kaspersky

Kaspersky Security for Mobile

Spis treści

Pomoc dotycząca Kaspersky Security for Mobile

Kaspersky Security for Mobile jest przeznaczony do ochrony i zarządzania firmowymi urządzeniami mobilnymi, a także osobistymi urządzeniami mobilnymi używanymi przez pracowników firmy do celów firmowych.

Komponenty i funkcje Kaspersky Security for Mobile zależą od konsoli Kaspersky Security Center, której używasz jako interfejsu do ochrony i zarządzania urządzeniami mobilnymi.

Wybierz odpowiednią sekcję Pomocy, w zależności od konsoli Kaspersky Security Center:

- Konsola administracyjna oparta na Microsoft Management Console
- Kaspersky Security Center Web Console lub Kaspersky Security Center Cloud Console

Oddzielne sekcje Pomocy opisują funkcje i działania, które są dostępne dla użytkowników aplikacji Kaspersky Endpoint Security for Android i Kaspersky Security for iOS.

Nowości

Kaspersky Security for iOS Technical Release 1

Nowa aplikacja Kaspersky Security for iOS jest przeznaczona do ochrony firmowych urządzeń z systemem iOS i oPadOS oraz zarządzania nimi. Aplikacja oferuje następujące kluczowe funkcje:

- Ochrona przed zagrożeniami internetowymi.
- Wykrywanie zdjęcia zabezpieczeń systemu.
- Zarządzanie firmowymi urządzeniami za pomocą Kaspersky Security Center Web Console i Cloud Console.

Kaspersky Endpoint Security for Android Technical Release 42

- Ulepszenia interfejsu użytkownika w aplikacji Kaspersky Endpoint Security for Android.
- Aplikacja Kaspersky Endpoint Security for Android wymaga teraz uprawnienia "Urządzenia Bluetooth w pobliżu" w systemie Android 12 lub nowszym, aby umożliwić administratorowi ograniczanie użycia funkcji Bluetooth.
- Wprowadzono ogólne ulepszenia i poprawki błędów.

Kaspersky Endpoint Security for Android Technical Release 41

- Ulepszenia interfejsu użytkownika w aplikacji Kaspersky Endpoint Security for Android.
- Ulepszenia interfejsu użytkownika w ustawieniach zasad wtyczki Kaspersky Security for Mobile (Policies) dla produktów Kaspersky Security Center Web Console i Cloud Console.
- Wprowadzono ogólne ulepszenia i poprawki błędów.

Kaspersky Endpoint Security for Android Technical Release 40

- Wprowadzono ogólne ulepszenia i poprawki błędów.

Kaspersky Endpoint Security for Android Technical Release 39

- Dodano obsługę Android 12L.
- Zaktualizowano następujące umowy i oświadczenia:
  - Umowa licencyjna
  - Oświadczenie Kaspersky Security Network
  - Oświadczenie dotyczące przetwarzania danych w celach marketingowych

Pamiętaj, że administrator może zaakceptować nowe warunki umów i oświadczeń w Konsoli administracyjnej. To umożliwi pominięcie tego etapu dla użytkowników aplikacji Kaspersky Endpoint Security for Android na urządzeniach.

- Wprowadzono ogólne ulepszenia i poprawki błędów.

Kaspersky Endpoint Security for Android Technical Release 33

- Podczas zarządzania aplikacją Kaspersky Endpoint Security for Android przy użyciu systemów EMM innych firm możesz teraz zaakceptować wiele umów licencyjnych użytkownika końcowego za pomocą jednego polecenia.
- Nie potrzebujesz już klucza do aktywacji Samsung KNOX.
- Struktura wersji komponentu Kaspersky Security for Mobile została zmodyfikowana w celu uwzględnienia numeru wydania.

Kaspersky Endpoint Security for Android Technical Release 32

- Aplikacja Kaspersky Endpoint Security for Android została zmodyfikowana w celu obsługi zaktualizowanych wymagań systemu Android.

Kaspersky Endpoint Security for Android Technical Release 31

- Jeśli Kaspersky Security Center nie jest zainstalowany w Twojej organizacji lub nie jest dostępny dla urządzeń mobilnych, użytkownicy mogą ręcznie aktywować aplikację Kaspersky Endpoint Security for Android na swoich urządzeniach.
- Kaspersky Security for Mobile obsługuje teraz funkcję Kart niestandardowych (Custom Tabs) dla przeglądarki Google Chrome.

