspersky. Jeśli jest to konieczne, administrator systemu może ręcznie wysłać plik śledzenia Agenta autoryzacji do Kaspersky w celu przeprowadzenia jego analizy.

Zarządzanie kontami Agenta autoryzacji

Do zarządzania kontami Agenta autoryzacji dostępne są następujące narzędzia Kaspersky Security Center:

- Zadanie grupowe dotyczące zarządzania kontami Agenta autoryzacji. Zadanie to umożliwia zarządzanie kontami Agenta autoryzacji dla grupy komputerów klienckich.
- Zadanie lokalne **Szyfrowanie (zarządzanie kontem)**. Zadanie to umożliwia zarządzanie kontami Agenta autoryzacji dla pojedynczych komputerów klienckich.

W celu skonfigurowania ustawień zadania zarządzania kontem Agenta autoryzacji:

1. Utwórz zadanie zarządzanie kontem Agenta autoryzacji (Tworzenie zadania lokalnego, Tworzenie zadania grupowego).
2. Otwórz sekcję **Ustawienia** w oknie **Właściwości: <Nazwa zadania zarządzania kontem Agenta autoryzacji>**.
3. Dodaj polecenia utworzenia kont Agenta autoryzacji.
4. Dodaj polecenia modyfikacji kont Agenta autoryzacji.
5. Dodaj polecenia usunięcia kont użytkowników Agenta autoryzacji.
6. Jeśli jest to konieczne, zmodyfikuj dodane polecenia do zarządzania kontami Agenta autoryzacji. W tym celu wybierz polecenie w tabeli **Polecenia do zarządzania kontami Agenta autoryzacji** i kliknij przycisk **Modyfikuj**.
7. Jeśli jest to konieczne, usuń dodane polecenia do zarządzania kontami Agenta autoryzacji. W tym celu, w tabeli **Polecenia do zarządzania kontami Agenta autoryzacji:** wybierz jedno lub kilka poleceń i kliknij przycisk **Usuń**.

   W przypadku, gdy chcesz wybrać kilka elementów, zaznacz je, trzymając wciśnięty klawisz **CTRL**.

8. Aby zapisać wprowadzone zmiany, w oknie właściwości zadania kliknij **OK**.
9. Uruchom zadanie.

Wykonane zostaną polecenia do zarządzania kontami Agenta autoryzacji dodane do zadania.

Dodawanie polecenia utworzenia konta Agenta autoryzacji

W celu dodania polecenia utworzenia konta Agenta autoryzacji:

1. Otwórz sekcję **Ustawienia** w oknie **Właściwości: <Nazwa zadania zarządzania kontem Agenta autoryzacji>**.

2. Kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz **Polecenie dodania konta**.

   Zostanie otwarte okno **Dodaj konto użytkownika**.

3. W polu **Dodaj konto użytkownika** okna **Konto użytkownika Windows** określ nazwę konta systemu Microsoft Windows, w oparciu o które zostanie utworzone konto Agenta autoryzacji.

   W tym celu ręcznie wpisz nazwę konta lub kliknij przycisk **Wybierz**.

4. Jeśli ręcznie wprowadziłeś nazwę konta systemu Microsoft Windows, kliknij przycisk **Zezwól**, aby określić identyfikator zabezpieczeń (SID) konta.

   Jeśli zdecydujesz się nie określać identyfikatora zabezpieczeń (SID) poprzez kliknięcie przycisku **Zezwól**, zostanie on określony w momencie wykonywania zadania na komputerze.

   > Określenie numeru SID konta systemu Microsoft Windows podczas dodawania polecenia utworzenia konta Agenta autoryzacji jest odpowiednie dla upewnienia się, że ręcznie wprowadzona nazwa konta systemu Microsoft Windows jest poprawna. Jeśli wprowadzone konto użytkownika systemu Microsoft Windows nie istnieje, należy do niezaufanej domeny lub nie istnieje na komputerze, dla którego zmodyfikowano zadanie lokalne **Szyfrowanie (zarządzanie kontem)**, zadanie zarządzania kontem Agenta autoryzacji zakończy się błędem.

5. Zaznacz pole **Zmień istniejące konto użytkownika**, aby mieć konto o tej samej nazwie, czyli wcześniej utworzone konto 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 jest niedostępny podczas dodawania polecenia tworzenia konta Agenta autoryzacji we właściwościach zadania lokalnego **Szyfrowanie (zarządzanie kontem)**.

6. W polu **Nazwa użytkownika** wpisz nazwę konta Agenta autoryzacji, która ma być wprowadzona podczas procesu autoryzacji, aby uzyskać dostęp do zaszyfrowanych dysków twardych.

7. 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.

8. Jeśli w poprzednim kroku wybrałeś opcję **Zezwól na uwierzytelnianie przy użyciu hasła**:

   a. W polu **Hasło** wpisz hasło do konta Agenta autoryzacji, które ma być wprowadzone podczas procesu autoryzacji, aby uzyskać dostęp do zaszyfrowanych dysków twardych.

   b. W polu **Potwierdź hasło** potwierdź hasło do konta Agenta autoryzacji wprowadzone w poprzednim kroku.

   c. Wykonaj jedną z poniższych czynności:

   - Zaznacz opcję **Zmień hasło podczas pierwszej autoryzacji**, jeśli chcesz, aby aplikacja wyświetlała żądanie zmiany hasła użytkownikowi przechodzącemu proces autoryzacji po raz pierwszy z poziomu konta określonego w poleceniu.

   - W innym przypadku zaznacz opcję **Nie wymagaj zmiany hasła**.

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.

10. Jeśli w poprzednim kroku zaznaczyłeś opcję **Zezwól na uwierzytelnianie przy użyciu certyfikatu**, kliknij przycisk **Przeglądaj** i w oknie **Wybierz plik certyfikatu** wybierz plik certyfikatu elektronicznego tokena lub karty inteligentnej.

11. Jeśli to konieczne, w polu **Opis polecenia** wprowadź szczegółowe informacje dotyczące konta Agenta autoryzacji, których potrzebujesz do zarządzania poleceniem.

12. Wykonaj jedną z poniższych czynności:

    - Zaznacz pole **Zezwól na autoryzację**, jeśli chcesz, aby aplikacja zezwalała użytkownikowi działającemu pod kontem określonym w poleceniu na dostęp do okna autoryzacji Agenta autoryzacji.

    - Zaznacz pole **Zablokuj autoryzację**, jeśli chcesz, aby aplikacja blokowała użytkownikowi działającemu pod kontem określonym w poleceniu dostęp do okna autoryzacji Agenta autoryzacji.

13. W oknie **Dodaj konto użytkownika** kliknij **OK**.

Dodawanie polecenia edycji konta Agenta autoryzacji

W celu dodania polecenia modyfikacji konta Agenta autoryzacji:

1. W sekcji **Ustawienia** okna **Właściwości: <Nazwa zadania zarządzania kontem Agenta autoryzacji>** otwórz menu kontekstowe przycisku **Dodaj** i wybierz element **Polecenie edycji konta**.

   Zostanie otwarte okno **Edytuj konto użytkownika**.

2. W polu **Konto użytkownika Windows** okna **Edytuj konto użytkownika** określ konto użytkownika systemu Microsoft Windows, w oparciu o które utworzone zostało konto Agenta autoryzacji, które chcesz zmodyfikować. W tym celu ręcznie wpisz nazwę konta lub kliknij przycisk **Wybierz**.

3. Jeśli ręcznie wprowadziłeś nazwę konta użytkownika systemu Microsoft Windows, kliknij przycisk **Zezwól**, aby określić identyfikatora zabezpieczeń (SID) konta użytkownika.

   Jeśli zdecydujesz się nie określać identyfikatora zabezpieczeń (SID) poprzez kliknięcie przycisku **Zezwól**, zostanie on określony w momencie wykonywania zadania na komputerze.

   > Określenie numeru SID konta użytkownika systemu Microsoft Windows podczas dodawania polecenia zmodyfikowania konta Agenta autoryzacji jest odpowiednie dla upewnienia się, że ręcznie wprowadzone konto użytkownika systemu Microsoft Windows jest poprawne. Jeśli wprowadzone konto użytkownika systemu Microsoft Windows nie istnieje lub należy do niezaufanej domeny, zadanie grupowe do zarządzania kontami Agenta autoryzacji zakończy się błędem.

4. 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 użytkownika Windows**, na nazwę wpisaną w polu poniżej.

5. Zaznacz pole **Modyfikuj ustawienia uwierzytelniania przy użyciu hasła**, aby możliwe było zmodyfikowanie ustawień autoryzacji opartej o hasło.

6. 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.

7. Jeśli w poprzednim kroku wybrałeś opcję **Zezwól na uwierzytelnianie przy użyciu hasła**:

   a. W polu **Hasło** wprowadź nowe hasło do konta Agenta autoryzacji.

   b. W polu **Potwierdź hasło** potwierdź hasło wprowadzone w poprzednim kroku.

8. 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 użytkownika Windows** na wartość określoną poniżej.

9. Określ wartość ustawienia zmiany hasła po autoryzacji w Agencie autoryzacji.

10. Zaznacz pole **Modyfikuj ustawienia uwierzytelniania przy użyciu certyfikatu**, aby możliwe było zmodyfikowanie ustawień autoryzacji opartej o certyfikat elektroniczny tokena lub karty inteligentnej.

11. 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.

12. Jeśli w poprzednim kroku zaznaczyłeś opcję **Zezwól na uwierzytelnianie przy użyciu certyfikatu**, kliknij przycisk **Przeglądaj** i w oknie **Wybierz plik certyfikatu** wybierz plik certyfikatu elektronicznego tokena lub karty inteligentnej.

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 użytkownika Windows**.

14. Zaznacz pole **Edytuj regułę dostępu do autoryzacji przy użyciu Agenta Autoryzacji**, jeśli chcesz, aby Kaspersky Endpoint Security zmienił regułę dostępu użytkownika do okna autoryzacji w Agencie autoryzacji na wartość określoną poniżej dla wszystkich konta Agenta autoryzacji, utworzonych w oparciu o konto systemu Microsoft Windows posiadające nazwę określoną w polu **Konto użytkownika Windows**.

15. Określ regułę dostępu do okna autoryzacji w Agencie autoryzacji.

16. W oknie **Edytuj konto użytkownika** kliknij **OK**.

Dodawanie polecenia usunięcia konta Agenta autoryzacji

W celu dodania polecenia usunięcia konta Agenta autoryzacji:

1. W sekcji **Ustawienia** okna **Właściwości: <Nazwa zadania zarządzania kontem Agenta autoryzacji>** otwórz menu kontekstowe przycisku **Dodaj** i wybierz element **Polecenie usunięcia konta**.

   Zostanie otwarte okno **Usuń konto użytkownika**.

2. W polu **Konto użytkownika Windows** okna **Usuń konto użytkownika** określ konto użytkownika systemu Microsoft Windows, w oparciu o które utworzone zostało konto Agenta autoryzacji, które chcesz usunąć. W tym celu ręcznie wpisz nazwę konta lub kliknij przycisk **Wybierz**.

3. Jeśli ręcznie wprowadziłeś nazwę konta użytkownika systemu Microsoft Windows, kliknij przycisk **Zezwól**, aby określić identyfikatora zabezpieczeń (SID) konta użytkownika.

   Jeśli zdecydujesz się nie określać identyfikatora zabezpieczeń (SID) poprzez kliknięcie przycisku **Zezwól**, zostanie on określony w momencie wykonywania zadania na komputerze.

   > Określenie numeru SID konta użytkownika systemu Microsoft Windows podczas dodawania polecenia usunięcia konta Agenta autoryzacji jest odpowiednie dla upewnienia się, że ręcznie wprowadzone konto użytkownika systemu Microsoft Windows jest poprawne. Jeśli wprowadzone konto użytkownika systemu Microsoft Windows nie istnieje lub należy do niezaufanej domeny, zadanie grupowe do zarządzania kontami Agenta autoryzacji zakończy się błędem.

4. W oknie **Usuń konto użytkownika** kliknij **OK**.

Przywracanie danych uwierzytelniających konta Agenta autoryzacji

> Instrukcje te są przeznaczone dla użytkowników komputerów klienckich z zainstalowanym Kaspersky Endpoint Security.

W celu przywrócenia nazwy użytkownika i hasła dla konta Agenta autoryzacji:

1. Agent autoryzacji zostaje załadowany na komputerze z zaszyfrowanymi dyskami twardymi przed załadowaniem systemu operacyjnego. W interfejsie Agenta autoryzacji kliknij przycisk **Nie pamiętam hasła**, aby zainicjować proces przywracania nazwy użytkownika i hasła dla konta Agenta autoryzacji.

2. Postępuj zgodnie z instrukcjami Agenta autoryzacji, aby uzyskać sekcje zgłoszeń dotyczące przywrócenia nazwy użytkownika i hasła dla konta Agenta autoryzacji.

3. Podyktuj zawartość sekcji zgłoszeń wraz z nazwą komputera administratorowi sieci LAN Twojej firmy.

4. Odwiedź sekcje z odpowiedziami na zgłoszenia dotyczące przywrócenia nazwy użytkownika i hasła dla konta Agenta autoryzacji, które zostały utworzone i udostępnione przez administratora sieci LAN.

5. Wprowadź nowe hasło do konta Agenta autoryzacji i potwierdź je.

   Nazwa użytkownika konta Agenta autoryzacji jest określana przy użyciu sekcji z odpowiedziami na zgłoszenia dotyczące przywrócenia nazwy użytkownika i hasła dla konta Agenta autoryzacji.

Po wprowadzeniu i potwierdzeniu nowego hasła dla konta Agenta autoryzacji, hasło zostanie zapisane, a użytkownik uzyska dostęp do zaszyfrowanych dysków twardych.

Odpowiadanie na żądanie użytkownika w sprawie odzyskania danych uwierzytelniających konta Agenta autoryzacji

W celu utworzenia i przesłania do użytkownika sekcji z odpowiedziami na zgłoszenie dotyczące przywrócenia nazwy użytkownika i hasła dla konta Agenta autoryzacji:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W folderze **Zarządzane urządzenia** otwórz folder z nazwą grupy administracyjnej zawierającej komputer użytkownika, który wysłał zgłoszenie z prośbą o przywrócenie nazwy użytkownika i hasła dla konta Agenta autoryzacji.

3. W obszarze roboczym wybierz zakładkę **Urządzenia**.

4. Na zakładce **Urządzenia** wybierz komputer użytkownika, który wysłał zgłoszenie z prośbą o przywrócenie nazwy użytkownika i hasła dla konta Agenta autoryzacji, i kliknij go prawym przyciskiem myszy w celu otwarcia menu kontekstowego.

5. Z menu kontekstowego wybierz opcję **Przydziel dostęp do urządzeń oraz danych w trybie offline**.

   Zostanie otwarte okno **Przydziel dostęp do urządzeń oraz danych w trybie offline**.

6. W oknie **Przydziel dostęp do urządzeń oraz danych w trybie offline** wybierz zakładkę **Agent autoryzacji**.

7. W sekcji **Używany algorytm szyfrujący** wybierz typ algorytmu szyfrowania.

8. Z listy rozwijalnej **Konto** wybierz nazwę konta Agenta autoryzacji utworzonego dla użytkownika, który prosi o przywrócenie nazwy konta i hasła dla Agenta autoryzacji.

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.

    Zawartość sekcji z odpowiedziami na żądanie użytkownika dotyczące przywrócenia nazwy użytkownika i hasła dla konta Agenta autoryzacji będzie wyświetlana w polu **Klucz dostępu**.

11. Podyktuj użytkownikowi zawartość sekcji z odpowiedziami.

Przeglądanie informacji szczegółowych dotyczących szyfrowania danych

Sekcja ta opisuje sposób przeglądania informacji szczegółowych dotyczących szyfrowania danych.

Informacje o stanie szyfrowania

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 jest niezdefiniowany*. Profil Kaspersky Security Center nie został zdefiniowany dla komputera.
- *Trwa szyfrowanie / deszyfrowanie*. 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 i / lub deszyfrowanie 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.
- *Nie jest obsługiwane*. Funkcja szyfrowania danych nie jest dostępna na komputerze.

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 z nazwą grupy administracyjnej, do której należy wybrany komputer.
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 przesuń suwak w prawą stronę, do samego końca.

   Kolumna **Stan szyfrowania** wyświetla stan szyfrowania danych na komputerach w wybranej grupie administracyjnej. Ten stan jest tworzony w oparciu o informacje dotyczące szyfrowania plików na dyskach lokalnych komputera, szyfrowanie dysków twardych komputera oraz szyfrowania dysków wymiennych podłączonych do komputera.

Przeglądanie statystyk szyfrowania w panelach szczegółów Kaspersky Security Center

W celu przejrzenia stanu szyfrowania w panelach szczegółów 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 szczegółów** kliknij przycisk **Dodaj**.

Zostanie otwarte okno **Nowy panel szczegółów**.

e. W oknie **Nowy panel szczegółów** grupy **Stan ochrony** wybierz element **Szyfrowanie urządzenia**.

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 urządzenia**.

h. Kliknij **OK**.

i. Powtórz czynności z kroków d – h, wybierając element **Szyfrowanie nośników wymiennych** w sekcji **Stan ochrony** okna **Nowy panel szczegółów**.

Dodane panele szczegółów pojawią się na liście **Panele szczegółów** 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. Wykonaj jedną z poniższych czynności:

- Z otwartego menu kontekstowego komputera wybierz **Ochrona**.
- 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 listę błędów 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 **Utwórz szablon raportu**.

   Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu.
4. Postępuj zgodnie z instrukcjami Kreatora szablonu raportu. W oknie **Wybierz typ szablonu raportu**, w sekcji **Inne** wybierz jeden z następujących elementów:

   - **Raport o stanie szyfrowania zarządzanego urządzenia**.
   - **Raport z szyfrowania danych przechowywanych na urządzeniu**.
   - **Raport o błędach szyfrowania**.
   - **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.

Zostanie rozpoczęty proces tworzenia raportu. Raport zostanie wyświetlony w nowym oknie.

Zarządzanie zaszyfrowanymi plikami z ograniczoną funkcją szyfrowania plików

Po zastosowaniu profilu Kaspersky Security Center i zaszyfrowaniu plików, Kaspersky Endpoint Security uzyska klucz szyfrowania niezbędny do uzyskania 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.

Uzyskiwanie dostępu do zaszyfrowanych plików bez połączenia z Kaspersky Security Center

Instrukcje te są przeznaczone dla użytkowników komputerów klienckich z zainstalowanym Kaspersky Endpoint Security.

W celu uzyskania dostępu do zaszyfrowanych plików bez połączenia z Kaspersky Security Center:

1. Podejmij próbę uzyskania dostępu do zaszyfrowanego pliku, którego potrzebujesz.

   Jeśli podczas próby uzyskania dostępu do pliku przechowywanego na lokalnym dysku komputera nie ma połączenia z Kaspersky Security Center, program Kaspersky Endpoint Security generuje plik żądania dostępu do wszystkich zaszyfrowanych plików przechowywanych na lokalnych dyskach komputera. Jeśli użytkownik próbuje uzyskać dostęp do pliku przechowywanego na dysku wymiennym, Kaspersky Endpoint Security generuje plik żądania dostępu do wszystkich zaszyfrowanych plików przechowywanych na dysku wymiennym. Zostanie otwarte okno **Zablokowano dostęp do pliku**.

2. Wyślij plik zawierający żądanie dostępu do zaszyfrowanych plików do administratora sieci lokalnej. W tym celu wykonaj jedną z następujących czynności:

   - Aby do administratora sieci lokalnej wysłać pocztą elektroniczną plik zawierający żądanie dostępu do zaszyfrowanych plików, kliknij przycisk **Wyślij przez e-mail**.
   - Aby zapisać plik zgłoszenia dostępu do zaszyfrowanych plików i dostarczyć go do administratora sieci LAN za pomocą innej metody, kliknij przycisk **Zapisz**.

3. Uzyskaj plik klucza dostępu do zaszyfrowanych plików, który został utworzony i udostępniony przez administratora sieci lokalnej.

4. Aktywuj klucz dostępu do zaszyfrowanych plików w jeden z następujących sposobów:

   - W dowolnym menedżerze plików wybierz plik klucza dostępu do zaszyfrowanych plików. Otwórz go, klikając go dwukrotnie.
   - Wykonaj następujące czynności:

     a. Otwórz okno główne Kaspersky Endpoint Security.

     b. Kliknij przycisk .

     Zostanie otwarte okno **Zdarzenia**.

     c. Wybierz zakładkę **Stan dostępu do plików oraz urządzeń**.

Na tej zakładce znajduje się lista wszystkich zgłoszeń dostępu do zaszyfrowanych plików.

d. Wybierz zgłoszenie, dla którego otrzymałeś plik klucza dostępu do zaszyfrowanych plików.

e. Aby wczytać otrzymany plik klucza dostępu do zaszyfrowanych plików, kliknij **Przeglądaj**.

Zostanie otwarte standardowe okno **Wybierz plik klucza dostępu** w Microsoft Windows.

f. W standardowym oknie **Wybierz plik klucza dostępu** z Microsoft Windows wybierz plik z rozszerzeniem .kesdr dostarczony przez administratora i nazwę odpowiadającą nazwie pliku zgłoszenia dostępu.

g. Kliknij przycisk **Otwórz**.

h. W oknie **Zdarzenia** kliknij **OK**.

Jeśli podczas próby uzyskania dostępu do pliku przechowywanego na lokalnym dysku komputera generowany jest plik z żądaniem dostępu do zaszyfrowanych plików, program Kaspersky Endpoint Security nadaje uprawnienia dostępu do wszystkich zaszyfrowanych plików przechowywanych na lokalnych dyskach komputera. Jeśli podczas próby uzyskania dostępu do pliku przechowywanego na dysku wymiennym generowany jest plik żądania dostępu do zaszyfrowanych plików, program Kaspersky Endpoint Security nadaje uprawnienia dostępu do wszystkich zaszyfrowanych plików przechowywanych na dysku wymiennym. Aby mieć dostęp do zaszyfrowanych plików przechowywanych na innych dyskach wymiennych, należy uzyskać oddzielny plik klucza dostępu dla każdego dysku wymiennego.

Nadawanie użytkownikowi uprawnień dostępu do zaszyfrowanych plików bez nawiązywania połączenia z Kaspersky Security Center

W celu nadania użytkownikowi uprawnień dostępu do zaszyfrowanych plików bez nawiązywania połączenia z Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej, w folderze **Zarządzane urządzenia** otwórz folder z nazwą grupy administracyjnej zawierającej komputer użytkownika, który żąda dostępu do zaszyfrowanych plików.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Na zakładce **Urządzenia** wybierz komputer użytkownika, który żąda dostępu do zaszyfrowanych plików, i kliknij go prawym przyciskiem myszy.
5. Z menu kontekstowego wybierz opcję **Przydziel dostęp do urządzeń oraz danych w trybie offline**.

   Zostanie otwarte okno **Przydziel dostęp do urządzeń oraz danych w trybie offline**.
6. W oknie **Przydziel dostęp do urządzeń oraz danych w trybie offline** wybierz zakładkę **Szyfrowanie**.
7. Na zakładce **Szyfrowanie** kliknij przycisk **Przeglądaj**.

   Zostanie otwarte standardowe okno **Wybierz plik żądania dostępu** w Microsoft Windows.
8. W oknie **Wybierz plik żądania dostępu** określ ścieżkę dostępu do pliku zgłoszenia, otrzymanego od użytkownika, i kliknij **Otwórz**.

   Kaspersky Security Center generuje plik klucza dostępu do zaszyfrowanych plików. Szczegółowe informacje dotyczące zgłoszenia użytkownika są wyświetlane na zakładce **Szyfrowanie**.
9. Wykonaj jedną z poniższych czynności:

- Aby wysłać do użytkownika wiadomość e-mail z wygenerowanym plikiem klucza, kliknij przycisk **Wyślij przez e-mail**.

- Aby zapisać plik klucza dostępu dla zaszyfrowanych plików i dostarczyć go do użytkownika za pomocą innej metody, kliknij przycisk **Zapisz**.

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 drzewie Konsoli administracyjnej, w folderze **Zarządzane urządzenia** otwórz folder z nazwą grupy administracyjnej, dla której chcesz zmodyfikować szablony wiadomości z prośbą o dostęp do zaszyfrowanego pliku.

3. W obszarze roboczym wybierz zakładkę **Profile**.

4. Wybierz interesujący Cię profil.

5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:

   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.

   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.

6. W sekcji **Szyfrowanie danych** wybierz podsekcję **Ogólne ustawienia szyfrowania**.

7. W sekcji **Szablony** kliknij przycisk **Szablony**.

   Zostanie otwarte okno **Szablony**.

8. Wykonaj następujące czynności:

   - Jeśli chcesz zmodyfikować szablon wiadomości użytkownika, wybierz zakładkę **Komunikat użytkownika**. Okno **Odmowa dostępu do pliku** 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 **Odmowa dostępu do pliku** 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 **Nadaj uprawnienia dostępu do zaszyfrowanych plików** i jest wysyłany do użytkownika po nadaniu mu uprawnień dostępu do zaszyfrowanych plików.

9. Zmodyfikuj szablony wiadomości.

   Możesz użyć przycisku **Domyślny** oraz listy rozwijalnej **Zmienna**.

10. Kliknij **OK**.

11. Aby zapisać zmiany, w oknie **Właściwości: <Nazwa profilu>** kliknij **OK**.

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 odzyskaniem danych na zaszyfrowanych urządzeniach zalecane jest anulowanie profilu szyfrowania Kaspersky Security Center na komputerze, na którym to działanie będzie wykonywane. Zapobiega to ponownemu zaszyfrowaniu dysku.

Uzyskiwanie dostępu do zaszyfrowanych urządzeń z poziomu interfejsu aplikacji

Instrukcje te są przeznaczone dla użytkowników komputerów klienckich z zainstalowanym Kaspersky Endpoint Security.

W celu uzyskania dostępu do zaszyfrowanych urządzeń z poziomu interfejsu aplikacji:

1. Podejmij próbę uzyskania dostępu do zaszyfrowanego urządzenia, którego potrzebujesz.

   Zostanie otwarte okno **Dostęp do danych jest zablokowany**.

2. Wyślij do administratora firmowej sieci LAN plik żądania dostępu z rozszerzeniem kesdc dla zaszyfrowanego urządzenia. W tym celu wykonaj jedną z następujących czynności:

   - Aby wysłać do administratora firmowej sieci LAN wiadomość e-mail z wygenerowanym plikiem żądania dostępu do zaszyfrowanego urządzenia, kliknij przycisk **Wyślij przez e-mail**.
   - Aby zapisać plik żądania dostępu do zaszyfrowanego urządzenia i dostarczyć go do administratora firmowej sieci LAN za pomocą innej metody, kliknij przycisk **Zapisz**.

   Jeśli zamknąłeś okno **Dostęp do danych jest zablokowany** bez zapisania pliku żądania dostępu lub bez wysłania pliku do administratora firmowej sieci LAN, możesz to zrobić w każdej chwili, w oknie **Zdarzenia**, na zakładce **Stan dostępu do plików oraz urządzeń**. Aby otworzyć to okno, w oknie głównym aplikacji kliknij przycisk .

3. Pobierz i zapisz plik klucza dostępu do zaszyfrowanego urządzenia, który został utworzony i dostarczony przez administratora firmowej sieci LAN.

4. W celu zastosowania pliku klucza dostępu do zaszyfrowanego urządzenia użyj jednej z następujących metod:

   - W dowolnym menedżerze plików odszukaj plik klucza dostępu do zaszyfrowanego urządzenia i kliknij go dwukrotnie, aby go otworzyć.
   - Wykonaj następujące czynności:

     a. Otwórz okno główne Kaspersky Endpoint Security.

     b. Kliknij przycisk , aby otworzyć okno **Zdarzenia**.

     c. Wybierz zakładkę **Stan dostępu do plików oraz urządzeń**.

Na tej zakładce znajduje się lista wszystkich zgłoszeń dostępu do zaszyfrowanych plików i urządzeń.

d. Wybierz zgłoszenie, dla którego otrzymałeś plik klucza dostępu do zaszyfrowanego urządzenia.

e. Aby wczytać otrzymany plik klucza dostępu do zaszyfrowanego urządzenia, kliknij **Przeglądaj**.

Zostanie otwarte standardowe okno **Wybierz plik klucza dostępu** w Microsoft Windows.

f. W standardowym oknie **Wybierz plik klucza dostępu** z Microsoft Windows wybierz plik z rozszerzeniem kesdr dostarczony przez administratora i nazwę odpowiadającą nazwie pliku żądania dostępu do zaszyfrowanego urządzenia.

g. Kliknij przycisk **Otwórz**.

h. W oknie **Stan dostępu do plików oraz urządzeń** kliknij **OK**.

Program Kaspersky Endpoint Security umożliwi dostęp do zaszyfrowanego urządzenia.

Nadawanie użytkownikowi uprawnień dostępu do zaszyfrowanych urządzeń

W celu nadania użytkownikowi uprawnień dostępu do zaszyfrowanego urządzenia:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej, w folderze **Zarządzane urządzenia** otwórz folder z nazwą grupy administracyjnej zawierającej komputer użytkownika, który żąda dostępu do zaszyfrowanego urządzenia.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Na zakładce **Urządzenia** wybierz komputer użytkownika, który żąda dostępu do zaszyfrowanego urządzenia, i kliknij go prawym przyciskiem myszy.
5. Z menu kontekstowego wybierz opcję **Przydziel dostęp do urządzeń oraz danych w trybie offline**.

   Zostanie otwarte okno **Przydziel dostęp do urządzeń oraz danych w trybie offline**.
6. W oknie **Przydziel dostęp do urządzeń oraz danych w trybie offline** wybierz zakładkę **Szyfrowanie**.
7. Na zakładce **Szyfrowanie** kliknij przycisk **Przeglądaj**.

   Zostanie otwarte standardowe okno **Wybierz plik żądania dostępu** w Microsoft Windows.
8. W oknie **Wybierz plik żądania dostępu** określ ścieżkę dostępu do pliku zgłoszenia z rozszerzeniem kesdc, który otrzymałeś od użytkownika.
9. Kliknij przycisk **Otwórz**.

   Kaspersky Security Center generuje plik klucza dostępu do zaszyfrowanego urządzenia z rozszerzeniem kesdr. Szczegółowe informacje dotyczące zgłoszenia użytkownika są wyświetlane na zakładce **Szyfrowanie**.
10. Wykonaj jedną z poniższych czynności:

    - Aby wysłać do użytkownika wiadomość e-mail z wygenerowanym plikiem klucza, kliknij przycisk **Wyślij przez e-mail**.
    - Aby zapisać plik klucza dostępu dla zaszyfrowanego urządzenia i dostarczyć go do użytkownika za pomocą innej metody, kliknij przycisk **Zapisz**.

Udostępnianie użytkownikowi klucza odzyskiwania dla dysków twardych zaszyfrowanych funkcją BitLocker

W celu wysłania do użytkownika klucza odzyskiwania dla dysku systemowego zaszyfrowanego funkcją BitLocker:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej, w folderze **Zarządzane urządzenia** otwórz folder z nazwą grupy administracyjnej zawierającej komputer użytkownika, który żąda dostępu do zaszyfrowanego dysku.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Na zakładce **Urządzenia** zaznacz komputer należący do użytkownika, który żąda dostępu do zaszyfrowanego dysku.
5. Kliknij go prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Przydziel dostęp do urządzeń oraz danych w trybie offline**.

   Zostanie otwarte okno **Przydziel dostęp do urządzeń oraz danych w trybie offline**.
6. W oknie **Przydziel dostęp do urządzeń oraz danych w trybie offline** 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.
8. Wyślij do użytkownika klucz, który jest wskazany w polu **klucz odzyskiwania**.

W celu wysłania do użytkownika klucza odzyskiwania dla dysku niesystemowego zaszyfrowanego funkcją BitLocker:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz kolejno **Dodatkowe → Ochrona i szyfrowanie danych → Zaszyfrowane urządzenia**.

   W obszarze roboczym wyświetlana jest lista zaszyfrowanych urządzeń.
3. W obszarze roboczym wybierz zaszyfrowane urządzenie, do którego dostęp chcesz odzyskać.
4. Kliknij je prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Uzyskaj klucz dostępu do określonego zaszyfrowanego urządzenia**.

   Zostanie otwarte okno **Przywróć dostęp do dysku zaszyfrowanego funkcją BitLocker**.
5. 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.

6. Wyślij do użytkownika klucz, który jest wskazany w polu **klucz odzyskiwania**.

Tworzenie pliku wykonywalnego Narzędzia przywracania zaszyfrowanego urządzenia

Instrukcje te są przeznaczone dla użytkowników komputerów klienckich z zainstalowanym Kaspersky Endpoint Security.

W celu utworzenia pliku wykonywalnego Narzędzia przywracania zaszyfrowanego urządzenia:

1. Otwórz okno główne aplikacji.
2. Kliknij przycisk znajdujący się w lewym dolnym rogu okna głównego aplikacji, aby otworzyć okno **Wsparcie użytkownika**.
3. W oknie **Wsparcie użytkownika** kliknij przycisk **Przywróć zaszyfrowane urządzenie**.

   Zostanie uruchomione Narzędzie do przywracania zaszyfrowanego urządzenia.
4. W oknie Narzędzia przywracania zaszyfrowanego urządzenia kliknij przycisk **Utwórz wersję autonomiczną**.

   Zostanie otwarte okno **Tworzenie autonomicznej wersji Narzędzia przywracania**.
5. W oknie **Zapisz w** wprowadź ręcznie ścieżkę do folderu zapisu pliku wykonywalnego Narzędzia przywracania zaszyfrowanego urządzenia lub kliknij przycisk **Przeglądaj**.
6. Kliknij **OK** w oknie **Tworzenie autonomicznej wersji Narzędzia przywracania**.

   Plik wykonywalny Narzędzia przywracania zaszyfrowanego urządzenia (fdert.exe) zostanie zapisany w wybranym folderze.

Przywracanie danych na zaszyfrowanych urządzeniach przy użyciu Narzędzia przywracania zaszyfrowanego urządzenia

Instrukcje te są przeznaczone dla użytkowników komputerów klienckich z zainstalowanym Kaspersky Endpoint Security.

W celu przywrócenia dostępu do zaszyfrowanego urządzenia przy użyciu Narzędzia przywracania zaszyfrowanego urządzenia:

1. Uruchom narzędzie przywracania zaszyfrowanego urządzenia na jeden z następujących sposobów:
   - Kliknij przycisk w oknie głównym aplikacji Kaspersky Endpoint Security, aby otworzyć okno **Wsparcie użytkownika**, w którym kliknij przycisk **Przywróć zaszyfrowane urządzenie**.
   - Uruchom plik wykonywalny fdert.exe Narzędzia przywracania zaszyfrowanego urządzenia. Ten plik jest tworzony przez Kaspersky Endpoint Security.

2. W oknie Narzędzia przywracania zaszyfrowanego urządzenia, z listy rozwijalnej **Wybierz urządzenie** wybierz zaszyfrowane urządzenie, do którego chcesz przywrócić dostęp.

3. Kliknij przycisk **Skanuj**, aby umożliwić narzędziu określenie akcji, jakie powinny zostać podjęte na urządzeniu: czy powinno zostać odblokowane, czy odszyfrowane.

   Jeśli komputer posiada dostęp do funkcji szyfrowania programu Kaspersky Endpoint Security, Narzędzie przywracania wyświetli okno z pytaniem o odblokowanie urządzenia. Mimo, że odblokowanie urządzenia nie odszyfrowuje go, w wyniku odblokowania urządzenie staje się bezpośrednio dostępne. Jeśli komputer nie posiada dostępu do funkcji szyfrowania programu Kaspersky Endpoint Security, Narzędzie przywracania wyświetli okno z pytaniem o odszyfrowanie urządzenia.

4. Kliknij przycisk **Napraw MBR**, jeśli diagnostyka zaszyfrowanego systemowego dysku twardego zwróciła wiadomość o problemach związanych z głównym rekordem rozruchowym (MBR) urządzenia.

   Naprawienie głównego rekordu rozruchowego urządzenia może przyśpieszyć proces zbierania informacji niezbędnych do odblokowywania lub deszyfrowania urządzenia.

5. W zależności od wyników diagnostyki kliknij przycisk **Odblokuj** lub **Odszyfruj**.

   Zostanie otwarte okno **Ustawienia odblokowania urządzenia** lub **Ustawienia deszyfrowania urządzeń**.

6. Jeśli chcesz odzyskać dane przy pomocy konta Agenta autoryzacji:

   a. Wybierz opcję **Użyj ustawień konta Agenta autoryzacji**.

   b. W polach **Nazwa** i **Hasło** określ dane uwierzytelniające konta 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.

7. Jeśli chcesz użyć klucza dostępu do przywrócenia danych:

   a. Wybierz opcję **Określ ręcznie klucz dostępu do urządzenia**.

   b. Kliknij przycisk **Pobierz klucz dostępu**.

   c. Zostanie otwarte okno **Pobierz klucz dostępu do urządzenia**.

   d. Kliknij przycisk **Zapisz** i wybierz folder, w którym ma być zapisany plik żądania dostępu z rozszerzeniem fdertc.

   e. 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.

   f. Pobierz i zapisz plik klucza dostępu, który został utworzony i dostarczony przez administratora firmowej sieci LAN.

   g. Kliknij przycisk **Wczytaj** i w otwartym oknie wybierz plik klucza dostępu z rozszerzeniem fdertr.

8. Jeśli odszyfrowujesz urządzenie, w oknie **Ustawienia deszyfrowania urządzeń** musisz także określić inne ustawienia deszyfrowania. W tym celu:

- Określ obszar deszyfrowania:
  - Jeśli chcesz odszyfrować całe urządzenie, zaznacz opcję **Odszyfruj całe urządzenie**.
  - Jeśli chcesz odszyfrować część danych na urządzeniu, zaznacz opcję **Odszyfruj określone obszary urządzenia** i użyj pól **Uruchom** i **Zakończone** do określenia granic obszaru deszyfrowania.
- Wybierz miejsce zapisu odszyfrowanych danych:
  - Jeśli chcesz, żeby dane na oryginalnym urządzeniu były nadpisane odszyfrowanymi danymi, odznacz pole **Zapisz dane do pliku po odszyfrowaniu**.
  - Jeśli chcesz zapisać odszyfrowane dane w innym miejscu niż oryginalne, zaszyfrowane dane, zaznacz pole **Zapisz dane do pliku po odszyfrowaniu** i użyj przycisku **Przeglądaj**, aby określić miejsce zapisu danych.

9. Kliknij **OK**.

Proces odblokowania / deszyfrowania urządzenia zostanie uruchomiony.

Odpowiedź na prośbę użytkownika o przywrócenie danych na zaszyfrowanych urządzeniach

W celu utworzenia pliku klucza dostępu do zaszyfrowanego urządzenia i przesłania go do użytkownika:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz kolejno **Dodatkowe** → **Ochrona i szyfrowanie danych** → **Zaszyfrowane urządzenia**.
3. W obszarze roboczym wybierz zaszyfrowane urządzenie, dla którego chcesz utworzyć plik klucza dostępu, a z menu kontekstowego urządzenia wybierz **Uzyskaj klucz dostępu do określonego zaszyfrowanego urządzenia**.

   Jeśli nie jesteś pewien, dla którego komputera został wygenerowany plik żądania dostępu, w drzewie Konsoli administracyjnej wybierz folder **Dodatkowe** → **Ochrona i szyfrowanie danych** i w obszarze roboczym kliknij odnośnik **Uzyskaj klucz szyfrowania urządzenia**.

   Zostanie otwarte okno **Zezwól na dostęp do urządzenia**.
4. Wybierz używany algorytm szyfrujący. W tym celu wybierz jedną z następujących opcji:
   - **AES256**, jeśli program Kaspersky Endpoint Security został zainstalowany z pakietu dystrybucyjnego znajdującego się w folderze aes256 na komputerze, na którym urządzenie zostało zaszyfrowane;
   - **AES56**, jeśli program Kaspersky Endpoint Security został zainstalowany z pakietu dystrybucyjnego znajdującego się w folderze aes56 na komputerze, na którym urządzenie zostało zaszyfrowane;
5. Kliknij przycisk **Przeglądaj**.

   Zostanie otwarte standardowe okno **Wybierz plik żądania dostępu** w Microsoft Windows.
6. W oknie **Wybierz plik żądania dostępu** określ ścieżkę dostępu do pliku zgłoszenia z rozszerzeniem fdertc, który otrzymałeś od użytkownika.

7. Kliknij przycisk **Otwórz**.

   Kaspersky Security Center generuje plik klucza dostępu z rozszerzeniem fdertr do zaszyfrowanego urządzenia.

8. Wykonaj jedną z poniższych czynności:

   - Aby wysłać do użytkownika wiadomość e-mail z wygenerowanym plikiem klucza, kliknij przycisk **Wyślij przez e-mail**.
   - Aby zapisać plik klucza dostępu dla zaszyfrowanego urządzenia i dostarczyć go do użytkownika za pomocą innej metody, kliknij przycisk **Zapisz**.

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 podczas szyfrowania danych.

   Dostęp do zaszyfrowanych danych zostanie nadany na tych samych warunkach, które zostały zastosowane przed awarią systemu operacyjnego.

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).

Ochrona sieci

Ta sekcja zawiera informacje o monitorowaniu ruchu sieciowego oraz instrukcje dotyczące sposobu skonfigurowania ustawień monitorowanych portów sieciowych.

Informacje o Ochronie sieci

Podczas działania programu Kaspersky Endpoint Security komponenty Ochrona poczty, Ochrona WWW i Ochrona komunikatorów monitorują strumienie danych, które są przesyłane poprzez określone protokoły i przechodzą przez otwarte porty TCP i UDP na Twoim komputerze. Na przykład, Ochrona poczty skanuje dane przesyłane przez SMTP, podczas gdy Ochrona WWW skanuje dane przesyłane przez HTTP i FTP.

Kaspersky Endpoint Security dzieli porty TCP i UDP systemu operacyjnego na kilka grup, w zależności od prawdopodobieństwa ich zagrożenia. Niektóre porty sieciowe zarezerwowane są dla usług, które mogą być podatne na atak. Zaleca się bardziej szczegółowe monitorowanie tych portów, ponieważ prawdopodobieństwo ich zaatakowania jest większe. 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. Ruch sieciowy takich portów i aplikacji będzie nadzorowany szczególnie dokładnie przez Ochronę poczty, Ochronę WWW i Ochronę komunikatorów.

Konfigurowanie ustawień monitorowania ruchu sieciowego

W celu skonfigurowania ustawień monitorowania ruchu sieciowego:

- Włącz monitorowanie wszystkich portów sieciowych.
- Utwórz listę monitorowanych portów sieciowych.
- Utwórz listę aplikacji, dla których monitorowane są wszystkie porty sieciowe.

Włączanie monitorowania wszystkich portów sieciowych

W celu włączenia monitorowania wszystkich portów sieciowych:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna wybierz sekcję **Ochrona antywirusowa**.
   W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.
3. W sekcji **Monitorowane porty** zaznacz **Monitoruj wszystkie porty sieciowe**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Tworzenie listy monitorowanych portów sieciowych

W celu utworzenia listy monitorowanych portów sieciowych:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna wybierz sekcję **Ochrona antywirusowa**.

   W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.
3. W sekcji **Monitorowane porty** zaznacz **Monitoruj tylko wybrane porty**.
4. 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.
5. Na liście portów sieciowych wykonaj następujące czynności:

   - Zaznacz pola obok tych portów sieciowych, które chcesz dodać do listy monitorowanych portów sieciowych.

     Domyślnie zaznaczone są pola obok wszystkich portów sieciowych znajdujących się w oknie **Porty sieciowe**.
   - Usuń zaznaczenie z pól obok tych portów sieciowych, które chcesz wykluczyć z listy monitorowanych portów sieciowych.
6. Jeśli post sieciowy nie jest wyświetlany na liście portów sieciowych, dodaj go w następujący sposób:

   a. Pod listą portów sieciowych kliknij odnośnik **Dodaj**, aby otworzyć okno **Port sieciowy**.

   b. Wprowadź numer portu sieciowego w polu **Port**.

   c. W polu **Opis** wprowadź nazwę portu.

   d. Kliknij **OK**.

      Okno **Port sieciowy** zostanie zamknięte. Nowo dodany port zostanie umieszczony na końcu listy.
7. W oknie **Porty sieciowe** kliknij **OK**.
8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

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, zaznacz pole **Monitoruj wszystkie porty sieciowe** w sekcji **Monitorowane porty** lub skonfiguruj monitorowanie wszystkich portów dla aplikacji, które nawiązują połączenie 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. Otwórz okno ustawień aplikacji.
2. W lewej części okna wybierz sekcję **Ochrona antywirusowa**.

   W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.
3. W sekcji **Monitorowane porty** zaznacz **Monitoruj tylko wybrane porty**.
4. Kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Porty sieciowe**.
5. Zaznacz pole **Monitoruj wszystkie porty dla określonych aplikacji**.
6. Na liście aplikacji, pod opcją **Monitoruj wszystkie porty dla określonych aplikacji** wykonaj następujące czynności:

   - Zaznacz pola obok nazw aplikacji, dla których chcesz monitorować wszystkie porty sieciowe.

     Domyślnie zaznaczone są pola obok wszystkich aplikacji znajdujących się w oknie **Porty sieciowe**.
   - Usuń zaznaczenia z pól obok nazw aplikacji, dla których nie chcesz monitorować wszystkich portów sieciowych.
7. Jeśli aplikacja nie znajduje się na liście aplikacji, dodaj ją w następujący sposób:

   a. Kliknij odnośnik **Dodaj** znajdujący się pod listą aplikacji i otwórz menu kontekstowe.

   b. Z otwartego menu wybierz sposób dodania aplikacji do listy aplikacji:

      - Aby wybrać aplikację z listy aplikacji zainstalowanych na komputerze, wybierz polecenie **Aplikacje**. Zostanie otwarte okno **Wybierz aplikację** umożliwiające określenie nazwy aplikacji.
      - Aby określić lokalizację pliku wykonywalnego aplikacji, wybierz polecenie **Przeglądaj**. Zostanie otwarte standardowe okno **Otwórz** z Microsoft Windows, w którym można określić nazwę pliku wykonywalnego aplikacji.

      Po wybraniu aplikacji zostanie otwarte okno **Aplikacja**.

   c. W polu **Nazwa** wprowadź nazwę wybranej aplikacji.

   d. Kliknij **OK**.

      Okno **Aplikacja** zostanie zamknięte. Dodana przez Ciebie aplikacja pojawi się na końcu listy aplikacji.
8. W oknie **Porty sieciowe** kliknij **OK**.
9. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Aktualizowanie baz danych i modułów aplikacji

Sekcja ta zawiera informacje o aktualizacji baz danych i modułów aplikacji, a także instrukcje dotyczące konfiguracji ustawień aktualizacji.

Informacje o aktualizacjach 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 określane automatycznie. Jeśli korzystasz z serwera proxy, konieczne może być dostosowanie ustawień połączenia.

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 wyświetlone są w **Aktualizacja**, w sekcji **Zadania**, na zakładce **Ochrona i kontrola** dostępnej w oknie głównym aplikacji.

Informacje o wynikach aktualizacji i wszystkich zdarzeniach zaistniałych podczas wykonywania zadania aktualizacji zapisywane są w raporcie Kaspersky Endpoint Security.

Informacje o źródłach 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.

Konfiguracja ustawień aktualizacji

Podczas konfiguracji ustawień aktualizacji możesz wykonać następujące czynności:

- Dodać nowe źródła uaktualnień.

  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.

  Jeżeli jako aktywne ustawiono kilka źródeł uaktualnień, Kaspersky Endpoint Security będzie podejmował próby nawiązywania połączenia z każdym z nich, począwszy od góry listy; uaktualnienia zostaną pobrane z pierwszego dostępnego źródła.

  > Jeśli jako źródło uaktualnień wybrałeś zasób znajdujący się poza siecią LAN, do wykonywania aktualizacji niezbędne jest połączenie internetowe.

- Wybrać region serwera aktualizacji Kaspersky.

  Jeżeli jako źródła uaktualnień używasz serwerów aktualizacji Kaspersky, możesz wybrać lokalizację serwera aktualizacji Kaspersky, z którego pobierane będą pakiety aktualizacyjne. Serwery aktualizacji Kaspersky znajdują się w kilku krajach. Korzystanie z najbliżej położonych serwerów aktualizacji Kaspersky pozwala zmniejszyć czas potrzebny na pobranie pakietu aktualizacji.

  Domyślnie aplikacja korzysta z informacji o bieżącej lokalizacji pobranych z rejestru systemu operacyjnego.

- Skonfigurować pobieranie uaktualnień programu Kaspersky Endpoint Security z foldera współdzielonego.

  Aby zaoszczędzić ruch internetowy, możesz skonfigurować pobieranie uaktualnień programu Kaspersky Endpoint Security z folderu współdzielonego podczas aktualizowania aplikacji na komputerach w sieci LAN. W tym celu jeden z komputerów w sieci LAN odbiera aktualny pakiet aktualizacji z serwera Kaspersky Security Center lub serwerów aktualizacji Kaspersky i kopiuje go do folderu współdzielonego. Następnie pozostałe komputery w sieci LAN pobierają pakiet uaktualnień z tego folderu współdzielonego.

- Wybrać tryb 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.

- Skonfigurować uruchamianie zadania aktualizacji z poziomu konta innego użytkownika.

Dodawanie źródła uaktualnień

W celu dodania źródła uaktualnień:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz **Aktualizacja**.
   W prawej części okna wyświetlane są ustawienia aktualizacji aplikacji.
3. W sekcji **Tryb uruchamiania i źródło uaktualnień** kliknij przycisk **Źródło uaktualnień**.
   Ten przycisk otwiera zakładkę **Źródło** w oknie **Aktualizacja**.
4. Na zakładce **Źródło** kliknij przycisk **Dodaj**.
   Zostanie otwarte okno **Wybierz źródło uaktualnień**.
5. W oknie **Wybierz źródło uaktualnień** należy wybrać folder z pakietem uaktualnień lub wprowadzić jego pełną ścieżkę dostępu w polu **Źródło**.
6. Kliknij **OK**.
7. W oknie **Aktualizacja** kliknij **OK**.
8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Wybieranie regionu serwera aktualizacji

W celu wybrania regionu serwera aktualizacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz **Aktualizacja**.
   W prawej części okna wyświetlane są ustawienia aktualizacji aplikacji.
3. W sekcji **Tryb uruchamiania i źródło uaktualnień** kliknij przycisk **Źródło uaktualnień**.
   Ten przycisk otwiera zakładkę **Źródło** w oknie **Aktualizacja**.
4. Na zakładce **Źródło**, w sekcji **Ustawienia regionalne** wybierz **Wybierz z listy**.
5. Z listy rozwijalnej wybierz kraj znajdujący się najbliżej Twojego miejsca zamieszkania.
6. Kliknij **OK**.
7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Konfigurowanie aktualizacji z foldera współdzielonego

Konfigurowanie aktualizacji Kaspersky Endpoint Security z foldera współdzielonego składa się z następujących kroków:

1. Włączenia kopiowania pakietu uaktualnień do foldera współdzielonego na jednym z komputerów w sieci lokalnej.
2. Konfigurowania pobierania uaktualnień Kaspersky Endpoint Security ze wskazanego foldera współdzielonego na pozostałe komputery w sieci lokalnej.

W celu włączenia kopiowanie pakietu uaktualnień do foldera współdzielonego:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz **Aktualizacja**.

   W prawej części okna wyświetlane są ustawienia aktualizacji aplikacji.
3. W sekcji **Dodatkowe** zaznacz pole **Kopiuj uaktualnienia do foldera**.
4. Określ ścieżkę dostępu do foldera współdzielonego, do którego będą kopiowane uaktualnienia. Możesz to zrobić w jeden z następujących sposobów:
   - Wprowadź ścieżkę dostępu do foldera współdzielonego w polu znajdującym się pod opcją **Kopiuj uaktualnienia do foldera**.
   - Kliknij przycisk **Przeglądaj**. Następnie, w oknie **Wybierz folder**, które zostanie otwarte, wybierz żądany folder i kliknij **OK**.
5. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

W celu skonfigurowania pobieranie uaktualnień programu Kaspersky Endpoint Security z foldera współdzielonego:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz **Aktualizacja**.

   W prawej części okna wyświetlane są ustawienia aktualizacji aplikacji.
3. W sekcji **Tryb uruchamiania i źródło uaktualnień** kliknij przycisk **Źródło uaktualnień**.

   Ten przycisk otwiera zakładkę **Źródło** w oknie **Aktualizacja**.
4. Na zakładce **Źródło** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Wybierz źródło uaktualnień**.
5. W oknie **Wybierz źródło uaktualnień** należy wybrać folder współdzielony zawierający pakiet uaktualnień lub wprowadzić jego pełną ścieżkę dostępu w polu **Źródło**.
6. Kliknij **OK**.
7. Na zakładce **Źródło** usuń zaznaczenia z pól obok nazw źródeł uaktualnień, których nie określiłeś jako folder współdzielony.
8. Kliknij **OK**.

9. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Wybieranie trybu uruchamiania zadania aktualizacji

W celu wybrania trybu uruchamiania zadania aktualizacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz **Aktualizacja**.

   W prawej części okna wyświetlane są ustawienia aktualizacji aplikacji.
3. Kliknij przycisk **Tryb uruchamiania**.

   Zostanie otwarte okno **Aktualizacja** na zakładce **Tryb uruchamiania**.
4. W sekcji **Tryb uruchamiania** wybierz jedną z następujących opcji 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 **Zgodnie z terminarzem**.
5. Wykonaj jedną z poniższych czynności:

   - Jeżeli wybrałeś opcję **Automatycznie** lub **Ręcznie**, przejdź do kroku 6 niniejszej instrukcji.
   - Jeżeli wybrałeś opcję **Zgodnie z terminarzem**, określ ustawienia terminarza uruchamiania zadania aktualizacji. W tym celu:

     a. Z listy rozwijalnej **Częstotliwość** wybierz czas uruchamiania aktualizacji. Wybierz jedną z następujących opcji: **Minuty**, **Godziny**, **Dni**, **Co tydzień**, **O określonym czasie**, **Co miesiąc** lub **Po uruchomieniu aplikacji**.

     b. W zależności od opcji wybranej na liście **Częstotliwość** określ wartości dla ustawień, które definiują czas uruchamiania zadania aktualizacji.

     c. W polu **Odrocz uruchomienie zadania na** określ czas, na jaki odroczone zostanie uruchomienie zadania aktualizacji po uruchomieniu Kaspersky Endpoint Security.

     > Jeżeli z listy rozwijalnej **Częstotliwość** wybrano opcję **Po uruchomieniu aplikacji**, pole **Odrocz uruchomienie zadania na** nie będzie dostępne.

     d. Jeżeli chcesz, aby Kaspersky Endpoint Security uruchamiał pominięte zadania aktualizacji, zaznacz pole **Uruchom pominięte zadania**.

     > Jeżeli z listy rozwijalnej **Częstotliwość** wybrano opcję **Godziny**, **Minuty** lub **Po uruchomieniu aplikacji**, pole **Uruchom pominięte zadania** nie będzie dostępne.

6. Kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

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 brak uprawnień autoryzowanego użytkownika serwera 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. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz **Aktualizacja**.

   W prawej części okna wyświetlane są ustawienia aktualizacji aplikacji.

3. W sekcji **Tryb uruchamiania i źródło uaktualnień** kliknij przycisk **Tryb uruchamiania**.

   Zostanie otwarte okno **Aktualizacja** na zakładce **Tryb uruchamiania**.

4. Na zakładce **Tryb uruchamiania**, w sekcji **Użytkownik** zaznacz pole **Uruchom zadanie jako**.

5. W polu **Nazwa** wprowadź nazwę konta użytkownika, którego uprawnienia są niezbędne do uzyskania dostępu do źródła uaktualnień.

6. W polu **Hasło** wprowadź hasło użytkownika, którego uprawnienia są niezbędne do uzyskania dostępu do źródła uaktualnień.

7. Kliknij **OK**.

8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Konfigurowanie aktualizacji modułów aplikacji

W celu skonfigurowania aktualizacji modułów aplikacji:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz **Aktualizacja**.

   W prawej części okna wyświetlane są ustawienia aktualizacji aplikacji.

3. W sekcji **Dodatkowe** należy wykonać jedną z następujących czynności:

- Jeśli chcesz, żeby aplikacja uwzględniała uaktualnienia modułów aplikacji w pakietach aktualizacji, zaznacz pole **Pobierz aktualizacje składników aplikacji**.
- Jeśli nie chcesz, żeby taka sytuacja miała miejsce, odznacz pole **Pobierz aktualizacje składników aplikacji**.

4. Jeśli w poprzednim kroku zaznaczono pole **Pobierz aktualizacje składników aplikacji**, określ warunki, pod jakimi aplikacja zainstaluje aktualizacje modułów:
   - Zaznacz pole **Instaluj krytyczne i zatwierdzone aktualizacje**, jeśli aplikacja ma automatycznie instalować krytyczne uaktualnienia modułów, a także inne uaktualnienia po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub przy pomocy Kaspersky Security Center.
   - Zaznacz pole **Instaluj tylko zatwierdzone aktualizacje**, jeśli aplikacja ma instalować uaktualnienia modułów po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub przy pomocy Kaspersky Security Center.
5. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

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.

Aby pobrać pakiet aktualizacji z serwerów Kaspersky, niezbędne jest połączenie internetowe.

W celu uruchomienia lub zatrzymania zadania aktualizacji:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Zadania**.

   Zostanie otwarta sekcja **Zadania**.
4. Kliknij prawym przyciskiem myszy wiersz z nazwą zadania aktualizacji.

   Zostanie otwarte menu wyboru akcji podejmowanych na zadaniu aktualizacji.
5. Wykonaj jedną z poniższych czynności:
   - Jeżeli chcesz uruchomić zadanie, wybierz z menu **Uruchom aktualizację**.

     Stan postępu zadania aktualizacji, wyświetlany po prawej stronie przycisku **Aktualizacja**, zmieni się na *Uruchomiono*.
   - Jeżeli chcesz zatrzymać zadanie, wybierz z menu **Zatrzymaj aktualizację**.

     Stan postępu zadania aktualizacji, wyświetlany po prawej stronie przycisku **Aktualizacja**, zmieni się na *Zatrzymano*.

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. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Zadania**.
   Zostanie otwarta sekcja **Zadania**.
4. Kliknij prawym przyciskiem myszy zadanie **Aktualizacja**, aby otworzyć menu kontekstowe.
5. Wybierz **Wycofaj aktualizację**.

Konfigurowanie ustawień serwera proxy

W celu skonfigurowania ustawień serwera proxy:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz **Aktualizacja**.
   W prawej części okna wyświetlane są ustawienia aktualizacji aplikacji.
3. W sekcji **Serwer proxy** kliknij przycisk **Ustawienia**.
   Zostanie otwarte okno **Ustawienia serwera proxy**.
4. W oknie **Ustawienia serwera proxy** zaznacz pole **Użyj serwera proxy**.
5. Określ ustawienia serwera proxy.
6. Kliknij **OK**.
7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Ustawienia serwera proxy można skonfigurować także w oknie głównym aplikacji, na zakładce **Ustawienia**, w sekcji **Ustawienia zaawansowane**.

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.

Sekcja ta opisuje właściwości oraz ustawienia zadań skanowania, poziomy ochrony, metody i technologie skanowania, a także instrukcje dotyczące działań wykonywanych na plikach, które nie zostały przetworzone przez program Kaspersky Endpoint Security podczas skanowania antywirusowego.