Kaspersky Endpoint Security for Android Technical Release 30

- Kaspersky Security for Mobile umożliwia teraz ochronę i zarządzanie urządzeniami mobilnymi w Kaspersky Security Center Cloud Console.
- Kaspersky Security for Mobile obsługuje teraz systemy iOS 15 i iPadOS 15.

Kaspersky Endpoint Security for Android Technical Release 29

- Kaspersky Endpoint Security for Android obsługuje teraz system Android 12.

Kaspersky Endpoint Security for Android Technical Release 27

- Kaspersky Security for Mobile umożliwia teraz ochronę i zarządzanie urządzeniami mobilnymi w Kaspersky Security Center Web Console.

Kaspersky Endpoint Security for Android Technical Release 26

- Kaspersky Endpoint Security obsługuje teraz licencje i subskrypcje z automatycznym odnawianiem.

Kaspersky Endpoint Security for Android Technical Release 22

- Kaspersky Endpoint Security obsługuje teraz Kaspersky Private Security Network, rozwiązanie, które umożliwia dostęp do baz danych reputacji Kaspersky Security Network bez wysyłania danych poza sieć korporacyjną.
- Kaspersky Endpoint Security for Android nie obsługuje już instalacji na urządzeniach z systemem Android w wersjach 4.2 - 4.4.4.

Kaspersky Endpoint Security for Android Technical Release 20

- Użytkownicy nie są proszeni o akceptację oświadczeń prawnych, jeśli administrator zdecydował się zaakceptować oświadczenia globalnie.
- Wydajność aplikacji została zoptymalizowana.

Kaspersky Endpoint Security for Android Technical Release 19

- Administrator może teraz akceptować Kaspersky Security Network i inne oświadczenia w imieniu użytkowników końcowych za pośrednictwem Kaspersky Security Center.
- Naprawiono kilka błędów i poprawiono stabilność działania.

Kaspersky Endpoint Security for Android Technical Release 18

- Kaspersky Security for Mobile obsługuje teraz usługi mobilne Huawei.
- Kaspersky Endpoint Security for Android jest teraz dostępny do zainstalowania z Huawei App Gallery.

Kaspersky Endpoint Security for Android Technical Release 17

- Kaspersky Endpoint Security jest teraz ukierunkowany na poziom API 29 i wyższy, powodując pewne zmiany w zachowaniu aplikacji na urządzeniach z systemem Android 10 lub nowszym.
- Nowe ustawienia siły hasła dla użytkownika, aby ustawiać hasła o wymaganej złożoności.
- Konfigurowanie używania odcisku palca jako metody odblokowywania ekranu jest teraz dostępne tylko w profilu roboczym Android.
- Naprawiono kilka błędów i poprawiono stabilność działania.

Kaspersky Endpoint Security for Android Technical Release 16

- Kaspersky Endpoint Security for Android obsługuje system Android 11.

- Program został dostosowany do nowych wymagań odnośnie uprawnień do geolokalizacji i korzystania z aparatu wprowadzonych w systemie Android 11. Więcej informacji o nowych zasadach dotyczących uprawnień dostępu do aparatu i lokalizacji można znaleźć w tej sekcji.

- Teraz możesz określać firmowe adresy e-mail użytkowników w konsoli EMM innej firmy. Te adresy e-mail będą wyświetlane w Kaspersky Security Center, pod warunkiem że skonfigurowano KscCorporateEmail.

Kaspersky Endpoint Security for Android Technical Release 14

- Ilekroć użytkownik zezwala lub odbiera uprawnienia administratora urządzenia do aplikacji, zdarzenie jest wysyłane do Konsoli zarządzającej.

- Parametr "KscGroup" może zostać skonfigurowany w konsolach EMM innych firm. Gdy urządzenie łączy się z Kaspersky Security Center, jest automatycznie dodawane do podfolderu w folderze Nieprzypisane urządzenia o tej samej nazwie, co grupa skonfigurowana w konsoli EMM.

Kaspersky Endpoint Security for Android Technical Release 13

- Nowy wygląd interfejsu użytkownika dla Kaspersky Endpoint Security for Android.

- Wszystkie sekcje pomocy bazują teraz online.

- Adresy IP zarządzanych urządzeń są teraz wysyłane do Kaspersky Security Center i mogą być przeglądane w sekcjach informacji o urządzeniu.