Informacje o zadaniach skanowania

Do wykrywania wirusów i innych typów szkodliwego oprogramowania oraz do sprawdzania integralności modułów aplikacji Kaspersky Endpoint Security wykorzystuje następujące zadania:

- **Pełne skanowanie**. Skanowanie szczegółowe całego komputera. Domyślnie 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
- **Skanowanie obszarów krytycznych**. Domyślnie, Kaspersky Endpoint Security skanuje pamięć jądra, uruchomione procesy i sektory startowe dysku.
- **Skanowanie obiektów**. Kaspersky Endpoint Security skanuje obiekty wybrane przez użytkownika. Możesz skanować każdy obiekt z poniższej listy:
  - Pamięć jądra
  - Obiekty uruchamiane wraz ze startem systemu operacyjnego
  - Kopię zapasową systemu operacyjnego
  - Skrzynkę odbiorczą programu Outlook
  - Wszystkie dyski twarde, wymienne i sieciowe
  - Dowolny wybrany plik
- **Sprawdzanie integralności**. Kaspersky Endpoint Security sprawdza, czy moduły aplikacji nie są uszkodzone lub zmodyfikowane.

Zadania Pełnego skanowania i Skanowania obszarów krytycznych nieco różnią się od innych zadań. Dla tych zadań nie zaleca się modyfikowania obszaru skanowania.

Po uruchomieniu zadań skanowania, ich postęp jest wyświetlany w polu obok nazwy uruchomionego zadania, w sekcji **Zadania** dostępnej w oknie głównym aplikacji Kaspersky Endpoint Security, na zakładce **Ochrona i kontrola**.

Informacje o wynikach skanowania oraz o zdarzeniach zaistniałych podczas wykonywania tego zadania zostają zapisane w raporcie Kaspersky Endpoint Security.

Uruchamianie i zatrzymywanie zadania skanowania

Bez względu na wybrany tryb uruchamiania zadania skanowania, możesz uruchomić lub zatrzymać zadanie w dowolnym momencie.

W celu uruchomienia lub zatrzymania zadania skanowania:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Zadania**.

   Zostanie otwarta sekcja **Zadania**.
4. Kliknij prawym przyciskiem myszy wiersz z nazwą zadania skanowania.

   Zostanie otwarte menu wyboru akcji podejmowanych na zadaniu skanowania.
5. Wykonaj jedną z poniższych czynności:

   - Jeżeli chcesz uruchomić zadanie, wybierz z menu **Uruchom skanowanie**.

     Stan postępu zadania, wyświetlany po prawej stronie przycisku z nazwą zadania skanowania, zmieni się na *Uruchomiono*.
   - Jeżeli chcesz zatrzymać zadanie, wybierz z menu **Zatrzymaj skanowanie**.

     Stan postępu zadania, wyświetlany po prawej stronie przycisku z nazwą zadania skanowania, zmieni się na *Zatrzymano*.

Konfigurowanie ustawień zadania skanowania

Podczas konfigurowania ustawień zadania skanowania można:

- Zmienić poziom ochrony.

  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.
- Zmienić akcję podejmowaną przez Kaspersky Endpoint Security po wykryciu zainfekowanego pliku.
- Zmodyfikować obszar skanowania.

  Możesz poszerzyć lub ograniczyć obszar skanowania, dodając bądź usuwając skanowane obiekty lub zmieniając typ skanowanych plików.
- Zoptymalizować skanowanie.

Możesz zoptymalizować skanowanie plików, zmniejszając czas skanowania i zwiększając szybkość działania programu Kaspersky Endpoint Security. Można to uzyskać poprzez skanowanie tylko nowych plików i tych plików, które zostały zmodyfikowane od ostatniego skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych. Możesz również ustawić ograniczenie skanowania pojedynczego pliku. Po upłynięciu określonego czasu, obiekt zostanie wykluczony z bieżącego skanowania (poza archiwami i plikami zawierającymi wiele obiektów).

Możesz także włączyć korzystanie z technologii iChecker i iSwift. Optymalizują one prędkość skanowania plików poprzez wykluczenie plików, które nie zostały zmodyfikowane od ostatniego skanowania.

- Skonfigurować skanowanie plików złożonych.
- Skonfigurować używanie metod skanowania.

  Gdy program Kaspersky Endpoint Security jest aktywny, używa analizy sygnatur. Podczas analizy sygnatur Kaspersky Endpoint Security porównuje wykryty obiekt z wpisami w swojej bazie danych. Zgodnie z zaleceniami ekspertów z Kaspersky, analiza sygnatur jest zawsze włączona.

  Aby zwiększyć efektywność ochrony, możesz użyć analizy heurystycznej. Podczas analizy heurystycznej Kaspersky Endpoint Security analizuje aktywność obiektów w systemie operacyjnym. Analiza heurystyczna może wykryć szkodliwe obiekty, dla których nie ma wpisów w bazach danych Kaspersky Endpoint Security.
- Wybrać tryb uruchamiania zadania skanowania.

  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.

  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 skanowania. Zadanie skanowania może zostać uruchomione dopiero po minięciu określonego czasu od uruchomienia programu Kaspersky Endpoint Security.
- Skonfigurować uruchamianie zadania skanowania z poziomu konta innego użytkownika.
- Określ ustawienia skanowania napędów wymiennych po ich podłączeniu.

Zmienianie poziomu ochrony

Podczas skanowania Kaspersky Endpoint Security używa rożnych kombinacji ustawień. Te kombinacje ustawień zapisywane w aplikacji są nazywane *poziomami ochrony*. Dostępne są trzy predefiniowane poziomy ochrony: **Wysoki**, **Zalecany** i **Niski**. Ustawienia **Zalecany** poziomu ochrony są uznawane za optymalne. Ten poziom jest zalecany przez ekspertów z Kaspersky.

W celu zmiany poziomu ochrony:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz podsekcję z nazwą żądanego zadania skanowania (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie obiektów**).

   W prawej części okna wyświetlone są ustawienia wybranego zadania skanowania.
3. W sekcji **Poziom ochrony** wykonaj jedną z poniższych czynności:

   - Jeśli chcesz zastosować jeden z predefiniowanych poziomów ochrony (**Wysoki**, **Zalecany** lub **Niski**), wybierz go, korzystając z suwaka.

- Jeżeli chcesz skonfigurować niestandardowy poziom ochrony, kliknij przycisk **Ustawienia** i w otwartym oknie określ ustawienia wraz z nazwą zadania skanowania.

  Po skonfigurowaniu niestandardowego poziomu ochrony, nazwa poziomu ochrony w sekcji **Poziom ochrony** zmieni się na **Niestandardowy**.

- Jeżeli chcesz zmienić poziom ochrony na **Zalecany**, kliknij przycisk **Domyślny**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zmienianie akcji podejmowanej na zainfekowanych plikach

W celu zmiany akcji podejmowanej na zainfekowanych plikach:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz podsekcję z nazwą żądanego zadania skanowania (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie obiektów**).

   W prawej części okna wyświetlone są ustawienia wybranego zadania skanowania.

3. W sekcji **Działanie podejmowane w przypadku wykrycia zagrożenia** wybierz żądaną opcję:

   - **Automatycznie wybierz akcję**.

   - **Wybierz akcję**.

4. Jeśli w poprzednim kroku wybrałeś opcję **Wybierz akcję**, zaznacz następujące pola:

   - Jeśli chcesz, żeby Kaspersky Endpoint Security leczył obiekty, w których zostały wykryte zagrożenia, zaznacz **Wykonaj leczenie**.

     Nawet jeśli wybrano tę opcję, Kaspersky Endpoint Security zastosuje akcję **Usuń** dla plików będących częścią aplikacji ze Sklepu Windows.

   - Jeśli chcesz, żeby Kaspersky Endpoint Security usuwał obiekty, w których zostały wykryte zagrożenia, zaznacz **Usuń**.

   - Jeśli chcesz, żeby Kaspersky Endpoint Security próbował wyleczyć obiekty, w których zostały wykryte zagrożenia, i usuwał obiekty, których nie może wyleczyć, zaznacz oba pola (**Wykonaj leczenie** i **Usuń**).

   - Jeśli nie chcesz, aby Kaspersky Endpoint Security podejmował jakiekolwiek działanie na obiektach, w których zostały wykryte zagrożenia, a zamiast tego powiadamiał użytkownika o wynikach skanowania tych obiektów, odznacz oba pola (**Wykonaj leczenie** i **Usuń**).

5. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Tworzenie listy skanowanych obiektów

W celu wygenerowania listy skanowanych obiektów możesz użyć jednej z następujących metod:

- W oknie głównym aplikacji, na zakładce**Ochrona i kontrola**
- Z poziomu okna ustawień aplikacji

> Ta metoda jest dostępna tylko dla zadań **Pełne skanowanie** i **Skanowanie obszarów krytycznych**. Lista skanowanych obiektów dla zadania **Skanowanie obiektów** może zostać utworzona na zakładce **Ochrona i kontrola**.

W celu utworzenia listy skanowanych obiektów w oknie głównym aplikacji, na zakładce Ochrona i kontrola:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Zadania**.
   Zostanie otwarta sekcja **Zadania**.
4. Kliknij nazwę zadania prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Obszar skanowania**.
   Zostanie otwarte okno **Obszar skanowania**.
5. Jeśli chcesz dodać nowy obiekt do obszaru skanowania:
   a. Kliknij przycisk **Dodaj**.
      Zostanie otwarte okno **Określ obszar skanowania**.
   b. Wybierz obiekt i kliknij **Dodaj**.
      Wszystkie obiekty wybrane w oknie **Określ obszar skanowania** są wyświetlane na liście **Obszar skanowania**.
   c. Kliknij **OK**.
6. Jeśli chcesz zmienić ścieżkę dostępu do obiektu w obszarze skanowania:
   a. Wybierz obiekt w obszarze skanowania.
   b. Kliknij przycisk **Modyfikuj**.
      Zostanie otwarte okno **Określ obszar skanowania**.
   c. Wprowadź nową ścieżkę dostępu do obiektu w obszarze skanowania.
   d. Kliknij **OK**.
7. Jeśli chcesz usunąć obiekt z obszaru skanowania:
   a. Wybierz obiekt, który chcesz usunąć z obszaru skanowania.
      W przypadku, gdy chcesz wybrać więcej obiektów, zaznacz je, trzymając wciśnięty klawisz **CTRL**.
   b. Kliknij przycisk **Usuń**.
      Zostanie wyświetlone okno potwierdzenia usunięcia obiektu.
   c. W oknie z potwierdzeniem usunięcia obiektu kliknij **Tak**.

Obiekty, które domyślnie znajdują się w obszarze skanowania, nie mogą zostać zmodyfikowane ani usunięte.

8. Aby wykluczyć obiekt z obszaru skanowania, w oknie **Obszar skanowania** usuń zaznaczenie z pola znajdującego się obok tego obiektu.

   Obiekt zostaje wykluczony ze skanowania, ale nadal znajduje się na liście w obszarze skanowania.

9. Kliknij **OK**.

10. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

W celu utworzenia listy skanowanych obiektów z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz podsekcję z nazwą żądanego zadania skanowania: **Pełne skanowanie** lub **Skanowanie obszarów krytycznych**.

   W prawej części okna wyświetlone są ustawienia wybranego zadania skanowania.

3. Kliknij przycisk **Obszar skanowania**.

   Zostanie otwarte okno **Obszar skanowania**.

4. Utwórz listę skanowanych obiektów zgodnie z krokami 5-10 poprzedniej instrukcji.

Wybieranie typu skanowanych plików

W celu wybrania typu skanowanych plików możesz skorzystać z następujących metod:

- W oknie głównym aplikacji, na zakładce**Ochrona i kontrola**
- Z poziomu okna ustawień aplikacji

Ta metoda jest dostępna tylko dla zadań **Pełne skanowanie** i **Skanowanie obszarów krytycznych**. Typy skanowanych plików dla zadania **Skanowanie obiektów** mogą zostać wybrane tylko na zakładce **Ochrona i kontrola**.

W celu wybrania typu skanowanych plików na zakładce Ochrona i Kontrola okna głównego aplikacji:

1. Otwórz okno główne aplikacji.

2. Wybierz zakładkę **Ochrona i kontrola**.

3. Kliknij sekcję **Zadania**.

   Zostanie otwarta sekcja **Zadania**.

4. Kliknij nazwę zadania prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Ustawienia**.

   Zostanie otwarte okno z nazwą wybranego zadania skanowania.

5. W oknie z nazwą wybranego zadania skanowania wybierz zakładkę **Zakres**.

6. W sekcji **Typy plików** określ typy plików, które mają być skanowane:

   - Jeżeli skanowane mają być wszystkie pliki, zaznacz pole **Wszystkie pliki**.
   - Jeżeli skanowaniu mają podlegać pliki o formatach najbardziej podatnych na infekcje, wybierz opcję **Pliki skanowane według formatu**.
   - Jeżeli skanowaniu mają podlegać pliki z rozszerzeniami najbardziej podatnymi na infekcje, zaznacz pole **Pliki skanowane według rozszerzenia**.

   Podczas wybierania typu skanowanych plików należy pamiętać, że:

   - Istnieją formaty plików (takie jak TXT), dla których prawdopodobieństwo zarażenia szkodliwym kodem i jego późniejszej aktywacji jest niskie. Istnieją jednak formaty zawierające lub mogące zawierać kod wykonywalny (na przykład .exe, .dll, .doc). Ryzyko przeniknięcia i aktywacji szkodliwego kodu w takich plikach jest wysokie.
   - Haker może przesłać na Twój komputer wirusa lub inne szkodliwe oprogramowanie 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, Ochrona plików analizuje nagłówek pliku niezależnie od rozszerzenia. Jeśli analiza wykaże, że plik posiada format EXE, aplikacja przeskanuje go.

7. W oknie z nazwą zadania skanowania kliknij **OK**.

8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

W celu wybrania typu skanowanych plików z poziomu okna ustawień aplikacji:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz podsekcję z nazwą żądanego zadania skanowania: **Pełne skanowanie** lub **Skanowanie obszarów krytycznych**.

   W prawej części okna wyświetlone są ustawienia wybranego zadania skanowania.

3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno z nazwą wybranego zadania skanowania.

4. W oknie z nazwą wybranego zadania skanowania wybierz zakładkę **Zakres**.

5. Wykonaj kroki 5-7 z poprzednich instrukcji.

Optymalizowanie skanowania plików

W celu zoptymalizowania skanowania plików:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz podsekcję z nazwą żądanego zadania skanowania (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie obiektów**).

   W prawej części okna wyświetlone są ustawienia wybranego zadania skanowania.

3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno z nazwą wybranego zadania skanowania.

4. W otwartym oknie wybierz zakładkę **Zakres**.

5. W sekcji **Optymalizacja skanowania** wykonaj następujące czynności:

   - Zaznacz pole **Skanuj tylko nowe i zmienione pliki**.

   - Zaznacz pole **Pomiń pliki skanowane dłużej niż** i określ czas skanowania dla pojedynczego pliku (w sekundach).

6. Kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

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.

W celu skonfigurowania skanowania plików złożonych:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz podsekcję z nazwą żądanego zadania skanowania (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie obiektów**).

   W prawej części okna wyświetlone są ustawienia wybranego zadania skanowania.

3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno z nazwą wybranego zadania skanowania.

4. W otwartym oknie wybierz zakładkę **Zakres**.

5. W sekcji **Skanowanie plików złożonych** określ, które pliki złożone mają być skanowane: archiwa, pakiety instalacyjne, pliki w formatach pakietu Office, pliki formatów pocztowych lub archiwa chronione hasłem.

6. Jeśli pole **Skanuj tylko nowe i zmienione pliki** jest odznaczone w sekcji **Optymalizacja skanowania**, kliknij odnośnik **wszystkie / nowe** obok nazwy typu pliku złożonego, jeśli dla każdego typu pliku złożonego chcesz określić, czy mają być skanowane wszystkie pliki tego typu lub tylko nowe pliki tego typu.

   Po kliknięciu odnośnika zmieni on swoją wartość.

   Jeżeli pole **Skanuj tylko nowe i zmienione pliki** jest zaznaczone, skanowane są tylko nowe pliki.

7. Kliknij przycisk **Dodatkowe**.

   Zostanie otwarte okno **Pliki złożone**.

8. W sekcji **Ograniczenie rozmiaru** wykonaj jedną z poniższych czynności:

   - Jeżeli nie chcesz, aby duże pliki złożone były rozpakowywane, zaznacz pole **Nie rozpakowuj dużych plików złożonych** i określ żądaną wartość w polu **Maksymalny rozmiar pliku**.

- Jeżeli chcesz, aby duże pliki złożone były rozpakowywane bez względu na ich rozmiar, usuń zaznaczenie z pola **Nie rozpakowuj dużych plików złożonych**.

Kaspersky Endpoint Security skanuje duże pliki wypakowane z archiwów bez względu na to, czy pole **Nie rozpakowuj dużych plików złożonych** jest zaznaczone.

9. Kliknij **OK**.
10. W oknie z nazwą zadania skanowania kliknij przycisk **OK**.
11. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Używanie metod skanowania

W celu użycia metody skanowania:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz podsekcję z nazwą żądanego zadania skanowania (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie obiektów**).

   W prawej części okna wyświetlone są ustawienia wybranego zadania skanowania.
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno z nazwą wybranego zadania skanowania.
4. W otwartym oknie wybierz zakładkę **Dodatkowe**.
5. Jeżeli chcesz, aby podczas skanowania aplikacja wykorzystywała analizę heurystyczną, w sekcji **Metody skanowania**zaznacz pole Analiza heurystyczna. Następnie użyj suwaka, aby ustawi poziom analizy heurystycznej: **Niski**, **Średni** lub **Szczegółowy**.
6. Kliknij **OK**.
7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Używanie technologii skanowania

W celu użycia technologii skanowania:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz podsekcję z nazwą żądanego zadania skanowania (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie obiektów**).

   W prawej części okna wyświetlone są ustawienia wybranego zadania skanowania.
3. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno z nazwą wybranego zadania skanowania.

4. W otwartym oknie wybierz zakładkę **Dodatkowe**.

5. W sekcji **Technologie skanowania** zaznacz pola obok nazwy technologii, której chcesz użyć podczas skanowania.

6. Kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Wybieranie trybu uruchamiania dla zadania skanowania

W celu wybrania trybu uruchamiania zadania skanowania:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz podsekcję z nazwą żądanego zadania (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie obiektów**).

   W prawej części okna wyświetlone są ustawienia wybranego zadania skanowania.

3. Kliknij przycisk **Tryb uruchamiania**.

   Okno z właściwościami wybranego zadania zostanie otwarte na zakładce **Tryb uruchamiania**.

4. W sekcji **Tryb uruchamiania** wybierz tryb uruchamiania zadania: **Ręcznie** lub **Zgodnie z terminarzem**.

5. Jeśli wybierzesz opcję **Zgodnie z terminarzem**, określ ustawienia terminarza. W tym celu:

   a. Z listy rozwijalnej **Częstotliwość** wybierz częstotliwość uruchamiania zadania (**Minuty**, **Godziny**, **Dni**, **Co tydzień**, **O określonym czasie**, **Co miesiąc**, lub **Po uruchomieniu aplikacji**, **Po każdej aktualizacji**).

   b. W zależności od wybranej częstotliwości, skonfiguruj ustawienia zaawansowane, które określają terminarz uruchamiania zadania.

   c. Jeżeli chcesz, aby Kaspersky Endpoint Security uruchamiał pominięte zadania skanowania, zaznacz pole **Uruchom pominięte zadania**.

   > Jeżeli z listy rozwijalnej **Częstotliwość** wybrano opcję **Minuty**, **Godziny**, **Po uruchomieniu aplikacji** lub **Po każdej aktualizacji**, pole **Uruchom pominięte zadania** nie będzie dostępne.

   a. Jeżeli chcesz, aby Kaspersky Endpoint Security zawieszał wykonywanie zadania, gdy ograniczone są zasoby komputera, zaznacz opcję **Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności**.

   Ta opcja terminarza pozwala zaoszczędzić zasoby komputera.

6. Kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Uruchamianie zadania skanowania z poziomu konta innego użytkownika

Domyślnie zadanie skanowania jest uruchamiane z poziomu konta, na które użytkownik zalogował się w systemie operacyjnym. Jednak może zaistnieć potrzeba uruchomienia zadania z poziomu konta innego użytkownika. Możesz wskazać użytkownika, który posiada odpowiednie uprawnienia, w ustawieniach zadania skanowania i uruchamiać skanowanie z poziomu konta tego użytkownika.

W celu skonfigurowania uruchamiania zadania skanowania z poziomu konta innego użytkownika:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz podsekcję z nazwą żądanego zadania (**Pełne skanowanie**, **Skanowanie obszarów krytycznych** lub **Skanowanie obiektów**).

   W prawej części okna wyświetlone są ustawienia wybranego zadania skanowania.
3. Kliknij przycisk **Tryb uruchamiania**.

   Zostanie otwarte okno z właściwościami wybranego zadania na zakładce **Tryb uruchamiania**.
4. Na zakładce **Tryb uruchamiania**, w sekcji **Użytkownik** zaznacz pole **Uruchom zadanie jako**.
5. W polu **Nazwa** wprowadź nazwę konta użytkownika, którego uprawnienia są niezbędne do uruchomienia zadania skanowania.
6. W polu **Hasło** wprowadź hasło użytkownika, którego uprawnienia są niezbędne do uruchomienia zadania skanowania.
7. Kliknij **OK**.
8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Skanowanie napędów wymiennych po ich podłączeniu do komputera

Niektóre szkodliwe programy wykorzystują luki systemu operacyjnego do rozprzestrzeniania się poprzez sieci lokalne i nośniki wymienne. Kaspersky Endpoint Security umożliwia skanowanie nośników wymiennych podłączanych do komputera w poszukiwaniu wirusów i innych szkodliwych programów.

W celu skonfigurowania skanowania napędów wymiennych po ich podłączeniu:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna wybierz sekcję **Zadania zaplanowane**.

   W prawej części okna zostaną wyświetlone ustawienia zadania.
3. W sekcji **Skanowanie napędów wymiennych po ich podłączeniu**, z listy rozwijalnej **Akcja po podłączeniu nośnika wymiennego** wybierz żądaną akcję:

   - **Nie skanuj**
   - **Skanowanie Szczegółowe**

     W tym trybie Kaspersky Endpoint Security skanuje wszystkie pliki znajdujące się na nośniku wymiennym, w tym pliki zawierające obiekty złożone.
   - **Szybkie skanowanie**

W tym trybie Kaspersky Endpoint Security skanuje tylko potencjalnie infekowalne pliki i nie rozpakowuje obiektów złożonych.

4. Jeżeli chcesz, aby Kaspersky Endpoint Security skanował tylko nośniki wymienne, których rozmiar nie przekracza określonej wartości, zaznacz pole **Maksymalny rozmiar nośnika wymiennego** i w polu obok określ wartość w megabajtach.

5. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Działania podejmowane na nieprzetworzonych plikach

Sekcja ta zawiera instrukcje dotyczące działań podejmowanych na zainfekowanych i prawdopodobnie zainfekowanych plikach, których Kaspersky Endpoint Security nie przetworzył podczas skanowania komputera w poszukiwaniu wirusów i innych zagrożeń.

Informacje o nieprzetworzonych plikach

Kaspersky Endpoint Security zapisuje informacje o plikach, które z jakiegoś powodu nie zostały przetworzone. Informacje te są zapisywane w postaci zdarzeń na liście nieprzetworzonych plików.

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.

Zainfekowany plik jest uznawany za *nieprzetworzony*, jeśli podczas skanowania Kaspersky Endpoint Security z jakiegoś powodu nie wykonał na nim akcji określonej w ustawieniach 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**.

Po zaktualizowaniu baz danych i modułów aplikacji możesz ręcznie uruchomić zadanie Skanowania obiektów dla plików z listy nieprzetworzonych plików . Po skanowaniu stan pliku może się zmienić. Możesz wykonać wymagane akcje na plikach, w zależności od ich stanu.

Na przykład, możesz wykonać następujące akcje:

- Usunąć pliki posiadające stan *Zainfekowany*.
- Przywrócić zainfekowane pliki, które zawierają ważne informacje, oraz przywrócić pliki, które są oznaczone jako *Wyleczony* lub *Niezainfekowany*.

- Poddać kwarantannie pliki posiadające stan *Prawdopodobnie zainfekowany*.

Zarządzanie listą nieprzetworzonych plików

Lista nieprzetworzonych plików pojawia się w formie tabeli.

Na nieprzetworzonych plikach można wykonać następujące działania:

- Przejrzeć listę nieprzetworzonych plików.
- Przeskanować nieprzetworzone pliki przy użyciu bieżącej wersji baz danych i modułów Kaspersky Endpoint Security.
- Przywrócić pliki z lisy nieprzetworzonych plików do ich oryginalnych folderów lub do innego foldera (gdy nie można zapisać plików w ich oryginalnych folderach).
- Usunąć pliki z listy nieprzetworzonych plików.
- Otworzyć folder, w którym pierwotnie znajdował się nieprzetworzony plik.

Podczas zarządzania danymi w tabeli możesz również wykonywać następujące czynności:

- Filtrować zdarzenia nieprzetworzonych plików według wartości kolumny lub warunków filtra niestandardowego.
- Używać funkcji wyszukiwania zdarzenia nieprzetworzonego pliku.
- Sortować zdarzenia nieprzetworzonych plików.
- Zmieniać kolejność i zestaw kolumn wyświetlanych na liście nieprzetworzonych plików.
- Grupować zdarzenia nieprzetworzonych plików.

W razie konieczności możesz skopiować wybrane zdarzenia nieprzetworzonych plików do schowka.

Uruchamianie zadania Skanowanie obiektów dla nieprzetworzonych plików

Możliwe jest ręczne uruchomienie zadania Skanowanie obiektów dla nieprzetworzonych plików. Zadanie można uruchomić, jeśli, na przykład, gdy z jakiegoś powodu ostatnie skanowanie zostało przerwane lub gdy chcesz ponownie przeskanować nieprzetworzone pliki po ostatniej aktualizacji baz danych i modułów.

W celu uruchomienia Skanowania obiektów dla nieprzetworzonych plików:

1. Otwórz okno główne aplikacji.
2. W górnej części okna głównego aplikacji kliknij odnośnik **Kwarantanna**, aby otworzyć okno **Pliki danych**.
3. W oknie **Pliki danych** wybierz zakładkę **Nieprzetworzone pliki**.
4. Z tabeli dostępnej na zakładce **Nieprzetworzone pliki** wybierz jedno lub kilka zdarzeń dotyczących plików, które chcesz przeskanować.

W przypadku, gdy chcesz wybrać więcej zdarzeń, zaznacz je, trzymając wciśnięty klawisz **CTRL**.

5. Skanowanie obiektów można uruchomić w jeden z następujących sposobów:

   - Kliknij przycisk **Skanuj ponownie**.
   - Kliknij obiekt prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Skanuj ponownie**.

Usuwanie plików z listy nieprzetworzonych plików

W celu usunięcia plików z listy nieprzetworzonych plików:

1. Otwórz okno główne aplikacji.
2. W górnej części okna głównego aplikacji kliknij odnośnik **Kwarantanna**, aby otworzyć okno **Pliki danych**.
3. W oknie **Pliki danych** wybierz zakładkę **Nieprzetworzone pliki**.
4. Z tabeli dostępnej na zakładce **Nieprzetworzone pliki** wybierz jeden lub kilka zdarzeń dotyczących plików, które chcesz usunąć.

   W przypadku, gdy chcesz wybrać więcej zdarzeń, zaznacz je, trzymając wciśnięty klawisz **CTRL**.
5. Usuń pliki w jeden z następujących sposobów:

   - Kliknij przycisk **Usuń**.
   - Kliknij go prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Usuń**.

Wykrywanie luk

Ta sekcja zawiera informacje o właściwościach i ustawieniach zadania Wykrywanie luk, a także instrukcje dotyczące zarządzania listą luk wykrytych przez Kaspersky Endpoint Security w trakcie działania zadania Wykrywanie luk.

Przeglądanie informacji o lukach w uruchomionych aplikacjach

Informacje o lukach w uruchomionych aplikacjach są dostępne, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla stacji roboczych. Informacje są niedostępne, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów plików.

W celu przejrzenia informacji o lukach w uruchomionych aplikacjach:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Otwórz sekcję **Kontrola węzła końcowego**.
4. Kliknij przycisk **Monitor aktywności aplikacji**.

   Zostanie otwarte okno **Kontrola uprawnień aplikacji** na zakładce **Monitor aktywności aplikacji**. Tabela **Monitor aktywności aplikacji** wyświetla informacje podsumowujące aktywność aplikacji uruchomionych w systemie operacyjnym. Stopień zagrożenia luki w uruchomionej aplikacji, zdefiniowany przez Monitor wykrywania luk, wyświetlany jest w kolumnie **Waga luki**.

Informacje o zadaniu Wykrywanie luk

Luki systemu operacyjnego mogą wynikać z błędów oprogramowania lub błędów technicznych, słabych haseł, działania złośliwego oprogramowania itd. Podczas skanowania w poszukiwaniu luk aplikacja analizuje system operacyjny i wyszukuje nieprawidłowości oraz uszkodzone ustawienia aplikacji firmy Microsoft i innych producentów.

Wykrywanie luk polega na diagnostyce bezpieczeństwa systemu operacyjnego oraz wykrywaniu takich cech oprogramowania, które mogą być wykorzystywane przez przestępców do rozsyłania szkodliwych obiektów i uzyskania dostępu do informacji osobistych.

Po uruchomieniu zadania Wykrywanie luk, jego postęp jest wyświetlany w polu obok nazwy uruchomionego zadania **Wykrywanie luk**, w sekcji **Zadania** dostępnej w oknie głównym aplikacji Kaspersky Endpoint Security, na zakładce **Ochrona i kontrola**.

Wyniki wykonania zadania Wykrywanie luk są zapisywane w raportach.

Uruchamianie i zatrzymywanie zadania Wykrywanie luk

Bez względu na wybrany tryb uruchamiania zadania Wykrywania luk, możesz uruchomić lub zatrzymać zadanie w dowolnym momencie.

W celu uruchomienia lub zatrzymania zadania Wykrywania luk:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Kliknij sekcję **Zadania**.

   Zostanie otwarta sekcja **Zadania**.
4. Kliknij prawym przyciskiem myszy wiersz z nazwą zadania Wykrywanie luk.

   Zostanie otwarte menu wyboru działań zadania Wykrywania luk.
5. Wykonaj jedną z poniższych czynności:

   - Aby uruchomić zadanie Wykrywanie luk, wybierz z menu **Uruchom skanowanie**.

     Stan postępu wykonywania zadania, wyświetlany po prawej stronie przycisku z nazwą zadania Wykrywanie luk, zmieni się na *Uruchomiono*.

   - Aby zatrzymać zadanie Wykrywanie luk, wybierz z menu **Zatrzymaj skanowanie**.

     Stan postępu wykonywania zadania, wyświetlany po prawej stronie przycisku z nazwą zadania Wykrywanie luk, zmieni się na *Zatrzymano*.

Konfigurowanie ustawień zadania Wykrywanie luk

Podczas konfigurowania ustawień zadania Wykrywania luk można:

- Utworzyć obszar zadania Wykrywanie luk.

  Możesz poszerzyć lub zwęzić obszar skanowania, dodając lub usuwając aplikacje skanowane w poszukiwaniu luk.

- Wybrać tryb uruchamiania zadania Wykrywanie luk.

  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.

- Skonfigurować uruchamianie zadania z poziomu konta innego użytkownika.

  Domyślnie zadanie skanowania jest uruchamiane z poziomu konta, na które użytkownik zalogował się w systemie operacyjnym. Jednak może zaistnieć potrzeba uruchomienia zadania z poziomu konta innego użytkownika. Możesz wskazać użytkownika, który posiada odpowiednie uprawnienia, w ustawieniach zadania skanowania i uruchamiać zadanie z poziomu konta tego użytkownika.

Tworzenie obszaru wykrywania luk

Obszar wykrywania luk to dostawca oprogramowania lub ścieżka do folderu instalacyjnego oprogramowania (na przykład wszystkie aplikacje firmy Microsoft, które zainstalowane są w folderze Program Files).

W celu utworzenia obszaru wykrywania luk:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz **Wykrywanie luk**.

   W prawej części okna wyświetlane są ustawienia zadania Wykrywanie luk.
3. W sekcji **Obszar skanowania**:

   a. Aby Kaspersky Endpoint Security szukał luk w aplikacjach firmy Microsoft zainstalowanych na komputerze, zaznacz pole **Microsoft**.

   b. Aby Kaspersky Endpoint Security szukał luk we wszystkich aplikacjach zainstalowanych na komputerze (innych niż te firmy Microsoft), zaznacz pole **Inni producenci**.

   c. W oknie **Dodatkowy obszar skanowania w poszukiwaniu luk** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Obszar wykrywania luk**.

   d. Utwórz obszar wykrywania luk. W tym celu użyj przycisków **Dodaj** i **Usuń**.

   e. W oknie **Obszar wykrywania luk** kliknij **OK**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Wybieranie trybu uruchamiania zadania Wykrywanie luk

W celu wybrania trybu uruchamiania zadania Wykrywanie luk:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz **Wykrywanie luk**.

   W prawej części okna wyświetlane są ustawienia zadania Wykrywanie luk.
3. Kliknij przycisk **Tryb uruchamiania**.

   Ten przycisk otwiera zakładkę **Tryb uruchamiania** w oknie **Wykrywanie luk**.
4. Na zakładce **Tryb uruchamiania** wybierz jedną z następujących opcji trybu uruchamiania zadania Wykrywanie luk:

   - Jeżeli chcesz uruchomić zadanie Wykrywanie luk ręcznie, wybierz **Ręcznie**.
   - Jeśli chcesz skonfigurować terminarz uruchamiania zadania Wykrywania luk, wybierz **Zgodnie z terminarzem**.
5. Wykonaj jedną z poniższych czynności:

   - Jeżeli wybrałeś opcję **Ręcznie**, przejdź do kroku 6 niniejszej instrukcji.
   - Jeżeli wybrałeś opcję **Zgodnie z terminarzem**, określ ustawienia terminarza uruchamiania zadania Wykrywanie luk. W tym celu:

     a. Z listy rozwijalnej **Częstotliwość** wybierz czas uruchamiania zadania Wykrywania luk. Wybierz jedną z następujących opcji: **Dni**, **Co tydzień**, **O określonym czasie**, **Co miesiąc**, **Po uruchomieniu aplikacji** lub **Po każdej aktualizacji**.

b. W zależności od opcji wybranej na liście **Częstotliwość** określ wartości dla ustawień, które definiują czas uruchamiania zadania Wykrywanie luk.

c. Jeżeli chcesz, aby Kaspersky Endpoint Security uruchamiał pominięte zadania Wykrywania luk, zaznacz pole **Uruchom pominięte zadania**.

> Jeżeli z listy rozwijalnej **Częstotliwość** wybrano opcję **Po uruchomieniu aplikacji** lub **Po każdej aktualizacji**, pole **Uruchom pominięte zadania** nie będzie dostępne.

6. Kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Uruchamianie zadania Wykrywanie luk z poziomu konta innego użytkownika

Domyślnie zadanie Wykrywania luk jest uruchamiane z poziomu konta, na które użytkownik zalogował się w systemie operacyjnym. Jednak może zaistnieć potrzeba uruchomienia zadania Wykrywania luk z poziomu konta innego użytkownika. Możesz wskazać użytkownika, który posiada odpowiednie uprawnienia, w ustawieniach zadania Wykrywania luk i uruchamiać zadanie z poziomu konta tego użytkownika.

W celu skonfigurowania uruchamiania zadania Wykrywania luk z poziomu konta innego użytkownika:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz **Wykrywanie luk**.

   W prawej części okna wyświetlane są ustawienia zadania Wykrywanie luk.

3. Kliknij przycisk **Tryb uruchamiania**.

   Ten przycisk otwiera zakładkę **Tryb uruchamiania** w oknie **Wykrywanie luk**.

4. Na zakładce **Tryb uruchamiania**, w sekcji **Użytkownik** zaznacz pole **Uruchom zadanie jako**.

5. W polu **Nazwa** wprowadź nazwę konta użytkownika, którego uprawnienia są niezbędne do uruchomienia zadania Wykrywanie luk.

6. W polu **Hasło** wprowadź hasło użytkownika, którego uprawnienia są niezbędne do uruchomienia zadania Wykrywanie luk.

7. Kliknij **OK**.

8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zarządzanie listą luk

Podczas zarządzania listą luk możesz wykonać następujące czynności:

- Przejrzeć listę luk.
- Uruchomić ponownie zadanie Wykrywanie luk po zaktualizowaniu baz danych i modułów aplikacji.

- Przejrzeć w oddzielnej sekcji szczegółowe informacje o luce i zaleceniach dotyczących jej naprawy.
- Ukryć na liście luk wybrane wpisy.
- Filtrować listę luk według rangi.
- Filtrować listę luk według stanu *Naprawione* i *Ukryta*.

Podczas zarządzania danymi w tabeli możesz również wykonywać następujące czynności:

- Filtrować listę luk według wartości kolumn lub niestandardowych warunków filtrowania.
- Użyć funkcji wyszukiwania luk.
- Sortować wpisy na liście luk.
- Zmieniać kolejność i rozmieszczenie kolumn wyświetlanych na liście luk.
- Grupować wpisy na liście luk.

Informacje o liście luk

Kaspersky Endpoint Security zapisuje wyniki zadania Wykrywanie luk na liście luk.

Jeżeli użytkownik przejrzy określone luki i wykona działania zalecane do ich wyeliminowania, Kaspersky Endpoint Security zmieni stan luk na *Naprawiona*.

Jeżeli użytkownik nie chce wyświetlić na liście luk wpisów dotyczących określonych luk, może wybrać opcję ich ukrycia. Kaspersky Endpoint Security przypisuje takim lukom stan *Ukryta*.

Lista luk pojawia się w postaci tabeli. Każdy wiersz tabeli zawiera następujące informacje:

- Ikonę wskazującą poziom zagrożenia luki. Wyróżniane są następujące poziomy zagrożeń luk:
  - Ikona . **Krytyczny**. Poziom zagrożenia stosowany jest do wysoce niebezpiecznych luk, które muszą zostać natychmiast naprawione. Cyberprzestępcy wykorzystują luki tego poziomu do infekowania systemu operacyjnego komputera lub do uzyskania dostępu do osobistych danych użytkownika. Firma Kaspersky zaleca natychmiastowe podjęcie wszystkich kroków niezbędnych do naprawienia luk z poziomem zagrożenia "Krytyczna".
  - Ikona . **Ważne**. Poziom zagrożenia stosowany jest do luk, które muszą zostać naprawione tak szybko, jak to możliwe. Cyberprzestępcy mogą aktywnie wykorzystywać luki posiadające ten poziom. Aktualnie oszuści nie wykorzystują aktywnie luk z poziomem zagrożenia "Ważna". Firma Kaspersky zaleca natychmiastowe podjęcie wszystkich kroków niezbędnych do naprawienia luk z poziomem zagrożenia "Ważna".
  - Ikona . **Ostrzeżenie**. Poziom zagrożenia stosowany jest do luk, których leczenie można odroczyć. Jednakże takie luki mogą stwarzać zagrożenie dla bezpieczeństwa komputera w przyszłości.
- Numer identyfikujący lukę.
- Nazwę aplikacji, w której została wykryta luka.
- Krótki opis luki.

- Informacje o producencie oprogramowania, które znajdują się w podpisie cyfrowym.
- Wynik działania podjętego w celu naprawy luki.

Ponowne uruchamianie zadania Wykrywanie luk

Aby zaktualizować informacje o wcześniej wykrytych lukach, możesz ponownie uruchomić zadanie Wykrywania luk. Ponowne uruchomienie zadania skanowania może być konieczne, jeśli skanowanie w poszukiwaniu luk zostało przerwane lub chcesz przeskanować komputer na obecność luk po ostatniej aktualizacji baz danych i modułów aplikacji.

W celu ponownego uruchomienia zadania Wykrywania luk:

1. Otwórz okno główne aplikacji.
2. W górnej części okna głównego aplikacji kliknij odnośnik **Kwarantanna**, aby otworzyć okno **Pliki danych**.
3. W oknie **Pliki danych** wybierz zakładkę **Luki**.

   Zakładka **Luki** zawiera listę luk, które Kaspersky Endpoint Security wykrył podczas wykonywania zadania wykrywania luk.
4. W prawym dolnym rogu okna **Pliki danych** kliknij przycisk **Skanuj ponownie**.

Kaspersky Endpoint Security zaktualizuje szczegółowe informacje o lukach na liście luk.

Stan luki naprawionej poprzez zainstalowanie proponowanej łatki nie zmieni się po kolejnym skanowaniu w poszukiwaniu luk.

Naprawianie luk

Możesz naprawić lukę, instalując uaktualnienie systemu operacyjnego, zmieniając konfigurację aplikacji lub instalując łatkę dla aplikacji.

Wykryte luki mogą nie dotyczyć zainstalowanych aplikacji lecz ich kopii. Łatka może naprawić lukę tylko, jeśli zainstalowano aplikację.

W celu naprawy luki:

1. Otwórz okno główne aplikacji.
2. W górnej części okna głównego aplikacji kliknij odnośnik **Kwarantanna**, aby otworzyć okno **Pliki danych**.
3. W oknie **Pliki danych** wybierz zakładkę **Luki**.

   Zakładka **Luki** zawiera listę luk, które Kaspersky Endpoint Security wykrył podczas wykonywania zadania wykrywania luk.
4. Na liście luk wybierz wpis odnoszący się do odpowiedniej luki.

W dolnej części listy luk zostanie otwarta sekcja z informacjami o luce i zaleceniami dotyczącymi jej naprawy.

Dla każdej wybranej luki dostępne są następujące informacje:

- Nazwę aplikacji, w której została wykryta luka.
- Wersja aplikacji, w której została wykryta luka.
- Poziom zagrożenia luki.
- Numer identyfikujący lukę.
- Data i czas ostatniego wykrycia luki.
- Zalecenia dotyczące naprawy luki (na przykład, odnośnik do strony z aktualizacjami systemu operacyjnego lub z łatką do aplikacji).
- Odnośnik do strony z opisem luki.

5. W celu zapoznania się ze szczegółowym opisem luki, należy kliknąć odnośnik **Dodatkowe informacje**, aby otworzyć stronę internetowa z opisem zagrożenia związanego z wybrana luką. Strona internetowa www.secunia.com umożliwia pobranie i zainstalowanie odpowiedniego uaktualnienia do bieżącej wersji aplikacji.

6. Wybierz jeden z poniższych sposobów naprawy luki:

   - Jeśli dla aplikacji jest dostępna jedna lub więcej łatek, zainstaluj wymaganą łatkę, postępując zgodnie z instrukcjami znajdującymi się obok nazwy łatki.
   - Jeśli dostępne jest uaktualnienie systemu operacyjnego, zainstaluj je, postępując zgodnie z instrukcjami znajdującymi się obok nazwy uaktualnienia.

   Luka zostanie naprawiona po zainstalowaniu łatki lub uaktualnienia. Kaspersky Endpoint Security przydzieli luce stan określający, że została naprawiona. Wpis dotyczący naprawionej luki wyświetlany jest na liście luk w kolorze szarym.

7. Jeśli w dolnej części okna nie ma informacji dotyczących wyeliminowania luki, możesz uruchomić zadanie Wykrywania luk ponownie po aktualizacji baz danych i modułów Kaspersky Endpoint Security. Ponieważ w trakcie skanowania systemu w poszukiwaniu luk Kaspersky Endpoint Security korzysta z baz danych luk, wpis dotyczący naprawionej luki może pojawić się po aktualizacji aplikacji.

Ukrywanie wpisów na liście luk

Istnieje możliwość ukrycia wpisu dotyczącego wybranej luki. Kaspersky Endpoint Security przypisuje stan *Ukryta* do wpisu wybranego na liście luk i oznaczonego jako ukryty. Następnie możesz przefiltrować listę luk według stanu *Ukryta*.

W celu ukrycia wpisu na liście luk:

1. Otwórz okno główne aplikacji.
2. W górnej części okna głównego aplikacji kliknij odnośnik **Kwarantanna**, aby otworzyć okno **Pliki danych**.
3. W oknie **Pliki danych** wybierz zakładkę **Luki**.

Zakładka **Luki** zawiera listę luk, które Kaspersky Endpoint Security wykrył podczas wykonywania zadania wykrywania luk.

4. Na liście luk zaznacz wpis dotyczący luki, którą chcesz ukryć.

   W dolnej części listy luk zostanie otwarta sekcja z informacjami o luce i zaleceniami dotyczącymi jej naprawy.

5. Kliknij przycisk **Ukryj**.

   Kaspersky Endpoint Security przypisze wybranej luce status *Ukryty*. Wpisy dotyczące luk posiadających stan *Ukryta* zostają przeniesione na koniec listy luk i stają się nieaktywne.

6. Aby na liście luk ukryć wpis dotyczący luki, w górnej części listy zaznacz pole **Ukryta**.

Filtrowanie listy luk według priorytetu

W celu przefiltrowania listy luk według priorytetu:

1. Otwórz okno główne aplikacji.

2. W górnej części okna głównego aplikacji kliknij odnośnik **Kwarantanna**, aby otworzyć okno **Pliki danych**.

3. W oknie **Pliki danych** wybierz zakładkę **Luki**.

   Zakładka **Luki** zawiera listę luk, które Kaspersky Endpoint Security wykrył podczas wykonywania zadania wykrywania luk. W górnej części listy luk, w wierszu **Wyświetl priorytet** pojawią się trzy ikony wskazujące poziom zagrożenia luki (Ostrzeżenie, Ważne, Krytyczne). Poprzez kliknięcie tych ikon możesz filtrować listę luk według poziomu zagrożenia.

4. Kliknij jedną, dwie lub trzy ikony poziomu zagrożenia luki. Na liście są wyświetlane luki odpowiadające wybranym poziomom zagrożenia. Aby anulować wyświetlanie luk odpowiadających określonemu poziomowi zagrożenia, kliknij ponownie ikonę odpowiedniego poziomu zagrożenia. Jeśli nie wybrano żadnego poziomu zagrożenia, lista luk będzie pusta.

Określone warunki filtrowania wpisów dotyczących luk są zapisywane po zamknięciu okna **Pliki danych**.

Filtrowanie listy luk według stanu Naprawione i Ukryta

W celu przefiltrowania listy luk według stanu Naprawione i Ukryta:

1. Otwórz okno główne aplikacji.

2. W górnej części okna głównego aplikacji kliknij odnośnik **Kwarantanna**, aby otworzyć okno **Pliki danych**.

3. W oknie **Pliki danych** wybierz zakładkę **Luki**.

   Zakładka **Luki** zawiera listę luk, które Kaspersky Endpoint Security wykrył podczas wykonywania zadania wykrywania luk.

4. Pola do zaznaczania, które odpowiadają stanowi luk, znajdują się obok ustawienia **Wyświetl luki**. W celu przefiltrowania listy luk według stanu *Naprawione*:

   - Wybierz opcję **Naprawiona**, aby na liście luk zostały wyświetlone naprawione luki. Wpisy dotyczące naprawionych luk są wyświetlane na liście luk w kolorze szarym.

- Aby ukryć wpisy dotyczące wykrytych luk na liście luk, usuń zaznaczenie z pola **Naprawiona**.

5. W celu przefiltrowania listy luk według stanu *Ukryta*:

   - Zaznacz opcję **Ukryta**, aby na liście luk zostały wyświetlone ukryte luki. Wpisy dotyczące ukrytych luk są wyświetlane na liście luk w kolorze szarym.

   - Aby ukryć wpisy dotyczące ukrytych luk na liście luk, usuń zaznaczenie pola **Ukryta**.

Określone warunki filtrowania wpisów dotyczących luk nie są zapisywane po zamknięciu okna **Pliki danych**.

Sprawdzanie integralności modułów aplikacji

Ta sekcja zawiera informacje o specyfikacji i ustawieniach zadania sprawdzania integralności.

Informacje o zadaniu 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.

Po uruchomieniu zadania sprawdzania integralności, jego postęp jest wyświetlany w polu obok nazwy zadania, w sekcji **Zadania** dostępnej w oknie głównym aplikacji Kaspersky Endpoint Security, na zakładce **Ochrona i kontrola**.

Wyniki wykonania zadania sprawdzania integralności są zapisywane w raportach.

Uruchamianie i zatrzymywanie zadania Sprawdzanie integralności

Bez względu na wybrany tryb uruchamiania, możesz uruchomić lub zatrzymać zadanie sprawdzania integralności w dowolnym momencie.

W celu uruchomienia lub zatrzymania zadania sprawdzania integralności:

1. Otwórz okno główne aplikacji.
2. Wybierz zakładkę **Ochrona i kontrola**.
3. Otwórz sekcję **Zadania**.
4. Kliknij prawym przyciskiem myszy wiersz z nazwą zadania sprawdzania integralności.
5. Wykonaj jedną z poniższych czynności:
   - Aby uruchomić zadanie Sprawdzanie integralności, wybierz z menu **Uruchom skanowanie**.

     Stan postępu zadania, wyświetlany po prawej stronie przycisku z nazwą tego zadania, zmieni się na *Uruchomiono*.
   - Jeżeli chcesz zatrzymać zadanie, z menu kontekstowego wybierz element **Zatrzymaj skanowanie**.

     Stan postępu zadania, wyświetlany po prawej stronie przycisku z nazwą tego zadania, zmieni się na *Zatrzymano*.

Wybieranie trybu uruchamiania zadania Sprawdzanie integralności

W celu wybrania trybu uruchamiania zadania Sprawdzanie integralności:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Zadania zaplanowane** wybierz **Sprawdzanie integralności**.

   W prawej części okna wyświetlane są ustawienia zadania sprawdzania integralności.

3. W sekcji **Tryb uruchamiania** wybierz jedną z następujących opcji:

   - Jeżeli chcesz ręcznie uruchomić zadanie Sprawdzanie integralności, wybierz **Ręcznie**.
   - Jeśli chcesz skonfigurować terminarz uruchamiania zadania Sprawdzanie integralności, wybierz **Zgodnie z terminarzem**.

4. Jeśli w poprzednim kroku wybrałeś opcję **Zgodnie z terminarzem**, określ ustawienia terminarza uruchamiania zadania. W tym celu:

   a. Z listy rozwijalnej **Częstotliwość** wybierz czas uruchamiania zadania. Wybierz jedną z następujących opcji: **Minuty**, **Godziny**, **Dni**, **Co tydzień**, **O określonym czasie**, **Co miesiąc** lub **Po uruchomieniu aplikacji**.

   b. W zależności od opcji wybranej na liście **Częstotliwość** określ wartości dla ustawień, które definiują czas uruchamiania zadania.

   c. Jeżeli chcesz, aby Kaspersky Endpoint Security uruchamiał pominięte zadania Sprawdzanie integralności, zaznacz pole **Uruchom pominięte zadania**.

      Jeżeli z listy rozwijalnej **Częstotliwość** wybrano opcję **Po uruchomieniu aplikacji**, **Minuty** lub **Godziny**, pole **Uruchom pominięte zadania** nie będzie dostępne.

   d. Jeżeli chcesz, aby Kaspersky Endpoint Security zawieszał wykonywanie zadania, gdy ograniczone są zasoby komputera, zaznacz opcję **Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności**.

      Ta opcja terminarza pozwala zaoszczędzić zasoby komputera.

5. Kliknij **OK**.

6. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zarządzanie raportami

Sekcja ta opisuje sposób konfigurowania ustawień raportów oraz zarządzania raportami.

Zasady zarządzania raportami

W raporcie zapisywane są informacje o działaniu każdego modułu programu Kaspersky Endpoint Security, wykonaniu każdego zadania skanowania, zadania aktualizacji, zadaia kontroli integralności oraz zadania wykrywania luk, a także o ogólnym działaniu aplikacji.

Dane są przedstawione w raporcie w formie tabeli zawierającej listę zdarzeń. 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 wykresu. Zdarzenia zapisywane podczas działania różnych komponentów lub 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.
- Raport **Wszystkie składniki ochrony**. Zawiera informacje o zdarzeniach zapisywanych podczas działania następujących modułów Kaspersky Endpoint Security:
  - Ochrona plików
  - Ochrona poczty.
  - Ochrona WWW.
  - Ochrona komunikatorów.
  - Kontrola systemu.
  - Zapora sieciowa.
  - Blokowanie ataków sieciowych.
  - Ochrona przed atakami BadUSB
- Raport z działania modułu lub wykonania zadania programu Kaspersky Endpoint Security.
- Raport **Szyfrowanie**. Zawiera informacje o zdarzeniach występujących podczas szyfrowania i deszyfrowania danych.

W raportach używane są następujące priorytety zdarzeń:

- **Zdarzenia informacyjne**. Ikona ℹ. Typowe zdarzenia nie zawierające istotnych informacji.
- **Ważne zdarzenia**. Ikona ⚠. Zdarzenia wymagające uwagi użytkownika, ponieważ odzwierciedlają istotną sytuację związaną z działaniem Kaspersky Endpoint Security.

- **Zdarzenia krytyczne**. Ikona . 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.
- 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. Kaspersky Endpoint Security usunie wszystkie wpisy z wybranych raportów, począwszy od najwcześniejszych wpisów, aż do najnowszych.

Konfigurowanie ustawień raportów

Podczas konfigurowania ustawień raportów możliwe jest:

- Skonfigurowanie maksymalnego czasu przechowywania raportów.

  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. Możesz wyłączyć ograniczenie czasu przechowywania raportu lub zmienić jego maksymalną wartość.

- Skonfigurowanie 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. Możesz anulować ograniczenie rozmiaru pliku raportu lub ustawić inną wartość.

Konfigurowanie maksymalnego czasu przechowywania raportu

W celu zmiany maksymalnego czasu przechowywania raportów:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz **Raporty i pliki danych**.
3. W prawej części okna, w sekcji **Parametry raportu** wykonaj następujące czynności:
   - Aby ograniczyć czas przechowywania raportów, zaznacz pole **Przechowuj raporty nie dłużej niż**. W polu obok opcji **Przechowuj raporty nie dłużej niż** określ maksymalny czas przechowywania raportów.

Domyślnie maksymalny czas przechowywania raportów wynosi 30 dni.

- Aby anulować ograniczenie czasu przechowywania raportów, usuń zaznaczenie z pola **Przechowuj raporty nie dłużej niż**.

Domyślnie ograniczenie czasu przechowywania raportu jest włączone.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Konfigurowanie maksymalnego rozmiaru pliku raportu

W celu skonfigurowania maksymalnego rozmiaru pliku raportu:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz **Raporty i pliki danych**.
3. W prawej części okna, w sekcji **Parametry raportu** wykonaj następujące czynności:
   - Aby ograniczyć rozmiar pliku raportu, zaznacz pole **Maksymalny rozmiar pliku**. W polu po prawej stronie opcji **Maksymalny rozmiar pliku** określ maksymalny rozmiar pliku raportu.

     Domyślnie maksymalny rozmiar pliku raportu wynosi 1024 MB.
   - Aby usunąć ograniczenie rozmiaru pliku raportu, usuń zaznaczenie z pola **Maksymalny rozmiar pliku**.

   Domyślnie ograniczenie rozmiaru pliku raportu jest włączone.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Wyświetl raporty

W celu wyświetlenia raportów:

1. Otwórz okno główne aplikacji.
2. W górnej części okna głównego aplikacji kliknij odnośnik **Raporty**, aby otworzyć okno **Raporty**.
3. Aby wygenerować raport Wszystkie składniki ochrony, w lewej części okna **Raporty**, na liście modułów i zadań wybierz **Wszystkie składniki ochrony**.

   Raport Wszystkie składniki ochrony wyświetlany jest w prawej części okna i zawiera listę zdarzeń dotyczących działań wszystkich modułów ochrony Kaspersky Endpoint Security.
4. W celu wygenerowania raportu z działania modułu lub zadania, na liście modułów i zadań, dostępnej w lewej części okna **Raporty**, wybierz moduł lub zadanie.

   Raport jest wyświetlany w prawej części okna i zawiera listę zdarzeń dotyczących działania wybranego modułu lub zadania Kaspersky Endpoint Security.

Domyślnie zdarzenia z raportu są sortowane rosnąco według wartości w kolumnie **Data zdarzenia**.

Przeglądanie informacji o zdarzeniu w raporcie

W raporcie można przejrzeć szczegółowe podsumowanie każdego zdarzenia.

W celu wyświetlenia szczegółowego podsumowania zdarzenia w raporcie:

1. Otwórz okno główne aplikacji.
2. W górnej części okna głównego aplikacji kliknij odnośnik **Raporty**, aby otworzyć okno **Raporty**.
3. W lewej części okna wybierz odpowiedni raport dotyczący komponentu lub zadania.

   Zdarzenia zapisane w raporcie są wyświetlane w postaci tabeli, w prawej części okna. Aby odszukać w raporcie określone zdarzenia, użyj filtra, wyszukiwania oraz sortowania.
4. Wybierz odpowiednie zdarzenie w raporcie.

W dolnej części okna zostaną wyświetlone informacje podsumowujące zdarzenie.

Zapisywanie raportu do pliku

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. Otwórz okno główne aplikacji.
2. W górnej części okna głównego aplikacji kliknij odnośnik **Raporty**, aby otworzyć okno **Raporty**.
3. Wykonaj jedną z poniższych czynności:

   - W celu wygenerowania raportu "Wszystkie składniki ochrony" wybierz **Wszystkie składniki ochrony** na liście komponentów i zadań.

     Raport "Wszystkie składniki ochrony" wyświetlany jest w prawej części okna i zawiera listę zdarzeń dotyczących działań wszystkich modułów ochrony.

   - Jeżeli chcesz wygenerować raport z działania wybranego komponentu lub zadania, wybierz ten komponent lub zadanie na liście komponentów i zadań.

     Raport ochrony wyświetlany jest w prawej części okna i zawiera listę zdarzeń dotyczących działań wybranego modułu lub zadania.
4. W razie konieczności możesz zmodyfikować wyświetlanie danych w raporcie poprzez:

   - Filtrowanie zdarzeń
   - Wyszukiwanie zdarzeń

- Zmienianie kolejności kolumn
- Sortowanie zdarzeń

5. Kliknij przycisk **Zapisz raport** znajdujący się w prawej górnej części okna.
   Zostanie otwarte menu kontekstowe.
6. W menu kontekstowym wybierz typ kodowania do zapisu pliku raportu: **Zapisz jako ANSI** or **Zapisz jako Unicode**.
   Zostanie otwarte standardowe okno **Zapisz jako** z Microsoft Windows.
7. W oknie **Zapisz jako** określ folder docelowy dla pliku raportu.
8. W polu **Nazwa pliku** wprowadź nazwę pliku raportu.
9. W polu **Rodzaj pliku** wybierz żądany format pliku raportu: TXT lub CSV.
10. Kliknij przycisk **Zapisz**.

Czyszczenie raportów

W celu usunięcia informacji z raportów:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz **Raporty i pliki danych**.
3. W prawej części okna, w sekcji **Parametry raportu** kliknij przycisk **Usuń raporty**.
   Zostanie otwarte okno **Czyszczenie raportów**.
4. Zaznacz pola obok raportów, z których chcesz usunąć informacje:
   - **Wszystkie raporty**.
   - **Ogólny raport ochrony**. Zawiera informacje o działaniu następujących modułów Kaspersky Endpoint Security:
     - Ochrona plików
     - Ochrona poczty.
     - Ochrona WWW.
     - Ochrona komunikatorów.
     - Kontrola systemu.
     - Zapora sieciowa.
     - Blokowanie ataków sieciowych.
     - Ochrona przed atakami BadUSB

- **Raport zadań skanowania**. Zawiera informacje o zakończonych zadaniach skanowania:
  - Pełne skanowanie
  - Skanowanie obszarów krytycznych
  - Skanowanie obiektów
  - Sprawdzenie integralności.
- **Raport zadania aktualizacji**. Zawiera informacje o zakończonych zadaniach aktualizacji:
- **Raport Zapory sieciowej**. Zawiera informacje o działaniu Zapory sieciowej.
- **Raport modułów kontroli**. Zawiera informacje o działaniu następujących modułów Kaspersky Endpoint Security:
  - Kontrola uruchamiania aplikacji.
  - Kontrola uprawnień aplikacji.
  - Monitor wykrywania luk.
  - Kontrola urządzeń.
  - Kontrola sieci.
- **Raport z szyfrowania danych**.

5. Kliknij **OK**.

Usługa powiadomień

Ta sekcja opisuje usługę powiadomień informujących użytkownika o zdarzeniach związanych z działaniem Kaspersky Endpoint Security oraz zawiera instrukcje dotyczące sposobu skonfigurowania parametrów powiadomień.