Kaspersky Endpoint Security for Android Technical Release 12

- Dodano możliwość zdalnego zaakceptowania Umowy licencyjnej w Kaspersky Security Center 12. Jeśli administrator zaakceptuje Umowę licencyjną i Politykę prywatności w Konsoli administracyjnej, aplikacja pominie te kroki w trakcie procesu instalacji.

- Dodano możliwość edytowania nazwy urządzenia w Kaspersky Security Center dla urządzenia, którzy korzystają z VMware AirWatch. Dodano nowe ustawienie do pliku konfiguracyjnego, który jest używany do konfigurowania aplikacji. Możesz dodać więcej informacji do nazwy urządzenia (na przykład, numer seryjny urządzenia). Ułatwia to znalezienie i posortowanie urządzeń w Kaspersky Security Center.

Kaspersky Endpoint Security for Android Technical Release 11

Naprawiono kilka błędów i poprawiono stabilność działania.

Kaspersky Endpoint Security for Android Technical Release 10

- Kaspersky Security for Mobile obsługuje teraz Kaspersky Security Center 12.

- Obsługa Kaspersky Safe Browser została przerwana w Kaspersky Security Center 12. Możesz używać funkcji Kaspersky Safe Browser podczas korzystania z Kaspersky Security Center 11 lub wcześniejszej wersji.

- Naprawiono kilka błędów i poprawiono stabilność działania.

Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3

- Dodano obsługę Kaspersky Endpoint Security for Android w Microsoft Intune (rozwiązanie Enterprise Mobility Management (EMM)). Kaspersky uczestniczy w AppConfig Community, aby zapewnić, że aplikacja działa z rozwiązaniami EMM firm trzecich.

- Dodano możliwość wyłączania powiadomień i wiadomości wyskakujących, gdy aplikacja działa w tle. Należy pamiętać, że wykonywanie tych działań w tle nie jest bezpieczne. Jeśli wyłączysz powiadomienia i wiadomości wyskakujące, gdy aplikacja działa w tle, aplikacja nie ostrzeże użytkowników o zagrożeniach w czasie rzeczywistym. Użytkownicy urządzeń mobilnych mogą poznać stan ochrony urządzenia tylko wtedy, gdy otworzą aplikację.

- Dodano możliwość zaakceptowania Umowy licencyjnej i Polityki prywatności w VMware AirWatch. Jeśli administrator zaakceptował Umowę licencyjną i Politykę prywatności w AirWatch Console, Kaspersky Endpoint Security for Android pominie krok akceptacji w Kreatorze wstępnej konfiguracji.

- Dodano Oświadczenie dotyczące przetwarzania danych na potrzeby modułu Ochrona WWW (Oświadczenie dotyczące modułu Ochrona WWW). Należy zaakceptować oświadczenie dotyczące korzystania z modułu Ochrona WWW. Kaspersky Endpoint Security for Android używa Kaspersky Security Network (KSN) do skanowania stron internetowych. Oświadczenie dotyczące modułu Ochrona WWW zawiera Warunki i postanowienia dotyczące wymiany danych z KSN. Możesz zaakceptować Oświadczenie dotyczące modułu Ochrona WWW w zasadzie lub poprosić o akceptację użytkownika urządzenia.

- Naprawiono kilka błędów i poprawiono stabilność działania.

Porównanie funkcji aplikacji w zależności od narzędzi do zarządzania

Możesz zarządzać urządzeniami mobilnymi w Kaspersky Security Center przy użyciu następujących narzędzi do zarządzania:

- Oparta na Microsoft Management Console (zwana dalej "opartą na MMC") Konsola administracyjna Kaspersky Security Center
- Kaspersky Security Center Web Console
- Kaspersky Security Center Cloud Console

W poniższej tabeli porównano funkcje dostępne w tych narzędziach.

Dostępność funkcji w zależności od narzędzi do zarządzania

	Konsola oparta na MMC	Web Console	Cloud Console
Ogólne			
Zarządzanie urządzeniami Android	Dostępne	Dostępne	Dostępne
Zarządzanie urządzeniami iOS	Dostępne (przez certyfikat APN)	Dostępne (przez aplikację Kaspersky Security for iOS)	Dostępne (przez aplikację Kaspersky Security for iOS)
Zarządzanie urządzeniami mobilnymi			
Dodawanie urządzeń za pomocą odnośnika Google Play	Dostępne	Dostępne	Dostępne
Dodawanie urządzeń za pomocą linku App Store	Niedostępne	Dostępne	Dostępne
Dodawanie urządzeń iOS za pomocą profilu IOS MDM	Dostępne	Niedostępne	Niedostępne
Dodawanie urządzeń poprzez tworzenie pakietu instalacyjnego	Dostępne	Niedostępne	Niedostępne
Wysyłanie poleceń na urządzenia mobilne	Dostępne	Dostępne (z wyjątkiem polecenia Mugshot)	Dostępne (z wyjątkiem polecenia Mugshot)
Usuwanie urządzeń mobilnych z Kaspersky Security Center	Dostępne	Dostępne (Usuwanie tylko z listy urządzeń. Aplikację należy usunąć z urządzenia ręcznie).	Dostępne (Usuwanie tylko z listy urządzeń. Aplikację należy usunąć z urządzenia ręcznie).
Zarządzanie certyfikatami			
Wystawianie certyfikatów pocztowych	Dostępne	Niedostępne	Niedostępne
Wystawianie certyfikatów VPN	Dostępne	Niedostępne	Niedostępne
Wystawianie certyfikatów mobilnych	Dostępne	Dostępne	Dostępne

Wystawianie certyfikatów mobilnych za pomocą narzędzi Serwera administracyjnego	Dostępne	Dostępne	Dostępne
Określanie plików certyfikatu	Dostępne	Niedostępne	Niedostępne
Integracja z infrastrukturą klucza publicznego	Dostępne	Niedostępne	Niedostępne
Zarządzanie zasadami			
Dostęp oparty na rolach do konfigurowania zasad grupy	Dostępne	Niedostępne	Niedostępne
Konfigurowanie synchronizacji urządzenia mobilnego z Kaspersky Security Center	Dostępne	Dostępne	Dostępne
Konfigurowanie skanowania antywirusowego na urządzeniach mobilnych	Dostępne	Dostępne	Dostępne
Konfigurowanie ochrony urządzenia mobilnego	Dostępne	Dostępne	Dostępne
Konfigurowanie aktualizacji antywirusowych baz danych	Dostępne	Dostępne	Dostępne
Konfigurowanie ochrony danych na skradzionym lub zagubionym urządzeniu	Dostępne	Dostępne	Dostępne
Konfigurowanie dostępu użytkownika do stron internetowych	Dostępne	Dostępne	Dostępne
Konfigurowanie kontroli aplikacji	Dostępne	Dostępne	Dostępne
Konfigurowanie kontroli zgodności	Dostępne	Dostępne	Dostępne
Konfigurowanie profilów roboczych Android	Dostępne	Niedostępne	Niedostępne
Konfigurowanie połączenia z siecią Wi-Fi	Dostępne	Niedostępne	Niedostępne
Samsung KNOX	Dostępne	Niedostępne	Niedostępne
Inne funkcje			
Globalna akceptacja Umowy licencyjnej w Kaspersky Security Center	Dostępne	Niedostępne	Niedostępne
Konfigurowanie Kaspersky Private Security Network	Dostępne	Niedostępne	Niedostępne

Pakiet dystrybucyjny

Zestaw dystrybucyjny Kaspersky Security for Mobile może zawierać różne komponenty, w zależności od wybranej wersji aplikacji.

Zarządzanie urządzeniami mobilnymi w Kaspersky Security Center Web Console

- `on_prem_ksm_devices_xx.x.x.x.zip`

  Archiwum zawierające pliki wymagane do instalacji wtyczki Kaspersky Security for Mobile (Devices):

  - `plugin.zip`

    Archiwum zawierające wtyczkę Kaspersky Security for Mobile (Devices).

  - `signature.txt`

    Plik zawierający podpis wtyczki Kaspersky Security for Mobile (Devices).

- `on_prem_ksm_policies_xx.x.x.x.zip`

  Archiwum zawierające pliki wymagane do instalacji wtyczki Kaspersky Security for Mobile (Policies):

  - `plugin.zip`

    Archiwum zawierające wtyczkę Kaspersky Security for Mobile (Policies).

  - `signature.txt`

    Plik zawierający podpis wtyczki Kaspersky Security for Mobile (Policies).

Zarządzanie urządzeniami mobilnymi w Kaspersky Security Center Cloud Console

Aby zarządzać urządzeniem mobilnym w Kaspersky Security Center Cloud Console, nie musisz pobierać pakietu dystrybucyjnego. Wystarczy utworzyć konto w Kaspersky Security Center Cloud Console. Więcej informacji na temat tworzenia konta znajdziesz w pomocy *Kaspersky Security Center Cloud Console*.