Informacje o powiadomieniach Kaspersky Endpoint Security

Podczas działania programu Kaspersky Endpoint Security pojawiają się różnego rodzaju zdarzenia. Powiadomienia o tych zdarzeniach mogą być czysto informacyjne lub zawierać krytyczne informacje. Na przykład, powiadomienia mogą informować o pomyślnej aktualizacji baz danych i modułów aplikacji lub rejestracji błędów komponentów, które muszą być rozwiązane.

Kaspersky Endpoint Security obsługuje rejestrowanie informacji o zdarzeniach w dzienniku aplikacji Microsoft Windows i / lub raporcie zdarzeń Kaspersky Endpoint Security.

Kaspersky Endpoint Security dostarcza powiadomienia w jeden z następujących sposobów:

- Pod postacią komunikatów wyskakujących w obszarze powiadomień paska zadań Microsoft Windows;
- W wiadomości e-mail.

Możliwe jest skonfigurowanie dostarczania powiadomień o zdarzeniach. Metoda dostarczania powiadomień jest konfigurowana dla każdego typu zdarzenia.

Konfigurowanie usługi powiadamiania

Podczas konfigurowania ustawień usługi powiadamiania możesz wykonać następujące czynności:

- Skonfigurować ustawienia raportów, w których program Kaspersky Endpoint Security zapisuje zdarzenia.
- Skonfigurować sposób wyświetlania powiadomień.
- Skonfigurować dostarczanie powiadomień przy użyciu wiadomości e-mail.

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. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz **Raporty i pliki danych**.

   Prawa część okna wyświetla ustawienia raportów i plików danych.

3. W sekcji **Powiadomienia** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Powiadomienia**.

   Moduły i zadania programu Kaspersky Endpoint Security są wyświetlane w lewej części okna. W prawej części okna wyświetlone są zdarzenia wygenerowane dla wybranego komponentu lub zadania.

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 lokalnym dzienniku** i **Zapisz w dzienniku zdarzeń systemu Windows**.

   Zdarzenia, dla których zaznaczono pola w kolumnie **Zapisz w lokalnym dzienniku**, są wyświetlane w **Raporty aplikacji i usług**, w sekcji **Raport zdarzeń Kaspersky Lab**. Zdarzenia, dla których zaznaczono pola w kolumnie **Zapisz w dzienniku zdarzeń systemu Windows**, są wyświetlane w **Dzienniki zdarzeń Windows**, w sekcji **Aplikacja**. Aby otworzyć raporty zdarzeń, kliknij **Start → Panel sterowania → Administracja → Podgląd zdarzeń**.

6. Kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Konfigurowanie wyświetlania i dostarczania powiadomień

W celu skonfigurowania wyświetlania i dostarczania powiadomień:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz **Raporty i pliki danych**.

   Prawa część okna wyświetla ustawienia raportów i plików danych.

3. W sekcji **Powiadomienia** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Powiadomienia**.

   Moduły i zadania programu Kaspersky Endpoint Security są wyświetlane w lewej części okna. W prawej części okna wyświetlone są zdarzenia wygenerowane dla wybranego komponentu lub zadania.

4. W lewej części okna wybierz komponent lub zadanie, dla którego chcesz skonfigurować dostarczanie powiadomień.

5. W kolumnie **Powiadomienia 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 **Poczta elektroniczna** zaznacz pola obok żądanych zdarzeń.

   Informacje o wybranych zdarzeniach są dostarczane za pośrednictwem poczty elektronicznej, jeśli skonfigurowano ustawienia dostarczania powiadomień e-mail.

7. Kliknij przycisk **Ustawienia powiadamiania przy użyciu e-mail**.

   Ten przycisk otwiera okno **Ustawienia powiadamiania przy użyciu e-mail**.

8. Zaznacz pole **Wysyłaj powiadomienia o zdarzeniach**, aby włączyć dostarczanie informacji o zdarzeniach Kaspersky Endpoint Security wybranych w kolumnie **Poczta elektroniczna**.

9. Określ ustawienia dostarczania powiadomień e-mail.

10. Kliknij **OK**.

11. W oknie **Ustawienia powiadamiania przy użyciu e-mail** kliknij **OK**.

12. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Konfigurowanie wyświetlania komunikatów o stanie aplikacji w obszarze powiadomień

W celu skonfigurowania wyświetlania komunikatów o stanie aplikacji w obszarze powiadomień:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz **Interfejs**.

   Ustawienia interfejsu Kaspersky Endpoint Security zostaną wyświetlone w prawej części okna.

3. W sekcji **Ostrzeżenia** zaznacz pola obok tych kategorii zdarzeń, o których chcesz być informowany w obszarze powiadomień systemu Microsoft Windows.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Jeśli wystąpią zdarzenia skojarzone z wybraną kategorią, ikon aplikacji w obszarze powiadomień paska zadań zmieni się na lub (w zależności od powagi komunikatu).

Zarządzanie Kwarantanną i Kopią zapasową

Sekcja ta opisuje sposób konfiguracji i zarządzania Kwarantanną i Kopią zapasową.

Informacje o Kwarantannie i Kopii zapasowej

Kwarantanna jest listą prawdopodobnie zainfekowanych plików. *Prawdopodobnie zainfekowane pliki* są to pliki, które zawierają wirusy i inne zagrożenia lub ich modyfikacje.

Kiedy Kaspersky Endpoint Security poddaje kwarantannie potencjalnie zainfekowany plik, nie kopiuje go, ale przenosi: usuwa plik z dysku twardego lub wiadomości e-mail i zapisuje w specjalnym miejscu przechowywania danych. Pliki w folderze kwarantanny zapisywane są w specjalnym formacie i nie stanowią zagrożenia.

Kaspersky Endpoint Security może wykryć prawdopodobnie zainfekowany plik i poddać go kwarantannie podczas skanowania antywirusowego, a także podczas działania komponentów: Ochrona plików, Ochrona poczty oraz Kontrola systemu.

Kaspersky Endpoint Security umieszcza pliki w Kwarantannie w następujących przypadkach:

- Kod pliku przypomina znany szkodliwy program lub ma strukturę podobną do szkodliwego obiektu i nie jest zarejestrowany w bazie danych Kaspersky Endpoint Security. W tym przypadku plik zostaje przeniesiony do Kwarantanny po przeprowadzeniu analizy heurystycznej przez Ochronę plików lub Ochronę poczty lub podczas skanowania antywirusowego. Analiza heurystyczna generuje bardzo mało fałszywych alarmów.

- Sekwencja działań wykonanych przez plik jest niebezpieczna. W tym przypadku plik jest umieszczany w Kwarantannie po przeprowadzeniu analizy jego zachowań przez Kontrolę systemu.

Kopia zapasowa to lista kopii zapasowych plików, które w wyniku procesu leczenia zostały usunięte lub zmodyfikowane. *Kopia zapasowa* to kopia pliku, która została utworzona przy pierwszej próbie wyleczenia lub usunięcia tego pliku. Kopie zapasowe plików są przechowywane w specjalnym formacie i nie stanowią zagrożenia.

Czasami niemożliwe jest zachowanie integralności plików w trakcie leczenia. W przypadku częściowej lub całkowitej utraty dostępu do istotnych informacji wyleczonego pliku, można spróbować przywrócić wyleczoną kopię pliku do jego oryginalnego folderu.

Możliwe, że po kolejnej aktualizacji baz danych lub modułów aplikacji, Kaspersky Endpoint Security będzie w stanie dokładnie zidentyfikować i zneutralizować zagrożenie. Z tego powodu, zalecane jest skanowanie plików poddanych kwarantannie po każdej aktualizacji baz danych i modułów aplikacji.

Konfigurowanie ustawień Kwarantanny i Kopii zapasowej

Miejsce przechowywania danych składa się z Kwarantanny i Kopii zapasowej. Konfigurowanie ustawień Kwarantanny i Kopii zapasowej polega na:

- Konfigurowaniu maksymalnego czasu przechowywania plików w Kwarantannie i Kopii zapasowej.

  Domyślnie czas ten wynosi 30 dni. Po minięciu zdefiniowanego czasu, Kaspersky Endpoint Security usunie najstarsze pliki z miejsca przechowywania danych. Możesz wyłączyć ograniczenie czasu przechowywania plików lub zmienić jego maksymalną wartość.

- Możesz skonfigurować maksymalny rozmiar Kwarantanny i Kopii zapasowej.

Domyślnie maksymalny rozmiar Kwarantanny i Kopii zapasowej wynosi 100 MB. Gdy miejsce przechowywania danych osiągnie zdefiniowaną wartość, Kaspersky Endpoint Security automatycznie usunie najstarsze pliki z Kwarantanny i Kopii zapasowej, aby maksymalny rozmiar miejsca przechowywania nie został przekroczony. Możesz wyłączyć ograniczenie rozmiaru Kwarantanny i Kopii zapasowej lub zmienić jego maksymalną wartość.

Konfigurowanie maksymalnego czasu przechowywania plików w Kwarantannie i Kopii zapasowej

W celu skonfigurowania maksymalnego czasu przechowywania plików w Kwarantannie i Kopii zapasowej:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz **Raporty i pliki danych**.
3. Wykonaj jedną z poniższych czynności:
   - Aby ograniczyć czas przechowywania plików w Kwarantannie i Kopii zapasowej, w prawej części okna, w sekcji **Ustawienia Kwarantanny oraz Kopii zapasowej** zaznacz pole **Przechowuj obiekty nie dłużej niż**. W polu po prawej stronie pola **Przechowuj obiekty nie dłużej niż** określ maksymalny czas przechowywania plików w Kwarantannie i Kopii zapasowej. Domyślnie czas ten wynosi 30 dni.
   - Aby anulować ograniczenie czasu przechowywania plików w Kwarantannie i Kopii zapasowej, w prawej części okna, w sekcji **Ustawienia Kwarantanny oraz Kopii zapasowej** odznacz pole **Przechowuj obiekty nie dłużej niż**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Konfigurowanie maksymalnego rozmiaru Kwarantanny i Kopii zapasowej

W celu skonfigurowania maksymalnego rozmiaru Kwarantanny i Kopii zapasowej:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz **Raporty i pliki danych**.
3. Wykonaj jedną z poniższych czynności:
   - Jeśli chcesz ograniczyć całkowity rozmiar Kwarantanny i Kopii zapasowej, w prawej części okna, w sekcji **Ustawienia Kwarantanny oraz Kopii zapasowej** zaznacz pole **Maksymalny rozmiar magazynu** i w polu po jego prawej stronie określ **maksymalny rozmiar** Kwarantanny i Kopii zapasowej.

     Domyślnie, maksymalny rozmiar magazynu danych zawierającego katalogi Kwarantanny i Kopii zapasowej wynosi 100 MB.
   - Jeśli chcesz usunąć ograniczenie rozmiaru Kwarantanny i Kopii zapasowej, w prawej części okna, w sekcji **Ustawienia Kwarantanny oraz Kopii zapasowej** odznacz pole **Maksymalny rozmiar magazynu**.

   Domyślnie rozmiar Kwarantanny i Kopii zapasowej jest nieograniczony.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Zarządzanie Kwarantanną

Kaspersky Endpoint Security automatycznie usuwa pliki posiadające dowolny stan z Kwarantanny po upłynięciu czasu przechowywania, zdefiniowanego w ustawieniach aplikacji.

Podczas zarządzania Kwarantanną możliwe są następujące operacje na plikach:

- Wyświetlanie plików poddanych kwarantannie przez program Kaspersky Endpoint Security.
- Skanowanie prawdopodobnie zainfekowanych plików przy użyciu bieżących wersji modułów i baz danych Kaspersky Endpoint Security.
- Przywracanie plików z Kwarantanny do folderów, z których zostały przeniesione.
- Usuwanie plików z Kwarantanny.
- Otwieranie folderu, w którym pierwotnie znajdowały się pliki.

Zestaw plików poddanych kwarantannie jest przedstawiony w postaci tabeli.

Podczas zarządzania danymi w tabeli możesz również wykonywać następujące czynności:

- Filtrować pliki poddane kwarantannie w oparciu o kolumny i warunki filtru niestandardowego.
- Korzystać z funkcji wyszukiwania plików poddanych kwarantannie.
- Sortować pliki poddane kwarantannie.
- Zmieniać kolejność i zestaw kolumn wyświetlanych w tabeli plików poddanych kwarantannie.

Możesz skopiować wybrane zdarzenia Kwarantanny do schowka. Aby wybrać kilka plików poddanych kwarantannie, kliknij dowolny plik prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Wybierz wszystkie**. Aby odznaczyć pliki, których nie chcesz skanować, kliknij je, trzymając wciśnięty klawisz **CTRL**.

Włączanie i wyłączanie skanowania plików w Kwarantannie po aktualizacji

Jeżeli podczas skanowania pliku Kaspersky Endpoint Security wykryje oznaki infekcji, ale nie będzie mógł określić, jaki szkodliwy program jest jej źródłem, wówczas przeniesie ten plik do Kwarantanny. Po aktualizacji baz danych i modułów, Kaspersky Endpoint Security będzie mógł jednoznacznie rozpoznać i zneutralizować zagrożenie. Możesz włączyć automatyczne skanowanie plików w Kwarantannie po każdej aktualizacji baz danych i modułów aplikacji.

Zalecamy regularne skanowanie plików w Kwarantannie. Skanowanie może zmienić stan plików. Niektóre pliki mogą zostać wyleczone i przywrócone do ich pierwotnej lokalizacji, co umożliwi dalszą pracę z nimi.

W celu włączenia skanowania plików poddanych kwarantannie po aktualizacji:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz **Raporty i pliki danych**.

   W prawej części okna wyświetlone są ustawienia zarządzania raportami i miejscami przechowywania.

3. W sekcji **Ustawienia Kwarantanny oraz Kopii zapasowej** należy wykonać jedną z następujących czynności:

   - Aby włączyć skanowanie plików poddanych kwarantannie po każdej aktualizacji Kaspersky Endpoint Security, zaznacz pole **Przeskanuj Kwarantannę po aktualizacji**.

   - Aby wyłączyć skanowanie plików poddanych kwarantannie po każdej aktualizacji Kaspersky Endpoint Security, usuń zaznaczenie z pola **Przeskanuj Kwarantannę po aktualizacji**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Uruchamianie zadania Skanowanie obiektów dla plików znajdujących się w Kwarantannie

Możliwe, że po kolejnej aktualizacji baz danych i modułów aplikacji, Kaspersky Endpoint Security dokładnie zidentyfikuje zagrożenie w pliku poddanym kwarantannie oraz zneutralizuje je. Jeżeli aplikacja nie jest skonfigurowana do skanowania plików poddanych kwarantannie automatycznie po każdej aktualizacji baz danych i modułów aplikacji, możesz ręcznie uruchomić zadanie Skanowanie obiektów dla plików w Kwarantannie.

W celu uruchomienia Skanowania obiektów dla plików poddanych kwarantannie:

1. Otwórz okno główne aplikacji.

2. W górnej części okna głównego aplikacji kliknij odnośnik **Kwarantanna**, aby otworzyć okno **Pliki danych**.

   Zostanie otwarte okno **Pliki danych** na zakładce **Kwarantanna**.

3. Na zakładce **Kwarantanna** wybierz jeden lub kilka prawdopodobnie zainfekowanych plików, które chcesz przeskanować.

   Aby wybrać kilka plików poddanych kwarantannie, kliknij dowolny plik prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Wybierz wszystkie**. Aby odznaczyć pliki, których nie chcesz skanować, kliknij je, trzymając wciśnięty klawisz **CTRL**.

4. Skanowanie obiektów można uruchomić w jeden z następujących sposobów:

   - Kliknij przycisk **Skanuj ponownie**.

   - Kliknij obiekt prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Skanuj ponownie**.

Po zakończeniu skanowania pojawi się powiadomienie o liczbie przeskanowanych plików i liczbie wykrytych zagrożeń.

Przywracanie plików z Kwarantanny

W celu przywrócenia plików z Kwarantanny:

1. Otwórz okno główne aplikacji.

2. W górnej części okna głównego aplikacji kliknij odnośnik **Kwarantanna**, aby otworzyć okno **Pliki danych**.

   Zostanie otwarte okno **Pliki danych** na zakładce **Kwarantanna**.

3. Jeśli chcesz przywrócić wszystkie pliki poddane kwarantannie, z menu kontekstowego dowolnego pliku wybierz **Przywróć wszystkie**.

   Kaspersky Endpoint Security przywróci wszystkie pliki z Kwarantanny do ich oryginalnych folderów.

4. W celu przywrócenia jednego lub kilku plików poddanych kwarantannie:

   a. Na zakładce **Kwarantanna** wybierz jeden lub kilka plików, które chcesz przywrócić z Kwarantanny.

      Aby wybrać kilka plików poddanych kwarantannie, kliknij dowolny plik prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Wybierz wszystkie**. Aby odznaczyć pliki, których nie chcesz skanować, kliknij je, trzymając wciśnięty klawisz **CTRL**.

   b. Przywróć pliki w jeden z następujących sposobów:

      - Kliknij przycisk **Przywróć**.
      - Kliknij plik prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Przywróć**.

   Kaspersky Endpoint Security przywróci wybrane pliki do ich oryginalnych folderów.

Usuwanie plików z Kwarantanny

W celu usunięcia plików z Kwarantanny:

1. Otwórz okno główne aplikacji.
2. W górnej części okna głównego aplikacji kliknij odnośnik **Kwarantanna**, aby otworzyć okno **Pliki danych**.

   Zostanie otwarte okno **Pliki danych** na zakładce **Kwarantanna**.

3. Jeśli chcesz usunąć wszystkie pliki z Kwarantanny, z menu kontekstowego dowolnego pliku wybierz **Usuń wszystkie**.

   Kaspersky Endpoint Security usunie wszystkie pliki z Kwarantanny.

4. W celu usunięcia jednego lub kilku plików poddanych kwarantannie:

   a. Z tabeli dostępnej na zakładce **Kwarantanna** wybierz jeden lub kilka prawdopodobnie zainfekowanych plików, które chcesz usunąć z Kwarantanny.

      Aby wybrać kilka plików poddanych kwarantannie, kliknij dowolny plik prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Wybierz wszystkie**. Aby odznaczyć pliki, których nie chcesz skanować, kliknij je, trzymając wciśnięty klawisz **CTRL**.

   b. Usuń pliki w jeden z następujących sposobów:

      - Kliknij przycisk **Usuń**.
      - Kliknij go prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Usuń**.

   Kaspersky Endpoint Security usunie wybrane pliki z Kwarantanny.

Zarządzanie Kopią zapasową

Jeżeli w pliku zostanie wykryty szkodliwy kod, Kaspersky Endpoint Security zablokuje plik, 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.

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).

Kaspersky Endpoint Security automatycznie usuwa kopie zapasowe plików posiadające dowolny stan z Kopii zapasowej po upłynięciu czasu przechowywania, zdefiniowanego w ustawieniach aplikacji.

Możesz także ręcznie usunąć dowolną kopię pliku z folderu Kopii zapasowej.

Zestaw kopii zapasowych plików jest przedstawiony w postaci tabeli.

Podczas zarządzania Kopią zapasową możesz wykonywać następujące działania na kopiach zapasowych plików:

- Przeglądać zestaw kopii zapasowych plików.
- Przywracać pliki z kopii zapasowych do ich oryginalnych folderów.
- Usuwać kopie zapasowe plików z Kopii zapasowej.

Podczas zarządzania danymi w tabeli możesz również wykonywać następujące czynności:

- Filtrować kopie zapasowe według kolumn lub niestandardowego warunku filtrowania.
- Użyć opcji wyszukiwania kopii zapasowej.
- Sortować kopie zapasowe.
- Zmieniać kolejność i zestaw kolumn wyświetlanych w tabeli kopii zapasowych.

Możesz skopiować wybrane zdarzenia Kopii zapasowej do schowka. Aby wybrać kilka plików Kopii zapasowej, kliknij dowolny plik prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Wybierz wszystkie**. Aby odznaczyć pliki, których nie chcesz skanować, kliknij je, trzymając wciśnięty klawisz **CTRL**.

Przywracanie plików z Kopii zapasowej

W celu przywrócenia plików z Kopii zapasowej:

1. Otwórz okno główne aplikacji.
2. W górnej części okna głównego aplikacji kliknij odnośnik **Kwarantanna**, aby otworzyć okno **Pliki danych**.
3. W oknie **Pliki danych** wybierz zakładkę **Kopia zapasowa**.

4. Jeśli chcesz przywrócić wszystkie pliki z Kopii zapasowej, z menu kontekstowego dowolnego pliku wybierz **Przywróć wszystkie**.

   Kaspersky Endpoint Security przywróci wszystkie pliki z kopii zapasowych do ich oryginalnych folderów.

5. W celu przywrócenia jednego lub kilku plików z Kopii zapasowej:

   a. Z tabeli dostępnej na zakładce **Kopia zapasowa** wybierz jeden lub kilka plików Kopii zapasowej.

      Aby wybrać kilka plików poddanych kwarantannie, kliknij dowolny plik prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Wybierz wszystkie**. Aby odznaczyć pliki, których nie chcesz skanować, kliknij je, trzymając wciśnięty klawisz **CTRL**.

   b. Przywróć pliki w jeden z następujących sposobów:

      - Kliknij przycisk **Przywróć**.
      - Kliknij plik prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Przywróć**.

   Kaspersky Endpoint Security przywróci wszystkie pliki z wybranych kopii zapasowych do ich oryginalnych folderów.

Usuwanie kopii zapasowych plików z Kopii zapasowej

W celu usunięcia kopii zapasowej pliku z Kopii zapasowej:

1. Otwórz okno główne aplikacji.
2. W górnej części okna głównego aplikacji kliknij odnośnik **Kwarantanna**, aby otworzyć okno **Pliki danych**.
3. W oknie **Pliki danych** wybierz zakładkę **Kopia zapasowa**.
4. Jeśli chcesz usunąć wszystkie pliki z Kopii zapasowej, wykonaj jedną z następujących czynności:
   - Z menu kontekstowego pliku wybierz **Usuń wszystkie**.
   - Kliknij przycisk **Wyczyść magazyn**.

   Kaspersky Endpoint Security usunie wszystkie kopie zapasowe plików z Kopii zapasowej.

5. Jeśli chcesz usunąć jeden lub więcej plików z Kopii zapasowej:

   a. Z tabeli dostępnej na zakładce **Kopia zapasowa** wybierz jeden lub kilka plików Kopii zapasowej.

      Aby wybrać kilka plików Kopii zapasowej, kliknij dowolny plik prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Wybierz wszystkie**. Aby odznaczyć pliki, których nie chcesz skanować, kliknij je, trzymając wciśnięty klawisz **CTRL**.

   b. Usuń pliki w jeden z następujących sposobów:

      - Kliknij przycisk **Usuń**.
      - Kliknij go prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Usuń**.

   Kaspersky Endpoint Security usunie wybrane kopie zapasowe plików z Kopii zapasowej.

Zaawansowane ustawienia aplikacji

Sekcja ta opisuje zaawansowane ustawienia programu Kaspersky Endpoint Security oraz sposób ich konfiguracji.

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. Otwórz okno ustawień aplikacji.
2. W lewej części okna wybierz sekcję **Ustawienia zaawansowane**.

   W prawej części okna wyświetlone są zaawansowane ustawienia aplikacji.
3. W sekcji **Zarządzanie ustawieniami** kliknij przycisk **Zapisz**.

   Zostanie otwarte standardowe okno **Proszę wybrać plik konfiguracyjny** z Microsoft Windows.
4. 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. Otwórz okno ustawień aplikacji.
2. W lewej części okna wybierz sekcję **Ustawienia zaawansowane**.

   W prawej części okna wyświetlone są zaawansowane ustawienia aplikacji.
3. W sekcji **Zarządzanie ustawieniami** kliknij przycisk **Otwórz**.

   Zostanie otwarte standardowe okno **Proszę wybrać plik konfiguracyjny** z Microsoft Windows.
4. Określ ścieżkę dostępu do pliku konfiguracyjnego.
5. Kliknij przycisk **Otwórz**.

Wszystkie wartości ustawień Kaspersky Endpoint Security zostaną ustawione zgodnie z wybranym plikiem konfiguracyjnym.

Strefa zaufana

Sekcja ta zawiera informacje dotyczące strefy zaufanej oraz instrukcję konfigurowania wykluczeń skanowania i tworzenia listy zaufanych aplikacji.

Informacje o strefie zaufanej

Strefa zaufana jest utworzoną przez administratora listą obiektów i aplikacji, które nie są monitorowane przez Kaspersky Endpoint Security. Innymi słowy, jest to zestaw wykluczeń ze skanowania.

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.

Ze skanowania możesz wykluczyć następujące obiekty:

- Pliki o określonych formatach
- Pliki wybierane w oparciu o maskę
- Wybrane pliki
- Foldery
- Procesy aplikacji

Wykluczenia ze skanowania

Wykluczenie ze skanowania to zestaw warunków, zgodnie z którymi Kaspersky Endpoint Security nie skanuje 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 jako dodatkowy składnik złośliwego programu. Przykładami takich aplikacji są narzędzia do zdalnej administracji, klienty IRC, serwery FTP, różne narzędzia do zatrzymywania lub ukrywania procesów, keyloggery, aplikacje służące do łamania haseł i auto-dialery. Takie aplikacje nie są klasyfikowane jako wirusy. Szczegółowe informacje o legalnym oprogramowaniu, które może zostać użyte przez cyberprzestępców do uszkodzenia komputera lub danych osobistych, znajdują się na stronie Encyklopedii Wirusów Kaspersky pod adresem http://www.securelist.pl/threats/detect.html.

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 Wirusów Kaspersky. Na przykład: użytkownik regularnie korzysta z programu Remote Administrator. Jest to aplikacja do zdalnej administracji umożliwiająca pracę na zdalnym komputerze. 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 wirusów 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:

- Ochrona plików
- Ochrona poczty.
- Ochrona WWW.
- Kontrola uprawnień aplikacji.
- Zadania skanowania
- Kontrola systemu.

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 dowolnego programu i monitoruje aktywność wszystkich aplikacji oraz ruch sieciowy będący wynikiem ich działania. Kaspersky Endpoint Security wykluczy ze skanowania aplikacje znajdujące się na liście zaufanych aplikacji.

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 Securit 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.

Tworzenie wykluczenia ze 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.

W celu utworzenia wykluczenia ze skanowania:

1. Otwórz okno ustawień aplikacji.
2. Wybierz sekcję **Ochrona antywirusowa** znajdującą się po lewej stronie.

W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.

3. W sekcji **Wykluczenia ze skanowania i zaufane aplikacje** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Strefa zaufana** na zakładce **Wykluczenia ze skanowania**.

4. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Wykluczenie ze skanowania**. W tym oknie możesz utworzyć wykluczenie ze skanowania przy użyciu jednego lub kilku kryteriów z sekcji **Właściwości**.

5. 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 **Przeglądaj**.

      W masce nazwy pliku lub folderu możesz użyć gwiazdki (*) zamiast dowolnego zestawu znaków.

      Na przykład, możesz użyć masek w celu dodania następujących ścieżek:

      - Ścieżki do plików znajdujących się w dowolnym folderze:
        - Maska „*.exe” będzie zawierała wszystkie ścieżki do plików, które posiadają rozszerzenie EXE.
        - Maska „test” będzie zawierała wszystkie ścieżki do plików o nazwie „test”.
      - Ścieżki do plików znajdujących się w określonym folderze:
        - Maska „C:\dir*.*” będzie zawierała wszystkie ścieżki do plików znajdujących się w folderze C:\dir\, ale nie w podfolderach C:\dir\.
        - Maska „C:\dir*” będzie zawierała wszystkie ścieżki do plików znajdujących się w folderze C:\dir\, ale nie w podfolderach C:\dir\.
        - Maska „C:\dir\” będzie zawierała wszystkie ścieżki do plików znajdujących się w folderze C:\dir\, ale nie w podfolderach C:\dir\.
        - Maska „C:\dir*.exe” będzie zawierała wszystkie ścieżki do plików z rozszerzeniem EXE, znajdujących się w folderze C:\dir\, ale nie w podfolderach C:\dir\.
        - Maska „C:\dir\test” będzie zawierała wszystkie ścieżki do plików o nazwie „test” znajdujących się w folderze C:\dir\, ale nie w podfolderach C:\dir\.
        - Maska „C:\dir*\test” będzie zawierała wszystkie ścieżki do plików o nazwie „test” znajdujących się w folderze C:\dir\ i w podfolderach C:\dir\.
      - Ścieżki do plików znajdujących się we wszystkich folderach z określoną nazwą:
        - Maska „dir*.*” będzie zawierała wszystkie ścieżki do plików w folderach o nazwie „dir”, ale nie w podfolderach tych folderów.
        - Maska „dir*” będzie zawierała wszystkie ścieżki do plików w folderach o nazwie „dir”, ale nie w podfolderach tych folderów.

- Maska „dir\” będzie zawierała wszystkie ścieżki do plików w folderach o nazwie „dir”, ale nie w podfolderach tych folderów.
- Maska „dir*.exe” będzie zawierała wszystkie ścieżki do plików z rozszerzeniem EXE, znajdujących się w folderach o nazwie „dir”, ale nie w podfolderach tych folderów.
- Maska „dir\test” będzie zawierała wszystkie ścieżki do plików o nazwie „test”, znajdujących się w folderach o nazwie „dir”, ale nie w podfolderach tych folderów.

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**.

6. 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 obiektu lub maskę nazwy zgodnie z klasyfikacją Encyklopedii wirusów Kaspersky:

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**.

7. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.

8. Wskaż moduły programu Kaspersky Endpoint Security, które będą używać wykluczenia ze skanowania:

a. Po kliknięcie 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.

9. W oknie **Wykluczenie ze skanowania** kliknij **OK**.

Dodane wykluczenie ze skanowania pojawi się na zakładce **Wykluczenia ze skanowania** okna **Strefa zaufana**. Skonfigurowane ustawienia tego wykluczenia pojawią się w sekcji **Opis wykluczenia ze skanowania**.

10. W oknie **Strefa zaufana** kliknij **OK**.

11. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Modyfikowanie wykluczenia ze skanowania

W celu zmodyfikowania wykluczenia ze skanowania:

1. Otwórz okno ustawień aplikacji.
2. Wybierz sekcję **Ochrona antywirusowa** znajdującą się po lewej stronie.
   W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.
3. W sekcji **Wykluczenia ze skanowania i zaufane aplikacje** kliknij przycisk **Ustawienia**.
   Zostanie otwarte okno **Strefa zaufana** na zakładce **Wykluczenia ze skanowania**.
4. Na liście wybierz wykluczenie ze skanowania, które chcesz zmodyfikować.
5. Zmień ustawienia wykluczenia ze skanowania w jeden z następujących sposobów:
   - Kliknij przycisk **Modyfikuj**.
     Zostanie otwarte okno **Wykluczenia ze skanowania**.
   - Otwórz okno do modyfikacji żądanego ustawienia, klikając odnośnik w polu **Opis wykluczenia ze skanowania**.
6. Jeśli w poprzednim kroku kliknąłeś przycisk **Modyfikuj**, w oknie **Wykluczenie ze skanowania** kliknij **OK**.
   Zmodyfikowane ustawienia tego wykluczenia ze skanowania pojawią się w sekcji **Opis wykluczenia ze skanowania**.
7. W oknie **Strefa zaufana** kliknij **OK**.
8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Usuwanie wykluczenia ze skanowania

W celu usunięcia wykluczenia skanowania:

1. Otwórz okno ustawień aplikacji.
2. Wybierz sekcję **Ochrona antywirusowa** znajdującą się po lewej stronie.
   W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.
3. W sekcji **Wykluczenia ze skanowania i zaufane aplikacje** kliknij przycisk **Ustawienia**.
   Zostanie otwarte okno **Strefa zaufana** na zakładce **Wykluczenia ze skanowania**.
4. Na liście wykluczeń ze skanowania wybierz żądane wykluczenie.
5. Kliknij przycisk **Usuń**.
   Usunięte wykluczenie zniknie z listy.
6. W oknie **Strefa zaufana** kliknij **OK**.

7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Włączanie i wyłączanie wykluczenia ze skanowania

W celu włączenia lub wyłączenia wykluczenia ze skanowania:

1. Otwórz okno ustawień aplikacji.
2. Wybierz sekcję **Ochrona antywirusowa** znajdującą się po lewej stronie.
   W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.
3. W sekcji **Wykluczenia ze skanowania i zaufane aplikacje** kliknij przycisk **Ustawienia**.
   Zostanie otwarte okno **Strefa zaufana** na zakładce **Wykluczenia ze skanowania**.
4. Na liście wykluczeń ze skanowania wybierz żądane wykluczenie.
5. Wykonaj jedną z poniższych czynności:
   - Aby włączyć wykluczenie ze skanowania, zaznacz pole obok jego nazwy.
   - Aby wyłączyć wykluczenie ze skanowania, odznacz pole obok jego nazwy.
6. Kliknij **OK**.
7. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Modyfikowanie listy zaufanych aplikacji

W celu zmodyfikowania listy zaufanych aplikacji:

1. Otwórz okno ustawień aplikacji.
2. Wybierz sekcję **Ochrona antywirusowa** znajdującą się po lewej stronie.
   W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.
3. W sekcji **Wykluczenia ze skanowania i zaufane aplikacje** kliknij przycisk **Ustawienia**.
   Zostanie otwarte okno **Strefa zaufana**.
4. W oknie **Strefa zaufana** przejdź na zakładkę **Zaufane aplikacje**.
5. W celu dodania aplikacji do listy zaufanych aplikacji:
   a. Kliknij przycisk **Dodaj**.
   b. Z otwartego menu kontekstowego wybierz:
      - **Aplikacje**, jeśli chcesz odszukać aplikację na liście aplikacji zainstalowanych na komputerze.
        Zostanie otwarte okno **Wybierz aplikację**.

- **Przeglądaj**, jeśli chcesz określić ścieżkę dostępu do pliku wykonywalnego odpowiedniej aplikacji.

  Zostanie otwarte standardowe okno **Otwórz plik** z Microsoft Windows.

c. Wybierz aplikację na jeden z następujących sposobów:

- Jeśli w poprzednim kroku wybrałeś **Aplikacje**, wybierz aplikację na liście aplikacji zainstalowanych na komputerze i w oknie **Wybierz aplikację** kliknij **OK**.
- Jeśli w poprzednim kroku wybrałeś **Przeglądaj**, określ ścieżkę dostępu do pliku wykonywalnego odpowiedniej aplikacji, a następnie w standardowym oknie **Otwórz** systemu Microsoft Windows kliknij przycisk **Otwórz**.

Działania te spowodują otwarcie okna **Wykluczenia ze skanowania dla aplikacji**.

a. Zaznacz pola obok reguł strefy zaufanej odpowiednich dla wybranej aplikacji:

- **Nie skanuj otwieranych plików**.
- **Nie monitoruj aktywności aplikacji**.
- **Nie dziedzicz ograniczeń nadrzędnego procesu (aplikacji)**.
- **Nie monitoruj aktywności aplikacji potomnych**.
- **Nie blokuj interakcji z interfejsem aplikacji**.
- **Nie skanuj ruchu sieciowego**.

b. Kliknij **OK** w oknie **Wykluczenia ze skanowania dla aplikacji**.

Dodana zaufana aplikacja pojawi się na liście zaufanych aplikacji.

6. W celu zmodyfikowania ustawień zaufanej aplikacji:

a. Z listy zaufanych aplikacji wybierz zaufaną aplikację.

b. Kliknij przycisk **Modyfikuj**.

c. Zostanie otwarte okno **Wykluczenia ze skanowania dla aplikacji**.

d. Zaznacz lub odznacz pola obok reguł strefy zaufanej odpowiednich dla wybranej aplikacji.

> Jeśli w oknie **Wykluczenia ze skanowania dla aplikacji** nie wybrano żadnych reguł strefy zaufanej, zaufana aplikacja będzie uwzględniana podczas skanowania. W tej sytuacji zaufana aplikacja nie zostanie usunięta z listy zaufanych, ale zaznaczenie z pola znajdującego się obok niej będzie usunięte.

e. Kliknij **OK** w oknie **Wykluczenia ze skanowania dla aplikacji**.

7. W celu usunięcia zaufanej aplikacji z listy zaufanych aplikacji:

a. Z listy zaufanych aplikacji wybierz zaufaną aplikację.

b. Kliknij przycisk **Usuń**.

8. W oknie **Strefa zaufana** kliknij **OK**.

9. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

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. Otwórz okno ustawień aplikacji.
2. Wybierz sekcję **Ochrona antywirusowa** znajdującą się po lewej stronie.

   W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.
3. W sekcji **Wykluczenia ze skanowania i zaufane aplikacje** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Strefa zaufana**.
4. W oknie **Strefa zaufana** przejdź na zakładkę **Zaufane aplikacje**.
5. Z listy zaufanych aplikacji wybierz odpowiednią aplikację.
6. Wykonaj jedną z poniższych czynności:
   - Aby wykluczyć zaufaną aplikację ze skanowania wykonywanego przez Kaspersky Endpoint Securit, zaznacz pole obok jej nazwy.
   - Jeżeli chcesz, aby zaufana aplikacja była skanowana przez Kaspersky Endpoint Securit, usuń zaznaczenie z pola obok jej nazwy.
7. Kliknij **OK**.
8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

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. Otwórz okno ustawień aplikacji.
2. Wybierz sekcję **Ochrona antywirusowa** znajdującą się po lewej stronie.

   W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.
3. W sekcji **Wykluczenia ze skanowania i zaufane aplikacje** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Strefa zaufana**.
4. W oknie **Strefa zaufana** przejdź na zakładkę **Magazyn zaufanych certyfikatów systemowych**.
5. Zaznacz pole **Użyj magazynu zaufanych certyfikatów systemowych**.

6. Z listy rozwijalnej **Magazyn zaufanych certyfikatów systemowych** wybierz magazyn, który ma być uznawany za zaufany.

7. W oknie **Strefa zaufana** kliknij **OK**.

8. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Autoochrona Kaspersky Endpoint Security

Sekcja ta opisuje mechanizm autoochrony oraz ochrony przed kontrolą zdalną programu Kaspersky Endpoint Security, a także instrukcje dotyczące konfiguracji ustawień tych mechanizmów.

Informacje o Autoochronie Kaspersky Endpoint Security

Kaspersky Endpoint Security chroni komputer przed szkodliwymi programami, w tym programami, które usiłują zablokować działanie programu Kaspersky Endpoint Security, a nawet próbują usunąć go z komputera.

Stabilność ochrony systemu komputera jest zapewniona przez mechanizmy autoochrony i ochrony przed zdalną kontrolą dostępne w Kaspersky Endpoint Security.

Autoochrona uniemożliwia modyfikowanie i usuwanie plików aplikacji, procesów pamięci i wpisów w rejestrze systemowym.

Ochrona przed zdalną kontrolą blokuje wszystkie próby kontrolowania usług aplikacji z poziomu zdalnego komputera.

Na komputerach działających pod kontrolą 64-bitowych systemów operacyjnych wyłącznie autoochrona Kaspersky Endpoint Security zapobiega wprowadzaniu zmian i usuwaniu plików aplikacji na dysku twardym oraz wpisów w rejestrze systemu.

Włączanie i wyłączanie Autoochrony

Domyślnie Autoochrona programu Kaspersky Endpoint Security jest włączona. W razie konieczności możesz ją wyłączyć.

W celu włączenia lub wyłączenia Autoochrony:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna wybierz sekcję **Ustawienia zaawansowane**.

   W prawej części okna wyświetlone są zaawansowane ustawienia aplikacji.

3. Wykonaj jedną z poniższych czynności:

   - Aby włączyć mechanizm autoochrony, zaznacz pole **Włącz autoochronę**.
   - Aby wyłączyć mechanizm autoochrony, usuń zaznaczenie z pola **Włącz autoochronę**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Włączanie i wyłączanie ochrony przed zdalną kontrolą

Domyślnie mechanizm ochrony przed kontrolą zdalną jest włączony. W razie konieczności możesz go wyłączyć.

W celu włączenia lub wyłączenia mechanizmu ochrony przed zdalną kontrolą:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna wybierz sekcję **Ustawienia zaawansowane**.
   W prawej części okna wyświetlone są zaawansowane ustawienia aplikacji.
3. Wykonaj jedną z poniższych czynności:
   - Aby włączyć ochronę przed zdalną kontrolą, zaznacz pole **Wyłącz możliwość zewnętrznego zarządzania usługą systemową**.
   - Aby wyłączyć ochronę przed zdalną kontrolą, usuń zaznaczenie z pola **Wyłącz możliwość zewnętrznego zarządzania usługą systemową**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Obsługiwanie aplikacji do zdalnej administracji

Czasami możesz potrzebować aplikacji do zdalnej administracji, gdy włączona jest ochrona przed kontrolą zewnętrzną.

W celu włączenia działania aplikacji do zdalnej administracji:

1. Otwórz okno ustawień aplikacji.
2. Wybierz sekcję **Ochrona antywirusowa** znajdującą się po lewej stronie.
   W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.
3. W sekcji **Wykluczenia ze skanowania i zaufane aplikacje** kliknij przycisk **Ustawienia**.
   Zostanie otwarte okno **Strefa zaufana**.
4. W oknie **Strefa zaufana** przejdź na zakładkę **Zaufane aplikacje**.
5. Kliknij przycisk **Dodaj**.
6. Z otwartego menu kontekstowego wybierz:
   - **Aplikacje**, aby odszukać aplikację do zdalnej administracji na liście aplikacji zainstalowanych na komputerze.
     Zostanie otwarte okno **Wybierz aplikację**.
   - **Przeglądaj**, aby określić ścieżkę dostępu do pliku wykonywalnego aplikacji do zdalnej administracji.
     Zostanie otwarte standardowe okno **Otwórz plik** z Microsoft Windows.

7. Wybierz aplikację na jeden z następujących sposobów:

   - Jeśli w poprzednim kroku wybrałeś **Aplikacje**, wybierz aplikację na liście aplikacji zainstalowanych na komputerze i w oknie **Wybierz aplikację** kliknij **OK**.

   - Jeśli w poprzednim kroku wybrałeś **Przeglądaj**, określ ścieżkę dostępu do pliku wykonywalnego odpowiedniej aplikacji, a następnie w standardowym oknie **Otwórz** systemu Microsoft Windows kliknij przycisk **Otwórz**.

   Działania te spowodują otwarcie okna **Wykluczenia ze skanowania dla aplikacji**.

8. Zaznacz pole **Nie monitoruj aktywności aplikacji**.

9. Kliknij **OK** w oknie **Wykluczenia ze skanowania dla aplikacji**.

   Dodana zaufana aplikacja pojawi się na liście zaufanych aplikacji.

10. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Wydajność Kaspersky Endpoint Security i kompatybilność z innymi aplikacjami

Sekcja ta zawiera informacje o wydajności programu Kaspersky Endpoint Security i jego kompatybilności z innymi aplikacjami. Znaleźć tu można również wskazówki dotyczące wybierania typów wykrywanych obiektów i trybu działania Kaspersky Endpoint Security.

Informacje o wydajności programu Kaspersky Endpoint Security i jego kompatybilności 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 Pełnego skanowania
- Zadanie Skanowania obszarów krytycznych
- Zadanie Skanowania obiektów
- Zadanie Wykrywania luk
- Zadanie Sprawdzanie integralności

Niezależnie od tego, czy tryb oszczędzania energii jest włączony, Kaspersky Endpoint Security wstrzymuje zadania szyfrowania po przejściu komputera przenośnego do trybu pracy na bateriach. Aplikacja wznawia zadania szyfrowania po przejściu komputera przenośnego z trybu pracy na bateriach do trybu głównego.

Udostępnianie zasobów komputera innym aplikacjom

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 oprogramowanie może 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 programów, 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 plików z powodu specyfiki Kaspersky Endpoint Security dla serwerów plików. 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 plików, włącz technologię Zaawansowanego leczenia dla serwerów plików i uruchom grupowe zadanie *Skanowania antywirusowego* w momencie wygodnym dla użytkowników serwera plików.

Wybieranie typów wykrywanych obiektów

W celu wybrania typów wykrywanych obiektów:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna wybierz sekcję **Ochrona antywirusowa**.

   W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.
3. W sekcji **Obiekty** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Wykrywane obiekty**.
4. Zaznacz pola obok typów obiektów, które mają być wykrywane przez Kaspersky Endpoint Security:
   - **Szkodliwe narzędzia**
   - **Adware**
   - **Auto-dialery**
   - **Inne**
   - **Spakowane pliki, które mogą wyrządzić szkody**
   - **Pliki wielokrotnie spakowane**
5. Kliknij **OK**.

   Okno **Wykrywane obiekty** zostanie zamknięte. W sekcji **Obiekty**, pod nagłówkiem **Włączone jest wykrywanie następujących rodzajów obiektów** wymienione są wybrane typy obiektów.
6. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Włączanie i wyłączanie Technologii zaawansowanego leczenia dla stacji roboczych

W celu włączenia lub wyłączenia Technologii zaawansowanego leczenia dla stacji roboczych:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna wybierz sekcję **Ochrona antywirusowa**.

   W prawej części okna wyświetlone są ustawienia ochrony antywirusowej.
3. W prawej części okna wykonaj jedną z poniższych czynności:

- Aby włączyć technologię zaawansowanego leczenia, zaznacz opcję **Włącz technologię zaawansowanego leczenia**.
- Aby wyłączyć technologię zaawansowanego leczenia, usuń zaznaczenie z opcji **Włącz technologię zaawansowanego leczenia**.

4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Jeśli zadanie zaawansowanego leczenia jest uruchamiane z poziomu Kaspersky Security Center, większość funkcji systemu operacyjnego jest niedostępna dla użytkownika. Po zakończeniu wykonywania zadania, stacja robocza jest uruchamiana ponownie.

Włączanie i wyłączanie Technologii zaawansowanego leczenia dla serwerów plików

W celu włączenia technologii zaawansowanego leczenia dla serwerów plików:

- Włącz technologię zaawansowanego leczenia we właściwościach aktywnego profilu Kaspersky Security Center. W tym celu:
  a. Otwórz sekcję **Ogólne ustawienia ochrony** w oknie właściwości profilu.
  b. Zaznacz pole **Włącz technologię zaawansowanego leczenia**.
  c. Aby zapisać wprowadzone zmiany, w oknie właściwości profilu kliknij **OK**.
- We właściwościach zadania grupowego Skanowanie antywirusowe programu Kaspersky Security Center zaznacz pole **Uruchom natychmiast zaawansowane leczenie**.

W celu wyłączenia technologii zaawansowanego leczenia dla serwerów plików:

- Włącz technologię zaawansowanego leczenia we właściwościach profilu Kaspersky Security Center. W tym celu:
  a. Otwórz sekcję **Ogólne ustawienia ochrony** w oknie właściwości profilu.
  b. Usuń zaznaczenie z pola **Włącz technologię zaawansowanego leczenia**.
  c. Aby zapisać wprowadzone zmiany, w oknie właściwości profilu kliknij **OK**.
- We właściwościach zadania grupowego Skanowanie antywirusowe programu Kaspersky Security Center usuń zaznaczenie z pola **Uruchom natychmiast zaawansowane leczenie**.

Włączanie i wyłączanie trybu oszczędzania energii

W celu włączenia lub wyłączenia trybu oszczędzania energii:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna wybierz sekcję **Ustawienia zaawansowane**.

   W prawej części okna wyświetlone są zaawansowane ustawienia aplikacji.

3. W sekcji **Tryb działania** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Tryb działania**.

4. W oknie **Tryb działania** wykonaj następujące czynności:

   - Aby włączyć tryb oszczędzania energii, zaznacz opcję **Odrocz zaplanowane zadania podczas pracy na bateriach**.

     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 Pełnego skanowania
     - Zadanie Skanowania obszarów krytycznych
     - Zadanie Skanowania obiektów
     - Zadanie Wykrywania luk
     - Zadanie Sprawdzanie integralności

   - Jeśli chcesz wyłączyć tryb oszczędzania energii, usuń zaznaczenie z opcji **Odrocz zaplanowane zadania podczas pracy na bateriach**. W tym przypadku Kaspersky Endpoint Security wykonuje zaplanowane zadania, bez względu na źródło zasilania komputera.

5. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Włączanie i wyłączanie udostępniania zasobów innym aplikacjom

W celu włączenia lub wyłączenia udostępniania zasobów innym aplikacjom:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna wybierz sekcję **Ustawienia zaawansowane**.

   W prawej części okna wyświetlone są zaawansowane ustawienia aplikacji.

3. W sekcji **Tryb działania** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Tryb działania**.

4. W oknie **Tryb działania** wykonaj następujące czynności:

   - Jeśli chcesz włączyć tryb udostępniania zasobów innym aplikacjom, zaznacz pole **Współdziel zasoby z innymi aplikacjami**.

     Jeśli skonfigurowano udostępnianie zasobów innym aplikacjom, Kaspersky Endpoint Security odracza zaplanowane zadania, które mogą spowolnić inne aplikacje:

     - Zadanie aktualizacji

- Zadanie Pełnego skanowania
- Zadanie Skanowania obszarów krytycznych
- Zadanie Skanowania obiektów
- Zadanie Wykrywania luk
- Zadanie Sprawdzanie integralności

- Jeśli chcesz wyłączyć tryb udostępniania zasobów innym aplikacjom, usuń zaznaczenie z pola **Współdziel zasoby z innymi aplikacjami**. W tym przypadku Kaspersky Endpoint Security wykonuje zaplanowane zadania, bez względu na działanie innych aplikacji.

Domyślnie aplikacja udostępnia zasoby innym aplikacjom.

5. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Ochrona hasłem

Sekcja ta zawiera informacje o ograniczaniu hasłem dostępu do Kaspersky Endpoint Security.

Informacje o ograniczaniu dostępu do Kaspersky Endpoint Security

Zdarza się, że z jednego komputera korzysta wielu użytkowników o rożnej umiejętności jego obsługi. Jeżeli użytkownicy nie mają ograniczonego dostępu do Kaspersky Endpoint Security i jego ustawień, może to zmniejszyć ogólny poziom ochrony komputera.

Istnieje możliwość ograniczenia dostępu do Kaspersky Endpoint Security poprzez ustawienie nazwy użytkownika i hasła oraz określenie działań, dla których aplikacja zapyta użytkownika o dane uwierzytelniające:

Podczas uaktualniania z poprzedniej wersji aplikacji do Kaspersky Endpoint Security 10 Service Pack 2 for Windows hasło zostaje zachowane (jeśli zostało ustawione). Jeśli modyfikujesz ustawienia ochrony hasłem po raz pierwszy, użyj domyślnej nazwy użytkownika KLAdmin.

Włączanie i wyłączanie ochrony hasłem

Zalecamy zachowanie ostrożności podczas używania hasła do ograniczania dostępu do aplikacji. Jeżeli zapomnisz hasło, skontaktuj się z działem pomocy technicznej Kaspersky w celu otrzymania instrukcji dotyczących wyłączenia ochrony hasłem.

W celu włączenia ochrony hasłem:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna wybierz sekcję **Ustawienia zaawansowane**.

   W prawej części okna wyświetlone są ustawienia aplikacji.

3. W sekcji **Ochrona hasłem** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona hasłem**.

4. Zaznacz opcję **Włącz ochronę hasłem**.

5. W polu **Nazwa użytkownika** wprowadź nazwę użytkownika, która musi być określona w oknie **Sprawdzenie hasła** podczas wykonywania działań zabezpieczonych hasłem.

6. W polu **Nowe hasło** wpisz hasło dostępu do aplikacji.

7. W polu **Potwierdź hasło** wpisz ponownie hasło.

8. Jeśli chcesz ograniczyć dostęp do wszystkich działań związanych z aplikacją, w sekcji **Zakres działania hasła** kliknij przycisk **Wybierz wszystkie**.

9. Jeśli chcesz selektywnie ograniczyć dostęp użytkownika, w sekcji **Zakres działania hasła** zaznacz pola obok nazw odpowiednich działań:

   - **Konfiguracja ustawień aplikacji**.
   - **Zakończenie działania aplikacji**.
   - **Wyłączenie składników ochrony**.
   - **Wyłączenie składników kontroli**.
   - **Usuwanie klucza**.
   - **Dezinstalacja / modyfikacja / przywracanie aplikacji**.
   - **Przywracanie dostępu do danych na zaszyfrowanych dyskach**.
   - **Wyświetl raporty**.

10. Kliknij przycisk **OK**.

    Aplikacja sprawdzi wprowadzone hasła. Jeśli hasła się zgadzają, aplikacja zastosuje hasło. Jeśli hasła nie są takie same, aplikacja wyświetli pytanie o ponowne potwierdzenie hasła w polu **Potwierdź hasło**.

Po włączeniu ochrony hasłem, aplikacja wyświetli pytanie o podanie hasła za każdym razem, gdy wykonywane będzie działanie uwzględnione w obszarze obowiązywania hasła. Jeżeli nie chcesz, aby podczas bieżącej sesji aplikacja wyświetliła pytanie o podanie hasła przy każdej próbie wykonania operacji chronionej hasłem, zaznacz opcję **Zapisz hasło dla bieżącej sesji**, dostępną w oknie **Sprawdzenie hasła**.

Jeżeli pole **Zapisz hasło dla bieżącej sesji** nie jest zaznaczone, aplikacja pyta użytkownika o hasło za każdym razem, gdy próbuje on wykonać operację chronioną hasłem.

W celu wyłączenia ochrony hasłem:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna wybierz sekcję **Ustawienia zaawansowane**.

W prawej części okna wyświetlone są ustawienia aplikacji.

3. W sekcji **Ochrona hasłem** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona hasłem**.

4. Usuń zaznaczenie z opcji **Włącz ochronę hasłem**.

   Możesz wyłączyć Ochronę hasłem tylko wtedy, gdy jesteś zalogowany jako KLAdmin. Nie można wyłączyć ochrony hasłem, jeśli używasz innego konta użytkownika lub hasła tymczasowego.

5. Kliknij przycisk **OK**.

Po wyłączeniu ochrony hasłem, ograniczony dostęp do aplikacji zostanie anulowany przy kolejnym uruchomieniu Kaspersky Endpoint Security.

Modyfikowanie hasła dostępu do Kaspersky Endpoint Security

W celu zmiany hasła dostępu do Kaspersky Endpoint Security:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna wybierz sekcję **Ustawienia zaawansowane**.

3. W sekcji **Ochrona hasłem** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona hasłem**.

4. W polu **Nazwa użytkownika** wprowadź nazwę użytkownika.

5. W polu **Nowe hasło** wpisz nowe hasło dostępu do aplikacji.

6. W polu **Potwierdź hasło** wprowadź ponownie nowe hasło.

7. Kliknij **OK**.

   Aplikacja sprawdzi wprowadzone hasła. Jeśli hasła są takie same, aplikacja zastosuje nowe hasło i zamknie okno **Ochrona hasłem**. Jeśli hasła nie są takie same, aplikacja wyświetli pytanie o ponowne potwierdzenie hasła w polu **Potwierdź hasło**.

8. Aby zapisać wprowadzone zmiany, w oknie ustawień aplikacji należy kliknąć przycisk **Zapisz**.

Informacje dotyczące korzystania z hasła tymczasowego

Podczas pracy na komputerach klienckich zarządzanych przez profil Kaspersky Security Center użytkownicy mogą potrzebować dostępu do opcji w Kaspersky Endpoint Security, które są chronione przy użyciu hasła na poziomie profilu. Jeśli ochrona hasłem jest włączona, tylko administrator Kaspersky Security Center może wykonywać działania określone w zakresie działania hasła. Jednakże, jeśli połączenie z Kaspersky Security Center zostało zerwane (na przykład wtedy, gdy urządzenie użytkownika znajduje poza siecią firmową), funkcje niezbędne do pracy z lokalnym interfejsem Kaspersky Security Center zostają ograniczone.

Aby użytkownik mógł wykonywać niezbędne działania bez użycia hasła, które jest ustawione w ustawieniach profilu, administrator Kaspersky Security Center może utworzyć hasło tymczasowe. Hasło tymczasowe posiada ograniczony czas ważności oraz ograniczony zakres działania. Po wprowadzeniu przez użytkownika hasła tymczasowego w lokalnym interfejsie aplikacji, działania dozwolone przez administratora Kaspersky Security Center stają się dostępne.

Jeśli hasło tymczasowe wygaśnie, program Kaspersky Endpoint Security będzie działał zgodnie z ustawieniami skonfigurowanymi w profilu Kaspersky Security Center. Działania chronione hasłem na poziomie profilu staną się niedostępne dla użytkownika.

Tworzenie hasła tymczasowego przy użyciu Konsoli administracyjnej Kaspersky Security Center

W celu utworzenia hasła tymczasowego i wysłania go do użytkownika:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej, w folderze **Zarządzane urządzenia** otwórz folder z nazwą grupy administracyjnej zawierającej komputer użytkownika, który prosi o hasło tymczasowe.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Z menu kontekstowego komputera należącego do użytkownika, który prosi o hasło tymczasowe, wybierz **Właściwości**.

   Zostanie otwarte okno **Właściwości: <Nazwa komputera>**.
5. W oknie **Właściwości: <Nazwa komputera>** wybierz sekcję **Aplikacje**.
6. Wybierz Kaspersky Endpoint Security Service Pack 2 for Windows i otwórz okno właściwości aplikacji, korzystając z jednej z następujących metod:

   - W dolnej części ekranu kliknij przycisk **Właściwości**.
   - Z menu kontekstowego aplikacji wybierz **Właściwości**.

   Zostanie otwarte okno **Ustawienia aplikacji "<Nazwa aplikacji>"**.
7. W oknie **Ustawienia aplikacji "<Nazwa aplikacji>"**, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Ustawienia aplikacji**.
8. W sekcji **Ochrona hasłem** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Ochrona hasłem**.
9. W oknie **Ochrona hasłem**, w sekcji **Hasło tymczasowe** kliknij przycisk **Ustawienia**.

   Ten przycisk jest dostępny, jeśli ochrona hasłem jest włączona dla Kaspersky Security Center w profilu Kaspersky Security Center działającym na komputerze.

   Zostanie otwarte okno **Stwórz hasło tymczasowe**.
10. W polu **Data wygaśnięcia** określ dzień, w który użytkownik nie będzie mógł już używać hasła tymczasowego.

W tym dniu hasło tymczasowe przestanie być ważne. Nowe hasło tymczasowe musi zostać utworzone w celu zapewnienia dostępu do działań wykonywanych w lokalnym interfejsie Kaspersky Endpoint Security.

11. W tabeli **Zakres działania hasła tymczasowego** zaznacz pola obok działań, które muszą być dostępne dla użytkownika, gdy hasło tymczasowe jest ważne.

12. Kliknij przycisk **Utwórz**.

    Zostanie otwarte okno **Hasło tymczasowe** zawierające zaszyfrowane hasło.

13. Skopiuj to hasło oraz instrukcje dotyczące jego stosowania, a następnie wyślij je do użytkownika.

Stosowanie hasła tymczasowego w interfejsie Kaspersky Endpoint Security

Instrukcje te są przeznaczone dla użytkowników komputerów klienckich z zainstalowanym Kaspersky Endpoint Security.

W celu użycia hasła tymczasowego:

1. Otwórz okno ustawień aplikacji.

2. W lewej części okna wybierz sekcję **Ustawienia zaawansowane**.

   W prawej części okna wyświetlone są ustawienia aplikacji.

3. W sekcji **Ochrona hasłem** kliknij przycisk **Hasło tymczasowe**.

   Zostanie otwarte okno **Hasło tymczasowe**.

4. Zaznacz opcję **Włącz hasło tymczasowe**.

5. W polu wejściowym określ hasło, które otrzymałeś od administratora Kaspersky Security Center.

6. W celu zapisania zmian kliknij **OK**.

Po wprowadzeniu hasła tymczasowego, działania określone przez administratora Kaspersky Security Center staną się dostępne. W oknie **Hasło tymczasowe** będzie wyświetlona data wygaśnięcia hasła tymczasowego oraz dozwolone działania.

Zdalne zarządzanie aplikacją poprzez Kaspersky Security Center

Sekcja ta opisuje zarządzanie Kaspersky Endpoint Security poprzez Kaspersky Security Center.

Informacje o zarządzaniu aplikacją poprzez Kaspersky Security Center

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

Więcej informacji na temat zarządzania aplikacją poprzez Kaspersky Security Center można znaleźć w *Podręczniku administratora Kaspersky Security Center*.

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

Wersja wtyczki zarządzającej może różnić się od wersji Kaspersky Endpoint Security zainstalowanej na komputerze klienckim. Jeśli zainstalowana wersja wtyczki zarządzającej posiada mnie 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.

Kwestie specjalne dotyczące pracy z różnymi wersjami wtyczek zarządzających

Możesz użyć wtyczki zarządzającej do zmiany następujących elementów:

- Profili
- Profili zasad
- Zadań grupowych
- Zadań lokalnych
- Lokalnych ustawień Kaspersky Endpoint Security

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 komponent, 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 komponentu. Zalecane jest zaktualizowanie wtyczki zarządzającej.

Zmienianie wcześniej zdefiniowanych ustawień przy użyciu nowszej wersji wtyczki zarządzającej

Możesz użyć nowszej wersji wtyczki zarządzającej do zmiany wszystkich wcześniej zdefiniowanych ustawień oraz do konfiguracji nowych ustawień, których nie było w poprzednio używanej wersji wtyczki.

W przypadku nowych ustawień nowsza wersja wtyczki zarządzającej stosuje domyślne wartości, gdy profil, profil zasad lub zadanie jest zapisywane po raz pierwszy.

Po zmianie ustawień profilu, profilu zasad lub zadania grupowego przy użyciu nowszej wersji wtyczki zarządzającej, te komponenty staną się niedostępne dla poprzedniej wersji wtyczki. Lokalne ustawienia Kaspersky Endpoint Security oraz ustawienia zadań lokalnych będą wciąż dostępne dla poprzednich wersji wtyczki zarządzającej.

Uruchamianie i zatrzymywanie działania Kaspersky Endpoint Security na komputerze klienckim

W celu uruchomienia i zatrzymania działania aplikacji na komputerze klienckim:

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. 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**.

   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. Wybierz Kaspersky Endpoint Security 10 for Windows.
8. Wykonaj następujące czynności:

   - W celu uruchomienia aplikacji, kliknij przycisk na prawo od listy aplikacji Kaspersky lub wykonaj następujące działania:

     a. Wybierz **Właściwości** w menu kontekstowym Kaspersky Endpoint Security lub kliknij przycisk **Właściwości** znajdujący się pod listą aplikacji firmy Kaspersky.

     Zostanie otwarte okno **Ustawienia aplikacji Kaspersky Endpoint Security 10 for Windows**.

     b. W sekcji **Ogólne**, w prawej części okna kliknij przycisk **Uruchom**.

   - W celu zatrzymania aplikacji, kliknij przycisk na prawo od listy aplikacji Kaspersky lub wykonaj następujące działania:

     a. Wybierz **Właściwości** w menu kontekstowym Kaspersky Endpoint Security lub kliknij przycisk **Właściwości** znajdujący się pod listą aplikacji firmy Kaspersky.

     Zostanie otwarte okno **Ustawienia aplikacji Kaspersky Endpoint Security 10 for Windows**.

b. W sekcji **Ogólne**, w prawej części okna kliknij przycisk **Zatrzymaj**.

Konfigurowanie ustawień Kaspersky Endpoint Securit

W celu skonfigurowania ustawień Kaspersky Endpoint Security:

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. 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. Wybierz aplikację Kaspersky Endpoint Security 10 for Windows.
8. Wykonaj jedną z poniższych czynności:

   - Wybierz **Właściwości** z menu kontekstowego Kaspersky Endpoint Security 10 for Windows.
   - Kliknij przycisk **Właściwości** pod listą aplikacji firmy Kaspersky.

   Zostanie otwarte okno **Ustawienia aplikacji Kaspersky Endpoint Security 10 for Windows**.
9. W sekcji **Ustawienia zaawansowane** skonfiguruj ustawienia dla Kaspersky Endpoint Security, a także ustawienia raportów i plików danych.

   Pozostałe sekcje okna **Ustawienia aplikacji Kaspersky Endpoint Security 10 for Windows** są takie same jak standardowe sekcje aplikacji Kaspersky Security Center. Opis tych sekcji można znaleźć w *Podręczniku administratora 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 zaawansowane**.
10. W celu zapisania zmian, wprowadzonych w oknie **Ustawienia aplikacji Kaspersky Endpoint Security 10 for Windows**, kliknij **OK**.

Zarządzanie zadaniami

Ta sekcja opisuje sposób zarządzania zadaniami dla Kaspersky Endpoint Security. Szczegółowe informacje dotyczące koncepcji zarządzania zadaniami poprzez Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

Informacje o zadaniach dla Kaspersky Endpoint Security

Kaspersky Security Center kontroluje aktywność aplikacji Kaspersky na komputerach klienckich za pomocą zadań. Zadania wykonują główne funkcje administracyjne, takie jak instalacja klucza, skanowanie komputera, a także aktualizacja baz danych i modułów aplikacji.

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 zbioru komputerów, które nie należą do grup administracyjnych.

  Zadania dla zbioru komputerów spoza grup administracyjnych odnoszą się tylko do komputerów klienckich określonych w ustawieniach zadania. Jeżeli nowe komputery klienckie zostaną dodane do zbioru komputerów, dla którego konfigurowane jest zadanie, zadanie to nie będzie stosowane dla tych nowych komputerów. Aby zadanie było stosowane dla tych komputerów, utwórz nowe zadanie lub zmodyfikuj ustawienia istniejącego zadania.

W celu zdalnego zarządzania Kaspersky Endpoint Security możesz użyć następujących zadań:

- **Dodaj klucz**. Kaspersky Endpoint Security dodaje klucz do aktywacji aplikacji, w tym klucz zapasowy.
- **Zmiana składników aplikacji**. Kaspersky Endpoint Security instaluje lub usuwa komponenty na komputerach klienckich zgodnie z listą komponentów określonych w ustawieniach zadania.
- **Inwentaryzacja**. Kaspersky Endpoint Security zbiera informacje o wszystkich plikach wykonywalnych aplikacji, które są przechowywane na komputerach.

  Możesz włączyć inwentaryzację modułów DLL i plików skryptu. W tym przypadku Kaspersky Security Center pobierze informacje o modułach DLL załadowanych na komputerze z zainstalowanym programem Kaspersky Endpoint Security oraz o plikach zawierających skrypty.

  Włączenie inwentaryzacji modułów DLL i plików skryptu znacząco zwiększa czas dostępu zadania inwentaryzacji oraz rozmiar bazy danych.

- **Aktualizacja**. Kaspersky Endpoint Security aktualizuje bazy danych i moduły zgodnie ze skonfigurowanymi ustawieniami aktualizacji.
- **Wycofywanie**. Kaspersky Endpoint Security wycofuje ostatnią aktualizację baz danych i modułów.
- **Skanowanie antywirusowe**. Kaspersky Endpoint Security skanuje obszary komputera, określone w ustawieniach zadania, w poszukiwaniu wirusów i innych zagrożeń.
- **Sprawdzanie połączenia z KSN**. Kaspersky Endpoint Security wysyła zapytanie o dostępność serwerów KSN i aktualizuje stan połączenia z KSN.

- **Sprawdzanie integralności**. Kaspersky Endpoint Security pobiera dane o zestawie modułów aplikacji zainstalowanych na komputerze klienckim i skanuje podpis cyfrowy każdego modułu.
- **Zarządzanie kontami Agenta autoryzacji**. Kaspersky Endpoint Security generuje polecenia dezinstalacji, dodawania lub modyfikacji kont Agenta autoryzacji.

Na zadaniach możesz wykonać następujące akcje:

- Uruchomić, zatrzymać, wstrzymać i wznowić zadania.
- Utwórz nowe zadania.
- Zmodyfikować ustawienia zadania.

Uprawnienia dostępu do ustawień 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.

Konfigurowanie trybu zarządzania zadaniem

W celu skonfigurowania trybu pracy z zadaniami w lokalnym interfejsie Kaspersky Endpoint Security:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, dla której chcesz skonfigurować tryb pracy z zadaniami w lokalnym interfejsie Kaspersky Endpoint Security.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz interesujący Cię profil.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W sekcji **Ustawienia zaawansowane** wybierz podsekcję **Ustawienia aplikacji**.
7. W sekcji **Tryb działania**:
   - Jeśli chcesz zezwolić użytkownikom na pracę z zadaniami lokalnymi w interfejsie i wierszu poleceń, zaznacz opcję **Zezwól na korzystanie z zadań lokalnych**.

     Jeśli pole jest odznaczone, funkcje zadań lokalnych zostają zatrzymane. W tym trybie zadania lokalne nie są uruchamiane zgodnie z terminarzem. Niedostępne jest również uruchamianie i modyfikowanie zadań lokalnych w lokalnym interfejsie Kaspersky Endpoint Security i podczas pracy z wierszem poleceń.

   - Jeśli chcesz zezwolić użytkownikom na przeglądanie listy zadań grupowych, zaznacz opcję **Zezwól na wyświetlanie zadań grupowych**.

- Jeśli chcesz zezwolić użytkownikom na modyfikowanie ustawień zadań grupowych, zaznacz opcję **Zezwól na zarządzanie zadaniami grupowymi**.

8. W celu zapisania zmian kliknij **OK**.

9. Zastosuj profil.

   Szczegółowe informacje dotyczące stosowania profili Kaspersky Security Center znajdują się w *Podręczniku administratora dla Kaspersky Security Center*.

Tworzenie zadania lokalnego

W celu utworzenia zadania lokalnego:

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. Wybierz komputer, dla którego chcesz utworzyć zadanie lokalne.

5. Wykonaj jedną z poniższych czynności:

   - Z menu kontekstowego komputera klienckiego wybierz opcję **Wszystkie zadania** Utwórz zadanie.

   - Z menu kontekstowego komputera klienckiego wybierz **Właściwości** i w otwartym oknie **Właściwości: <Nazwa komputera>**, na zakładce **Zadania** kliknij przycisk **Dodaj**.

   - Z listy rozwijalnej **Wybierz akcję** wybierz **Utwórz zadanie**.

   Zostanie uruchomiony Kreator tworzenia zadania.

6. Postępuj zgodnie z instrukcjami Kreatora tworzenia zadania.

Tworzenie zadania grupowego

W celu utworzenia zadania grupowego:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. Wykonaj jedną z poniższych czynności:

   - W drzewie Konsoli administracyjnej wybierz folder **Zarządzane urządzenia**, aby utworzyć zadanie grupowe dla wszystkich komputerów zarządzanych przez Kaspersky Security Center.

   - W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.

3. Wybierz zakładkę **Zadania** w obszarze roboczym.

4. Kliknij przycisk **Utwórz zadanie**.

   Zostanie uruchomiony Kreator tworzenia zadania.

5. Postępuj zgodnie z instrukcjami Kreatora tworzenia zadania.

Tworzenie zadania dla wyboru urządzeń

W celu utworzenia zadania dla wyboru urządzenia:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz **Zadania**.
3. Kliknij przycisk **Utwórz zadanie**.

   Zostanie uruchomiony Kreator tworzenia zadania.

4. Postępuj zgodnie z instrukcjami Kreatora tworzenia zadania.
5. W oknie **Wybierz urządzenia, do których zostanie przypisane zadanie** kliknij przycisk **Przypisz zadanie do wyboru urządzeń**.
6. W następnym oknie kliknij przycisk **Wybierz**.

   Zostanie otwarte okno **Wybór urządzeń**.

7. Wybierz żądane urządzenia.
8. Kliknij przycisk **OK** w oknie **Wybór urządzeń**.
9. Postępuj zgodnie z instrukcjami Kreatora tworzenia zadania.

Uruchamianie, zatrzymywanie, wstrzymywanie i wznawianie zadania

Jeśli aplikacja Kaspersky Endpoint Security jest uruchomiona na komputerze klienckim, możesz uruchomić, zatrzymać, wstrzymać i wznowić zadania na tym komputerze poprzez Kaspersky Security Center. Jeśli działanie Kaspersky Endpoint Security jest wstrzymane nie można uruchomić, wyłączyć, wstrzymać lub wznowić zadania z poziomu Kaspersky Security Center.

W celu uruchomienia, wyłączenia, wstrzymania i wznowienia zadania lokalnego:

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. Wybierz komputer, na którym chcesz uruchomić, zatrzymać, wstrzymać lub wznowić zadanie lokalne.

5. Kliknij prawym przyciskiem myszy komputer kliencki, aby wyświetlić jego menu kontekstowe, z którego wybierz **Właściwości**.

   Zostanie otwarte okno właściwości komputera klienckiego.

6. Wybierz sekcję **Zadania**.

   W prawej części okna pojawi się lista zadań lokalnych.

7. Wybierz zadanie lokalne, które chcesz uruchomić, zatrzymać, wstrzymać lub wznowić.

8. Wykonaj wymagane działanie na zadaniu przy użyciu jednej z następujących metod:

   - Kliknij lokalne zadanie prawym przyciskiem myszy, aby otworzyć jego menu kontekstowe, z którego wybierz **Uruchom** / **Zatrzymaj** / **Wstrzymaj** / **Wznów**.
   - Aby uruchomić lub zatrzymać zadanie lokalne, kliknij przycisk / znajdujący się po prawej stronie listy zadań lokalnych.
   - Wykonaj następujące czynności:

     a. Kliknij przycisk **Właściwości** pod listą zadań lokalnych bądź wybierz **Właściwości** z menu kontekstowego zadania.

        Zostanie otwarte okno **Właściwości: <nazwa zadania>**.

     b. Na zakładce **Ogólne** kliknij przycisk **Uruchom** / **Zatrzymaj** / **Wstrzymaj** / **Wznów**.

W celu uruchomienia, zatrzymania, wstrzymania lub wznowienia zadania grupowego:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder z nazwą odpowiedniej grupy administracyjnej, dla której chcesz uruchomić, zatrzymać, wstrzymać lub wznowić zadanie grupowe.

3. Wybierz zakładkę **Zadania** w obszarze roboczym.

   W prawej części okna zostaną wyświetlone zadania grupowe.

4. Wybierz zadanie grupowe, które chcesz uruchomić, zatrzymać, wstrzymać lub wznowić.

5. Wykonaj wymagane działanie na zadaniu przy użyciu jednej z następujących metod:

   - Z menu kontekstowego zadania grupowego wybierz **Uruchom** / **Zatrzymaj** / **Wstrzymaj** / **Wznów**.
   - Kliknij przycisk / po prawej stronie okna, aby uruchomić lub zatrzymać zadanie grupowe.
   - Wykonaj następujące czynności:

     a. Kliknij odnośnik **Ustawienia zadania** w prawej części obszaru roboczego Konsoli administracyjnej lub wybierz **Właściwości** z menu kontekstowego zadania.

        Zostanie otwarte okno **Właściwości: <nazwa zadania>**.

     b. Na zakładce **Ogólne** kliknij przycisk **Uruchom** / **Zatrzymaj** / **Wstrzymaj** / **Wznów**.

W celu uruchomienia, wyłączenia, wstrzymania lub wznowienia zadania dla wybranych komputerów:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W folderze **Zadania** drzewa Konsoli administracyjnej wybierz zadanie dla wybranych komputerów, które chcesz uruchomić, zatrzymać, wstrzymać lub wznowić.

3. Wykonaj jedną z poniższych czynności:

   - Z menu kontekstowego zadania wybierz **Uruchom** / **Zatrzymaj** / **Wstrzymaj** / **Wznów**.
   - W prawej części okna kliknij przycisk / , aby uruchomić lub zatrzymać zadanie dla określonych komputerów.
   - Wykonaj następujące czynności:

     a. Kliknij odnośnik **Ustawienia zadania** w prawej części obszaru roboczego Konsoli administracyjnej lub wybierz **Właściwości** z menu kontekstowego zadania.

     Zostanie otwarte okno **Właściwości: <nazwa zadania>**.

     b. Na zakładce **Ogólne** kliknij przycisk **Uruchom** / **Zatrzymaj** / **Wstrzymaj** / **Wznów**.

Modyfikowanie ustawień zadania

W celu zmodyfikowania ustawień zadania lokalnego:

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. Wybierz komputer, dla którego chcesz skonfigurować ustawienia aplikacji.
5. Kliknij prawym przyciskiem myszy komputer kliencki, aby wyświetlić jego menu kontekstowe, z którego wybierz **Właściwości**.

   Zostanie otwarte okno właściwości komputera klienckiego.
6. Wybierz sekcję **Zadania**.

   W prawej części okna pojawi się lista zadań lokalnych.
7. Z listy zadań lokalnych wybierz żądane zadanie lokalne.
8. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:

   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
9. W oknie **Właściwości:<Nazwa zadania lokalnego>** wybierz sekcję **Ustawienia**.
10. Zmodyfikuj ustawienia lokalnego zadania.
11. Aby zapisać zmiany, w oknie **Właściwości: <Nazwa zadania lokalnego>** kliknij **OK**.
12. Aby zapisać zmiany, w oknie **Właściwości: <Nazwa komputera>** kliknij **OK**.

W celu zmodyfikowania ustawień zadania grupowego:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** otwórz folder z nazwą odpowiedniej grupy administracyjnej.
3. Wybierz zakładkę **Zadania** w obszarze roboczym.
   Zadania grupowe są wyświetlane w obszarze roboczym Konsoli administracyjnej.
4. Wybierz żądane zadanie grupowe.
5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
6. W oknie **Właściwości: <Nazwa zadania grupowego>** wybierz sekcję **Ustawienia**.
7. Zmodyfikuj ustawienia zadania grupowego.
8. Aby zapisać zmiany, w oknie **Właściwości: <Nazwa zadania grupowego>** kliknij **OK**.

W celu zmodyfikowania ustawień zadania dla wyboru komputerów:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zadania** drzewa Konsoli administracyjnej wybierz zadanie dla wyboru komputerów, którego ustawienia chcesz zmodyfikować.
3. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:
   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.
4. W oknie **Właściwości: <Nazwa zadania dla wyboru komputerów>** wybierz sekcję **Ustawienia**.
5. Zmodyfikuj ustawienia dla wyboru komputerów.
6. Aby zapisać zmiany, w oknie **Właściwości: <Nazwa zadania dla wyboru komputerów>** kliknij **OK**.

Z wyjątkiem sekcji **Ustawień**, wszystkie sekcje w oknie właściwości zadania są identyczne jak te w Kaspersky Security Center. Bardziej szczegółowe informacje można znaleźć w *Podręczniku administratora Kaspersky Security Center*. Sekcja **Ustawienia** zawiera określone ustawienia Kaspersky Endpoint Security 10 for Windows. Jej zawartość zależy od wybranego zadania lub typu zadania.

Zarządzanie profilami

Ta sekcja opisuje tworzenie i konfigurowanie profili dla Kaspersky Endpoint Security. Więcej informacji na temat zarządzania Kaspersky Endpoint Security przy użyciu profili Kaspersky Security Center można znaleźć w *Podręczniku administratora Kaspersky Security Center*.

Informacje o profilach

Istnieje możliwość wykorzystania profili do wprowadzenia identycznych ustawień programu Kaspersky Endpoint Security na wszystkich komputerach klienckich należących do grupy administracyjnej.

Możesz lokalnie zmienić wartości ustawień, określone przez profil dla pojedynczych komputerów w grupie administracyjnej, przy użyciu Kaspersky Endpoint Security. Możesz lokalnie zmienić tylko te ustawienia, których modyfikacja nie jest zablokowana przez profil.

Możliwość zmodyfikowania ustawień aplikacji na komputerze klienckim jest determinowana przez stan "blokady" ustawienia w profilu:

- Jeśli ustawienie jest "zablokowane" (), nie możesz lokalnie zmodyfikować wartości tego ustawienia. Wartość ustawienia określona przez profil jest używana dla wszystkich komputerów klienckich w obrębie grupy administracyjnej.

- W przypadku, gdy ustawienie jest "odblokowane" (), można je lokalnie modyfikować. Lokalnie skonfigurowane ustawienie jest stosowane do wszystkich komputerów klienckich w obrębie grupy administracyjnej. Ustawienie narzucone przez profil nie jest stosowane.

Po pierwszym zastosowaniu profilu, ustawienia lokalne zostają zmienione na zgodne z profilem.

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 profilu, przejdź do sekcji **Bezpieczeństwo** okna właściwości Serwera administracyjnego Kaspersky Security Center.

Rozróżnić można następujące obszary funkcyjne Kaspersky Endpoint Security:

- Ochrona antywirusowa. Ten obszar funkcyjny zawiera Ochronę plików, Ochronę poczty, Ochronę WWW, Ochronę komunikatorów, Wykrywanie luk oraz zadania skanowania.

- Kontrola uruchamiania aplikacji. Ten obszar funkcyjny zawiera komponent Kontrola uruchamiania aplikacji.

- Kontrola urządzeń. Ten obszar funkcyjny zawiera moduł Kontrola urządzeń.

- Szyfrowanie. Ten obszar funkcyjny zawiera moduły szyfrujące foldery, pliki i dyski twarde.

- Strefa zaufana. Obszar funkcyjny zawiera Strefę zaufaną.

- Kontrola sieci. Ten obszar funkcyjny zawiera moduł Kontrola sieci.

- Ochrona przed wniknięciem. Ten obszar funkcyjny zawiera Monitor aktywności aplikacji, Monitor wykrywania luk, Zaporę sieciową, Blokowanie ataków sieciowych oraz Kontrolę uprawnień aplikacji.

- Podstawowa funkcjonalność. Ten obszar funkcyjny zawiera ogólne ustawienia aplikacji, które nie zostały określone dla innych obszarów funkcyjnych, czyli: licencjonowanie, ustawienia KSN, zadania inwentaryzacji, zadania aktualizacji modułów i baz danych aplikacji, Autoochrona, zaawansowane ustawienia aplikacji, raporty i magazyny, ustawienia ochrony hasłem, a także ustawienia interfejsu aplikacji.

Na profilu można wykonać następujące akcje:

- Utworzyć profil.

- Zmodyfikować ustawienia profilu.

  Jeśli konto użytkownika, z poziomu którego uzyskujesz dostęp do Serwera administracyjnego, nie posiada uprawnień modyfikacji ustawień pewnych obszarów funkcyjnych, wówczas nie jest możliwe modyfikowanie ustawień tych obszarów funkcyjnych.

- Usunąć profil.
- Zmienić stan profilu.

Informacje na temat korzystania z profili, które nie są związane z interakcją z Kaspersky Endpoint Security, można znaleźć w *Podręczniku administratora Kaspersky Security Center*.

Tworzenie profilu

W celu utworzenia profilu:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. Wykonaj jedną z poniższych czynności:
   - W drzewie Konsoli administracyjnej wybierz folder **Zarządzane urządzenia**, aby utworzyć profil dla wszystkich komputerów zarządzanych przez Kaspersky Security Center.
   - 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. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Utwórz profil**.
   - Kliknij profil prawym przyciskiem myszy, aby otworzyć jego menu kontekstowe, z którego wybierz **Utwórz** Profil.

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

Modyfikowanie ustawień profilu

W celu zmodyfikowania ustawień profilu:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** drzewa Konsoli administracyjnej otwórz folder odpowiedniej grupy administracyjnej, dla której chcesz zmodyfikować ustawienia profilu.
3. W obszarze roboczym wybierz zakładkę **Profile**.

4. Wybierz interesujący Cię profil.

5. Otwórz okno **Właściwości: <Nazwa profilu>** za pomocą jednej z następujących metod:

   - Z otwartego menu kontekstowego profilu wybierz **Właściwości**.
   - Kliknij odnośnik **Konfiguruj profil** znajdujący się w prawej części obszaru roboczego Konsoli administracyjnej.

   Ustawienia profilu Kaspersky Endpoint Security 10 for Windows zawierają ustawienia komponentu i ustawienia aplikacji. Sekcje **Ochrona antywirusowa** i **Kontrola węzła końcowego** okna **Właściwości: <Nazwa profilu>** wyświetlają ustawienia komponentów ochrony i kontroli, sekcja **Szyfrowanie danych** wyświetla ustawienia szyfrowania plików i folderów, a sekcja **Ustawienia zaawansowane** wyświetla ustawienia aplikacji.

   Aby włączyć wyświetlanie ustawień szyfrowania danych i ustawień składnika kontroli w ustawieniach profilu, zaznacz odpowiednie pola w oknie **Ustawienia interfejsu** programu Kaspersky Security Center.

6. Zmodyfikuj ustawienia profilu.

7. Aby zapisać zmiany, w oknie **Właściwości: <Nazwa profilu>** kliknij **OK**.

Wybieranie ustawień wyświetlanych w profilu Kaspersky Security Center

W celu wybrania ustawień wyświetlanych w profilu Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. Z menu kontekstowego węzła **Serwer administracyjny – <Nazwa komputera>** wybierz Widok → **Ustawienia interfejsu**.

   Zostanie otwarte okno **Ustawienia interfejsu**.

3. W oknie **Ustawienia interfejsu** zaznacz pola obok ustawień, które mają być wyświetlane w ustawieniach tworzenia profilu Kaspersky Security Center oraz we właściwościach profilu:

   - Zaznacz pole **Wyświetlaj składniki kontroli węzła końcowego**, aby włączyć wyświetlanie ustawień składnika kontroli w oknie Kreatora tworzenia nowego profilu programu Kaspersky Security Center oraz we właściwościach profilu.
   - Zaznacz pole **Pokaż ochronę danych i szyfrowania**, aby włączyć wyświetlanie ustawień szyfrowania danych w Kreatorze tworzenia nowego profilu programu Kaspersky Security Center oraz we właściwościach profilu.

4. Kliknij **OK**.

Wysyłanie wiadomości użytkownika na serwer Kaspersky Security Center

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 uruchamiania aplikacji zablokowała uruchomienie aplikacji.

Szablon wiadomości z prośbą o zezwolenie na uruchomienie zablokowanej aplikacji jest dostępny w interfejsie Kaspersky Endpoint Security, w sekcji Kontrola uruchamiania 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 Security Center, komunikat użytkownika zostanie wysłana 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 Security Center, 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: Pola wiadomości są uzupełniane wartościami z szablonu zdefiniowanego w profilu Kaspersky Security Center.

- Jeśli na komputerze z zainstalowanym produktem Kaspersky Endpoint Security działa profil użytkownika mobilnego z Kaspersky Security Center, metoda używana do wysyłania wiadomości zależy od tego, czy jest połączenie z Kaspersky Security Center.

  - Jeśli zostało nawiązane połączenie z Kaspersky Security Center, Kaspersky Endpoint Security wysyła standardowa wiadomość na Serwer administracyjny Kaspersky Security Center.

  - Jeśli nie zostało nawiązane połączenie z Kaspersky Security Center, komunikat użytkownika jest wysyłana do administratora sieci lokalnej za pośrednictwem poczty elektronicznej.

  W obu przypadkach pola wiadomości są uzupełniane wartościami z szablonu zdefiniowanego w profilu Kaspersky Security Center.

Przeglądanie wiadomości użytkowników w miejscu przechowywania zdarzeń programu Kaspersky Security Center

Komponenty Kontrola uruchamiania aplikacji, Kontrola urządzeń i Kontrola sieci umożliwiają użytkownikom sieci LAN, którzy mają zainstalowany program Kaspersky Endpoint Security, wysyłanie wiadomości do administratora.

Użytkownik może wysyłać wiadomości do administratora na dwa sposoby:

- Jako zdarzenie w miejscu przechowywania zdarzeń programu Kaspersky Security Center.

  Żądanie użytkownika jest wysyłane do miejsca przechowywania zdarzeń programu Kaspersky Security Center, jeżeli aplikacja Kaspersky Endpoint Security zainstalowana na komputerze użytkownika działa zgodnie z aktywnym profilem.

- Jako wiadomość e-mail.

Żądanie użytkownika jest wysyłane za pośrednictwem poczty elektronicznej, jeśli aplikacja Kaspersky Endpoint Security, zainstalowana na komputerze użytkownika, nie działa pod kontrolą profilu lub działa pod kontrolą profilu użytkownika mobilnego.

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 **Zgłoszenia użytkownika**.
4. Wybierz wiadomość, która ma zostać wysłana do administratora.
5. Otwórz okno **Ustawienia zdarzeń** w jeden z następujących sposobów:

   - Kliknij zdarzenie prawym klawiszem myszy. Z otwartego menu kontekstowego wybierz **Właściwości**.
   - W prawej części obszaru roboczego Konsoli administracyjnej kliknij **Otwórz okno właściwości zdarzenia**.

Uczestnictwo w Kaspersky Security Network

Sekcja zawiera informacje o uczestnictwie w Kaspersky Security Network oraz instrukcje dotyczące włączania i wyłączania korzystania z Kaspersky Security Network.

Informacje o uczestnictwie w Kaspersky Security Network

Aby lepiej chronić Twój komputer, Kaspersky Endpoint Security wykorzystuje dane zebrane 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.

W zależności od lokalizacji infrastruktury, dostępna jest globalna usługa KSN (infrastruktura znajduje się na serwerach Kaspersky) oraz prywatna usługa KSN (infrastruktura znajduje się na innych serwerach, na przykład w sieci dostawcy usługi internetu).

Po zmianie licencji wyślij szczegóły dotyczące nowego klucza do dostawcy usługi, aby móc korzystać z usługi Prywatna sieć KSN. W przeciwnym razie, wymiana danych z KSN nie będzie możliwa.

Dzięki użytkownikom uczestniczącym w KSN, Kaspersky może szybko gromadzić informacje o typach i źródłach zagrożeń, opracowywać rozwiązania do ich neutralizacji i ograniczać liczbę fałszywych alarmów wyświetlanych przez komponenty aplikacji.

Podczas uczestniczenia w KSN aplikacja automatycznie wysyła do KSN statystyki wygenerowane podczas działania aplikacji. Aplikacja może także wysyłać pewne pliki (lub części plików), których cyberprzestępcy mogą użyć do uszkodzenia komputera lub danych, do Kaspersky w celu przeprowadzenia dodatkowego skanowania.

Żadne dane osobowe użytkowników nie są gromadzone, przetwarzane, ani przechowywane przez Kaspersky Lab. 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 Umowy Kaspersky Security Network znajduje się w pakiecie dystrybucyjnym aplikacji.

Aby zmniejszyć obciążenie na serwerach KSN, Kaspersky może opublikować antywirusowe bazy danych aplikacji, które tymczasowo wyłączą lub częściowo ograniczą żądania do Kaspersky Security Network. W tym przypadku stan połączenia z KSN to *Włączony z ograniczeniami*.

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 przesyłać informacje do KSN, nawet bez bezpośredniego dostępu do internetu.
- KSN Proxy buforuje przetwarzane dane, ograniczając obciążenie zewnętrznego połączenia sieciowego i przyśpieszając odbieranie informacji żądanych przez komputer użytkownika.

Więcej szczegółowych informacji o usłudze KSN Proxy jest dostępnych w *Podręczniku administratora Kaspersky Security Center*.

Ustawienia KSN Proxy można skonfigurować we właściwościach profilu *Kaspersky Security Center*.

Uczestnictwo w Kaspersky Security Network nie jest obowiązkowe. Aplikacja oferuje użytkownikowi możliwość uczestnictwa w KSN podczas wstępnej konfiguracji aplikacji. Użytkownik może rozpocząć lub zakończyć uczestniczenie w KSN w dowolnym momencie.

Włączanie i wyłączanie korzystania z Kaspersky Security Network

W celu włączenia lub wyłączenia korzystania z Kaspersky Security Network:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna, w sekcji **Ustawienia zaawansowane** wybierz podsekcję **Ustawienia KSN**.

   W prawej części okna wyświetlane są ustawienia Kaspersky Security Network.
3. Wykonaj jedną z poniższych czynności:
   - Jeśli chcesz włączyć usługę Kaspersky Security Network, zaznacz pole **Akceptuję Umowę KSN oraz warunki uczestnictwa**.
   - Jeśli chcesz wyłączyć usługę Kaspersky Security Network, odznacz pole **Akceptuję Umowę KSN oraz warunki uczestnictwa**.
4. W celu zapisania zmian należy kliknąć przycisk **Zapisz**.

Sprawdzanie połączenia z Kaspersky Security Network

W celu sprawdzenia połączenia z Kaspersky Security Network:

1. Otwórz okno główne aplikacji.
2. W górnej części okna kliknij przycisk **Kaspersky Security Network**.

   Zostanie otwarte okno **Kaspersky Security Network**.

   W lewej części okna **Kaspersky Security Network**, w postaci okrągłego przycisku **KSN** wyświetlony jest tryb połączenia z Kaspersky Security Network:
   - Jeśli Kaspersky Endpoint Security nie jest połączony z Kaspersky Security Network, przycisk **KSN** jest szary. Pod przyciskiem **KSN** wyświetlany jest stan *Wyłączone*.
   - Jeśli Kaspersky Endpoint Security jest połączony z Kaspersky Security Network i dostępne są serwery KSN, przycisk **KSN** jest zielony. Pod przyciskiem **KSN** pojawią się następujące informacje: stan *Włączone*, typ używanej sieci KSN – **Prywatna sieć KSN** lub **Globalna sieć KSN**, a także data i godzina ostatniej

synchronizacji z serwerami KSN. W prawej części okna będą wyświetlone statystyki dotyczące reputacji plików, zasobów sieciowych i oprogramowania.

Kaspersky Endpoint Security zbiera dane statystyczne dotyczące korzystania z KSN po otwarciu okna **Kaspersky Security Network**. Statystyki nie są aktualizowane w czasie rzeczywistym.

- Jeśli Kaspersky Endpoint Security jest połączony z Kaspersky Security Network, ale serwery KSN są niedostępne, przycisk **KSN** jest czerwony. Pod przyciskiem **KSN** wyświetlany jest stan *Włączone*.

  Jeśli czas ostatniej synchronizacji z serwerami KSN przekroczył 15 minut lub posiada stan *Nieznany*, oznacza to, że serwery KSN są niedostępne. W takiej sytuacji zalecane jest skontaktowanie się z pomocą techniczną lub dostawcą usługi.

  Nawiązanie połączenia z serwerami Kaspersky Security Network może być niemożliwe, gdy:

  - Komputer nie jest połączony z internetem.
  - Aplikacja nie została aktywowana lub licencja wygasła.
  - Wykryto problemy z kluczem (na przykład, klucz został umieszczony na czarnej liście).

Sprawdzanie reputacji pliku w Kaspersky Security Network

Usługa KSN umożliwia pobieranie informacji o aplikacjach, które znajdują się w bazach danych firmy Kaspersky. Umożliwia to elastyczne zarządzanie profilami uruchamiania aplikacji na poziomie firmy i tym samym zapobiega uruchamianiu programów typu adware oraz innych programów, które mogą zostać użyte przez cyberprzestępców do uszkodzenia komputera lub danych.

W celu sprawdzenia reputacji pliku w Kaspersky Security Network:

1. Kliknij prawym klawiszem myszy plik, którego reputację chcesz sprawdzić, aby otworzyć jego menu kontekstowe.
2. Wybierz opcję **Sprawdź reputację w KSN**.

   Ta opcja jest dostępna, jeśli zaakceptowałeś warunki Umowy Kaspersky Security Network.

   Zostanie otwarte okno **<Nazwa pliku> - Reputacja w KSN**. Okno <Nazwa pliku> - **Reputacja w KSN** wyświetla następujące informacje o sprawdzanym pliku:

   - **Ścieżka dostępu**. Ścieżka dostępu do pliku na dysku.
   - **Wersja**. Wersja aplikacji (ta informacja jest wyświetlana tylko dla plików wykonywalnych).
   - **Podpis cyfrowy**. Obecność podpisu cyfrowego.
   - **Podpisano**. Data podpisania certyfikatu podpisem cyfrowym.
   - **Utworzony**. Data utworzenia pliku.

- **Zmodyfikowany**. Data ostatniej modyfikacji pliku.
- **Rozmiar**. Przestrzeń dysku zajmowana przez plik.
- Informacja o liczbie użytkowników, którzy ufają plikowi lub blokują plik.

Udoskonalona ochrona z użyciem Kaspersky Security Network

Kaspersky oferuje użytkownikom dodatkową warstwę zabezpieczenia poprzez Kaspersky Security Network. Ta metoda ochrony została zaprojektowana do walki z zaawansowanymi zagrożeniami i atakami zero-day. Zintegrowana technologia chmury oraz doświadczenie analityków wirusów z Kaspersky sprawiają, że program Kaspersky Endpoint Security to najlepszy wybór, jeśli chodzi o ochronę przed najbardziej wyszukanymi zagrożeniami sieciowymi.

Szczegóły dotyczące udoskonalonej ochrony w Kaspersky Endpoint Security są dostępne na stronie internetowej Kaspersky.

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.

Forum internetowe firmy Kaspersky

Jeżeli zapytanie nie wymaga natychmiastowej odpowiedzi, można przedyskutować je z ekspertami z firmy Kaspersky lub innymi użytkownikami jej oprogramowania na forum internetowym.

Na tym forum możesz przeglądać istniejące tematy, pozostawiać swoje komentarze i tworzyć nowe tematy.

Kontakt z działem pomocy technicznej

W tej sekcji opisano sposoby uzyskania pomocy technicznej oraz warunki, na jakich jest ona udzielana.

Jak uzyskać pomoc techniczną?

Jeśli nie znajdziesz rozwiązania swojego problemu w dokumentacji dla aplikacji lub w jednym z dodatkowych źródeł informacji o aplikacji, zalecamy skontaktować się z działem pomocy technicznej. Eksperci z działu pomocy technicznej odpowiedzą na Twoje pytania związane z instalacją i użytkowaniem aplikacji.

Wsparcie użytkownika jest oferowana tylko tym użytkownikom, którzy zakupili licencję komercyjną. Użytkownicy posiadający licencję testową nie są uprawnieni do otrzymania pomocy technicznej.

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:

- Dzwoniąc do pomocy technicznej
- Wysyłając zgłoszenie do pomocy technicznej poprzez portal Kaspersky CompanyAccount

Wsparcie użytkownika za pośrednictwem telefonu

Możesz skontaktować się z pomocą techniczną firmy Kaspersky Lab za pośrednictwem telefonu. Informacje dotyczące sposobów kontaktu z pomocą techniczną znajdują się na stronie internetowej działu pomocy technicznej Kaspersky.

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

Wsparcie użytkownika poprzez CompanyAccount

Kaspersky CompanyAccount to portal dla firm, które korzystają z aplikacji Kaspersky. Portal Kaspersky CompanyAccount został zaprojektowany w celu ułatwienia interakcji między użytkownikiem a specjalistami z Kaspersky przy użyciu zgłoszeń elektronicznych. Portal Kaspersky CompanyAccount może zostać użyty do śledzenia stanu swoich zgłoszeń elektronicznych oraz do przechowywania historii tych zgłoszeń.

Możesz zarejestrować wszystkich pracowników firmy pod jednym kontem na portalu CompanyAccount. Pojedyncze konto umożliwia scentralizowane zarządzanie zgłoszeniami elektronicznymi od zarejestrowanych pracowników do Kaspersky, a także zarządzanie uprawnieniami tych pracowników poprzez Kaspersky CompanyAccount.

Portal Kaspersky CompanyAccount jest dostępny w następujących językach:

- Angielski
- Hiszpański
- Włoski
- Niemiecki
- Polski
- Portugalski
- Rosyjski
- Francuski
- Japoński

Więcej informacji o portalu Kaspersky CompanyAccount można znaleźć na stronie działu pomocy technicznej.

Zbieranie informacji dla pomocy technicznej

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 pomocy technicznej mogą również potrzebować dodatkowych informacji o systemie operacyjnym, uruchomionych na komputerze procesach, szczegółowego raportu z działania modułów aplikacji i plików zrzutu pamięci z awarii aplikacji.

Możesz zebrać wymagane informacje z pomocą Kaspersky Endpoint Security. Zebrane informacje można zapisać na dysku twardym w celu późniejszego ich przesłania w dogodnym dla użytkownika momencie.

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 i przesyłania zbieranych informacji diagnostycznych.
- Konfigurację przechwytywania i rejestrowania ruchu sieciowego.

Eksperci z pomocy technicznej dostarczą wszystkie informacje potrzebne do wykonania tych działań (opis sekwencji kroków, ustawienia, które mają zostać zmodyfikowane, pliki konfiguracyjne, skrypty, dodatkowe funkcje wiersza polecenia, moduły diagnostyczne, narzędzia do zadań specjalnych itd.) oraz poinformują o zakresie danych zbieranych do celów diagnostycznych. Zebrane rozszerzone informacje diagnostyczne są zapisywane na komputerze użytkownika. Dane, które zostały zebrane, nie są automatycznie przesyłane do Kaspersky.

Ustawienia użyte do określenia adresu serwera zrzutu dla wysłania plików zrzutów do Kaspersky są przechowywane na komputerze użytkownika. Jeśli jest to konieczne, wartości tych ustawień można zmodyfikować w kluczu rejestru systemu operacyjnego `"DumpServerConfigUrl"="https://dmpcfg.kaspersky-labs.com/dumpserver/config.xml"`.

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.

Tworzenie pliku śledzenia

W celu utworzenia pliku śledzenia:

1. Otwórz okno główne aplikacji.
2. W oknie głównym aplikacji kliknij przycisk .

   Zostanie otwarte okno **Wsparcie użytkownika**.
3. W oknie **Pomoc techniczna** kliknij przycisk **Śledzenie systemu**.

   Zostanie otwarte okno **Informacje dla działu pomocy technicznej**.
4. W celu uruchomienia procesu śledzenia należy zaznaczyć pole **Włącz śledzenie**.
5. Z listy rozwijalnej **Poziom** wybierz poziom śledzenia.

   Zaleca się uzgodnić wymagany poziom śledzenia ze specjalistami pomocy technicznej. Jeżeli z pomocy technicznej nie zostały przekazane żadne zalecenia, należy ustawić poziom śledzenia na **Normalny (500)**.
6. Odtwórz sytuację, która spowodowała wystąpienie problemu.
7. Aby zatrzymać proces śledzenia, wróć do okna **Informacje dla działu pomocy technicznej** i odznacz pole **Włącz śledzenie**.

Po utworzeniu pliku śledzenia, możesz przesłać wyniki śledzenia na serwer Kaspersky.

Zawartość i przechowywanie plików śledzenia

Użytkownik jest odpowiedzialny za bezpieczeństwo zgromadzonych danych, zwłaszcza za monitorowanie i ograniczanie dostępu do zgromadzonych danych, które są przechowywane na komputerze, dopóki nie zostaną one wysłane do Kaspersky.

Pliki śledzenia są przechowywane na komputerze w postaci zmodyfikowanej uniemożliwiającej ich odczytanie tak długo, jak aplikacja jest używana i są trwale usuwane, gdy aplikacja jest usuwana.

Pliki śledzenia są przechowywane w folderze ProgramData\Kaspersky Lab.

Plik śledzenia posiada nazwę w następującym formacie: `KES<numer wersji_dataXX.XX_czasXX.XX_pidXXX.><typ pliku śledzenia>.log.enc1`.

Plik śledzenia Agenta autoryzacji jest przechowywany w folderze informacji o woluminie systemowym i posiada następującą nazwę: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Możesz przejrzeć dane zapisane w plikach śledzenia. W celu uzyskania informacji dotyczących przeglądania danych, skontaktuj się z działem pomocy technicznej Kaspersky.

Wszystkie pliki śledzenia zawierają następujące dane:

- Czas zdarzenia.
- Liczbę procesów wykonania.

  Plik śledzenia Agenta autoryzacji nie zawiera tej informacji.

- Komponent aplikacji, który wywołał zdarzenie.
- Poziom priorytetu zdarzenia (zdarzenie informacyjne, ostrzeżenie, zdarzenie krytyczne, błąd).
- Opis zdarzenia dotyczący wykonania polecenia przez moduł aplikacji oraz wynik wykonania tego polecenia.

Zawartość plików śledzenia SRV.log, GUI.log oraz ALL.log

Oprócz ogólnych danych, pliki śledzenia SRV.log, GUI.log i ALL.log mogą przechowywać następujące informacje:

- Dane osobowe, łącznie z nazwiskiem, imieniem oraz drugim imieniem, jeśli takie dane są uwzględnione w ścieżce dostępu do plików na komputerze lokalnym.
- Nazwa użytkownika i hasło, jeśli były otwarcie przesyłane. Dane te mogą być zapisywane w plikach śledzenia podczas skanowania ruchu internetowego. Ruch sieciowy jest zapisywany w plikach śledzenia tylko z trafmon2.ppl.
- 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.

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 zawiera nie tylko ogólne dane, ale także informacje o zdarzeniach występujących podczas działania modułu połączeniowego Kaspersky Security Center.

Zawartość plików śledzenia wtyczek aplikacji

Pliki śledzenia wtyczek aplikacji zawierają nie tylko ogólne dane, ale także następujące informacje:

- Plik śledzenia shellex.dll.log wtyczki, która uruchamia zadania skanowania z poziomu menu kontekstowego, zawiera informacje o wykonaniu zadania skanowania oraz dane wymagane do debugowania wtyczki.
- Plik śledzenia mcou.OUTLOOK.EXE wtyczki modułu Ochrona poczty może zawierać fragmenty wiadomości e-mail wraz z adresami e-mail.

Zawartość pliku śledzenia Agenta autoryzacji

Oprócz ogólnych danych, plik śledzenia Agenta autoryzacji zawiera informacje o działaniu Agenta autoryzacji oraz o działaniach wykonywanych przez użytkownika na Agencie autoryzacji.

Włączanie i wyłączanie wysłania plików zrzutu pamięci i plików śledzenia do Kaspersky

W celu włączenia lub wyłączenia przesyłania plików zrzutu pamięci i plików śledzenia do Kaspersky:

1. Otwórz okno ustawień aplikacji.
2. W lewej części okna wybierz sekcję **Ustawienia zaawansowane**.

   W prawej części okna wyświetlone są zaawansowane ustawienia aplikacji.
3. W sekcji **Tryb działania** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Tryb działania**.
4. W oknie **Tryb działania** zaznacz pole **Włącz zapisywanie zrzutów pamięci**, aby włączyć zapisywanie plików zrzutu pamięci aplikacji.
5. Wykonaj jedną z poniższych czynności:

   - Zaznacz pole **Wysyłaj pliki zrzutu oraz śledzenia do Kaspersky**, jeśli chcesz, aby w przypadku błędu aplikacji, przy jej następnym uruchomieniu, w oknie **Prześlij na serwer informacje dla działu pomocy technicznej** zostało wyświetlone pytanie o wysłanie plików zrzutu i śledzenia do Kaspersky w celu ich analizy.
   - Jeśli nie chcesz, aby to miało miejsce, odznacz pole **Wysyłaj pliki zrzutu oraz śledzenia do Kaspersky**.

6. Kliknij przycisk **OK** w oknie **Tryb działania**.

7. Aby zapisać zmiany, w oknie głównym aplikacji kliknij przycisk **Zapisz**.

Przesyłanie plików na serwer pomocy technicznej

Pliki zawierające informacje o systemie operacyjnym, plikach śledzenia i plikach zrzutu muszą zostać wysłane do ekspertów z działu pomocy technicznej firmy Kaspersky.

W celu wysłania plików na serwer działu pomocy technicznej:

1. Uruchom ponownie program Kaspersky Endpoint Security po jakichkolwiek problemach z jego działaniem.

   Spowoduje to otwarcie okna **Poprzednie uruchomienie aplikacji nie powiodło się**.

   > Okno **Poprzednie uruchomienie aplikacji nie powiodło się** będzie uruchamiane przy każdym uruchomieniu Kaspersky Endpoint Security (także po ponownym uruchomieniu komputera), dopóki nie wyślesz plików zrzutu i plików śledzenia do pomocy technicznej lub nie klikniesz przycisku **Nie wysyłaj**.

2. W oknie **Poprzednie uruchomienie aplikacji nie powiodło się** otwórz listę wygenerowanych plików, klikając **tutaj**.

3. Zaznacz pola obok tych plików, które chcesz wysłać do pomocy technicznej.

4. Kliknij przycisk **Wyświetl tekst Regulacji**.

   Zostanie otwarte okno **Regulacje dotyczące dostarczania danych**.

5. Przeczytaj Regulacje dotyczące dostarczania danych i kliknij przycisk **Zamknij**.

6. W oknie **Poprzednie uruchomienie aplikacji nie powiodło się** zaznacz pole **Zgadzam się z Regulacjami dotyczącymi dostarczania danych**.

7. Kliknij przycisk **Wyślij**.

   Zostanie otwarte okno **Numer zgłoszenia**.

8. W oknie **Numer zgłoszenia** wprowadź numer przypisany do Twojego zgłoszenia po skontaktowaniu się z działem pomocy technicznej za pośrednictwem portalu Kaspersky CompanyAccount.

9. Kliknij **OK**.

Wybrane pliki danych zostaną spakowane i przesłane na serwer działu pomocy technicznej.

Włączanie i wyłączanie ochrony plików zrzutu i plików śledzenia

Pliki zrzutu oraz pliki śledzenia zawierają informacje o systemie operacyjnym, a także poufne 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 lokalny administrator, a także użytkownik, który włączył zapisywanie plików zrzutu pamięci i plików śledzenia.

- Dostęp do plików śledzenia może uzyskać tylko administrator systemowy i lokalny administrator.

W celu włączenia lub wyłączenia ochrony plików zrzutu i plików śledzenia:

1. Otwórz okno ustawień aplikacji.
2. Wybierz sekcję **Ustawienia zaawansowane** znajdującą się po lewej stronie.
   W prawej części okna wyświetlone są ustawienia aplikacji.
3. W sekcji **Tryb działania** kliknij przycisk **Ustawienia**.
   Zostanie otwarte okno **Tryb działania**.
4. Wykonaj jedną z poniższych czynności:
   - Jeśli chcesz włączyć ochronę, zaznacz pole **Włącz ochronę zrzutów pamięci i plików śledzenia**.
   - Jeśli chcesz wyłączyć ochronę, odznacz pole **Włącz ochronę zrzutów pamięci i plików śledzenia**.
5. Kliknij przycisk **OK** w oknie **Tryb działania**.
6. Aby zapisać zmiany, w oknie głównym aplikacji kliknij przycisk **Zapisz**.

Pliki zrzutu i pliki śledzenia, które zostały zapisane, gdy ochrona była aktywna, pozostaną chronione nawet po wyłączeniu tej funkcji.

Słownik

Agent autoryzacji

Interfejs służący do przejścia procesu autoryzacji w celu uzyskania dostępu do zaszyfrowanych dysków twardych i załadowania systemu operacyjnego po zaszyfrowaniu dysku twardego.

Agent sieciowy

Składnik Kaspersky Security Center umożliwiający interakcję Serwera administracyjnego z aplikacjami firmy Kaspersky zainstalowanymi na określonym węźle sieciowym (stacji roboczej lub serwerze). Ten komponent jest wspólny dla wszystkich aplikacji firmy Kaspersky działających pod systemem Windows. Dla aplikacji działających pod innymi systemami operacyjnymi przeznaczone są dedykowane wersje Agenta sieciowego.

Aktualizacja

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

Aktywny klucz

Klucz, który jest aktualnie używany przez aplikację.

Analiza heurystyczna

Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa.

Analiza przy użyciu sygnatur

Technologia wykrywania zagrożeń, która wykorzystuje bazy danych Kaspersky Endpoint Security zawierające opisy znanych zagrożeń oraz metody ich neutralizowania. Ochrona wykorzystująca analizę przy użyciu sygnatur zapewnia minimalny akceptowalny poziom bezpieczeństwa. Zgodnie z zaleceniami ekspertów z Kaspersky, metoda ta jest zawsze włączona.

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

Dokument elektroniczny zawierający klucz prywatny, informacje o właścicielu klucza oraz obszar klucza i potwierdzający, że klucz publiczny należy do właściciela. Certyfikat musi być podpisany przez centrum certyfikacji, które wydało certyfikat.

Certyfikat licencji

Dokument, który jest dostarczany użytkownikowi wraz z plikiem klucza lub kodem aktywacyjnym. Zawiera informacje o licencji nadanej użytkownikowi.

Czarna lista adresów

Lista adresów e-mail, z których wszystkie przychodzące wiadomości są blokowane przez Kaspersky bez względu na zawartość wiadomości.

Exploity

Kod programu, który wykorzystuje luki w systemie lub oprogramowaniu. Exploity są często używane do instalowania szkodliwego oprogramowania na komputerze bez wiedzy użytkownika.

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.

Klucz dodatkowy

Klucz, który daje prawo do korzystania z aplikacji, chociaż nie jest on aktualnie w użyciu.

Kopia zapasowa

Miejsce przechowywania kopii zapasowych plików utworzonych przed ich leczeniem lub usunięciem.

Kwarantanna

Kaspersky Endpoint Security umieszcza potencjalnie zainfekowane pliki w tym folderze. Pliki poddane kwarantannie są przechowywane w postaci zaszyfrowanej.

Łata

Mały dodatek do aplikacji, który naprawia błędy wykryte podczas działania aplikacji lub instaluje uaktualnienia.

Leczenie

Metoda przetwarzania zainfekowanych obiektów skutkująca pełnym lub częściowym odzyskaniem danych. Nie każdy zainfekowany obiekt może zostać wyleczony.

Maska pliku

Reprezentacja nazwy i rozszerzenia pliku przy użyciu symboli wieloznacznych.

Maski plików mogą zawierać dowolne znaki dozwolone w nazwach plików oraz symbole wieloznaczne:

- ***** – zastępuje zero lub więcej znaków.
- **?**– reprezentuje dowolny pojedynczy znak.

Należy pamiętać, że nazwa pliku i jego rozszerzenie zawsze są oddzielone kropką.

Moduły aplikacji

Pliki zawarte w pliku instalacyjnym aplikacji, które realizują podstawowe funkcje aplikacji. Każdemu rodzajowi zadania wykonywanego przez aplikację (ochrona w czasie rzeczywistym, skanowanie na żądanie i aktualizacja) odpowiada oddzielny moduł wykonywalny. Poprzez uruchomienie pełnego skanowania komputera z poziomu okna głównego aplikacji można rozpocząć wykonanie modułu tego zadania.

Network Agent Connector

Funkcja aplikacji pozwalająca na połączenie jej z Agentem sieciowym. Agent sieciowy umożliwia zdalne zarządzanie aplikacją poprzez Kaspersky Security Center.

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 ochronę antywirusową, 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.

Odcisk palca certyfikatu

Informacje używane do zidentyfikowania klucza certyfikatu. Odcisk palca jest tworzony poprzez zastosowanie kryptograficznej funkcji sumy kontrolnej do wartości klucza.

Phishing

Rodzaj oszustwa internetowego, które polega na wysyłaniu wiadomości elektronicznych w celu kradzieży poufnych informacji, najczęściej danych finansowych.

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.

Potencjalnie zainfekowany plik

Plik zawierający zmodyfikowany kod znanego wirusa lub kod przypominający wirusa, który nie został jeszcze wykryty przez specjalistów z Kaspersky. Prawdopodobnie zainfekowane pliki są wykrywane przy użyciu analizatora heurystycznego.

Przedmiot certyfikatu

Posiadacz klucza prywatnego skojarzonego z certyfikatem. Może to być użytkownik, aplikacja, dowolny obiekt wirtualny, komputer lub usługa.

Przenośny Menedżer plików

To jest aplikacja oferującą interfejs do pracy z zaszyfrowanymi plikami na nośnikach wymiennych, gdy funkcja szyfrowania nie jest dostępna na komputerze.

Przenoszenie plików do kwarantanny

Metoda przetwarzania prawdopodobnie zainfekowanego pliku, w której dostęp do pliku jest zablokowany, a sam plik zostaje przeniesiony z oryginalnej lokalizacji do folderu Kwarantanny. Jest on tam przechowywany w postaci zaszyfrowanej, co eliminuje ryzyko infekcji.

Serwer administracyjny

Moduł aplikacji Kaspersky Security Center realizujący funkcje scentralizowanego przechowywania informacji na temat wszystkich aplikacji firmy Kaspersky zainstalowanych w sieci korporacyjnej. Może być używany do zarządzania tymi aplikacjami.

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.

Usługa sieciowa

Ustaw parametry definiujące aktywność sieciową. Dla tej aktywności sieciowej możesz utworzyć regułę sieciową, która reguluje działanie Zapory sieciowej.

Ustawienia aplikacji

Ustawienia aplikacji, które są wspólne dla wszystkich typów zadań, odpowiadające za działanie aplikacji jako całości, np. ustawienia wydajności aplikacji, raportów, przechowywania kopii zapasowej.

Ustawienia zadania

Ustawienia aplikacji charakterystyczne dla każdego typu zadań.

Wystawca certyfikatu

Centrum certyfikacji, które wydało certyfikat.

Zadanie

Funkcje wykonywane przez aplikacje firmy Kaspersky jako zadania, na przykład: Ochrona plików w czasie rzeczywistym, Pełne skanowanie urządzenia, Aktualizacja baz danych.

Zainfekowany plik

Plik zawierający szkodliwy kod (kod znanego szkodliwego programu, który został wykryty podczas skanowania pliku). Kaspersky nie zaleca korzystania z takich plików, ponieważ mogą prowadzić do zainfekowania komputera.

Znormalizowana postać adresu zasobu sieciowego

Znormalizowana postać adresu zasobu sieciowego to tekstowa reprezentacja adresu zasobu sieciowego, uzyskana poprzez normalizację. Normalizacja to proces, w którym tekstowa reprezentacja adresu zasobu sieciowego zmienia się zgodnie z określonymi regułami (na przykład, wykluczenie portu połączenia, hasła i loginu HTTP z reprezentacji adresu zasobu sieciowego; dodatkowo adres zasobu sieciowego jest zmieniany z dużych znaków na małe).

W kontekście ochrony antywirusowej celem normalizacji adresu zasobu sieciowego jest pominięcie kolejnych skanowań adresów stron internetowych, które mają różną składnię, a fizycznie są takie same.

Przykład:

Nieznormalizowana postać adresu: www.Example.com\.

Znormalizowana postać adresu: www.example.com.

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 nazwy usług są własnością ich właścicieli.

Adobe, Acrobat i Shockwave są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Adobe Systems Incorporated zarejestrowanymi w Stanach Zjednoczonych i / lub innych krajach.

Mac i FireWire 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 innych krajach.

Słowo i znak Bluetooth oraz jego logo są własnością Bluetooth SIG, Inc.

Borland jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Borland Software Corporation w Stanach Zjednoczonych i innych krajach.

Citrix i Citrix Provisioning Services są znakami towarowymi firmy Citrix Systems, Inc. i/lub jej oddziałów, zarejestrowanymi w Urzędzie Patentowym w Stanach Zjednoczonych i innych krajach.

dbase jest znakiem towarowym firmy dataBased Intelligence, Inc.

EMC i SecurID są znakami towarowymi EMC Corporation lub zastrzeżonymi znakami towarowymi EMC Corporation zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

ICQ jest znakiem towarowym i / lub znakiem usługowym firmy ICQ LLC.

Intel i Pentium są znakami towarowymi firmy Intel Corporation zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

Logitech jest zastrzeżonym znakiem towarowym lub znakiem towarowym firmy Logitech Company zarejestrowanym w Stanach Zjednoczonych i innych krajach.

Mail.ru jest zastrzeżonym znakiem towarowym firmy Mail.Ru. LLC.

Microsoft, Windows, Internet Explorer, Access, Excel, PowerPoint, Outlook, Outlook Express, Windows Server, Visual Basic, Visual FoxPro, BitLocker, LifeCam Cinema, PowerShell i Surface są znakami towarowymi firmy Microsoft Corporation zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

Mozilla i Thunderbird są znakami towarowymi firmy Mozilla Foundation.

Novell jest znakiem towarowym firmy Novell, Inc. zarejestrowanym w Stanach Zjednoczonych i innych krajach.

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

SafeNet to zastrzeżony znak towarowy firmy SafeNet, Inc.

UNIX jest znakiem towarowym zarejestrowanym w Stanach Zjednoczonych i innych krajach i jest używany zgodnie z licencją nadaną przez X/Open Company Limited.