Zarządzanie urządzeniami mobilnymi w Konsoli administracyjnej opartej na MMC

- `Klcfginst_en.exe`

  Plik instalacyjny wtyczki zarządzającej Kaspersky Endpoint Security for Android do zarządzania aplikacją poprzez system zdalnego zarządzania Kaspersky Security Center.

- `Klmdminst.exe`

  Plik instalacyjny wtyczki zarządzającej Kaspersky Device Management for iOS do zarządzania aplikacją poprzez system zdalnego zarządzania Kaspersky Security Center.

Plik aplikacji Kaspersky Endpoint Security for Android

`KES10_xx_xx_xxx.apk` — plik pakietu Android aplikacji Kaspersky Endpoint Security for Android.

Pliki pomocnicze

- `sc_package_xx.exe`

  Samorozpakowujące się archiwum zawierające pliki wymagane do zainstalowania aplikacji Kaspersky Endpoint Security for Android poprzez utworzenie pakietów instalacyjnych:

  - `adb.exe, AdbWinApi.dll, AdbWinUsbApi.dll`

    Pliki wymagane do tworzenia pakietów instalacyjnych.

  - `installer.ini`

    Plik konfiguracyjny zawierający ustawienia połączenia z Serwerem administracyjnym.

  - `KES10_xx_xx_xxx.apk`

    Plik pakietu Android aplikacji Kaspersky Endpoint Security for Android.

  - `kmlisten.exe`

    Narzędzie do dostarczania pakietów instalacyjnych za pośrednictwem komputera administratora.

  - `kmlisten.ini`

    Plik konfiguracyjny zawierający ustawienia narzędzia `kmlisten.exe`.

  - `kmlisten.kpd`

    Plik z opisem aplikacji.

- `SigningUtility.zip`

  Archiwum zawierające narzędzie do podpisywania pakietów dystrybucyjnych aplikacji Kaspersky Endpoint Security for Android oraz kontenerów dla urządzeń iOS.

Dokumentacja

- Pomoc dla Kaspersky Security for Mobile.

Praca w Kaspersky Security Center Web Console i Kaspersky Security Center Cloud Console

Ta sekcja Pomocy opisuje ochronę i zarządzanie urządzeniami mobilnymi przy użyciu Kaspersky Security Center Web Console (zwanej dalej także Web Console) lub Kaspersky Security Center Cloud Console (zwanej dalej także Cloud Console).

Informacje o zarządzaniu urządzeniami mobilnymi w Kaspersky Security Center Web Console i Cloud Console

Możesz zarządzać urządzeniami mobilnymi w Kaspersky Security Center Web Console i Cloud Console przy użyciu następujących komponentów:

- **Aplikacja Kaspersky Endpoint Security for Android**

  Aplikacja Kaspersky Endpoint Security for Android zapewnia ochronę urządzeń mobilnych przed zagrożeniami internetowymi, wirusami i innymi programami, które stanowią zagrożenie.

- **Aplikacja Kaspersky Security for iOS**

  Aplikacja Kaspersky Security for iOS chroni urządzenia mobilne przed atakami phishingowymi i złośliwym oprogramowaniem.

- **Wtyczka Kaspersky Security for Mobile (Devices)**

  Wtyczka Kaspersky Security for Mobile (Devices) dostarcza interfejs do zarządzania urządzeniami mobilnymi i zainstalowanymi na nich aplikacjami mobilnymi za pośrednictwem Kaspersky Security Center Web Console i Cloud Console.

- **Wtyczka Kaspersky Security for Mobile (Policies)**

  Wtyczka Kaspersky Endpoint Security for Mobile (Policies) umożliwia zdefiniowanie ustawień konfiguracyjnych dla urządzeń podłączonych do Kaspersky Security Center przy użyciu zasad grupy.

Wtyczki są zintegrowane z *systemem zdalnego zarządzania Kaspersky Security Center*. Możesz użyć Kaspersky Security Center Web Console lub Cloud Console do zarządzania urządzeniami mobilnymi, a także komputerami klienckimi i systemami wirtualnymi. Po podłączeniu urządzeń mobilnych do Serwera administracyjnego jest możliwość zarządzania nimi. Możesz zdalnie monitorować zarządzane urządzenia.

Najważniejsze funkcje zarządzania urządzeniami mobilnymi w Kaspersky Security Center Web Console i Cloud Console

Kaspersky Security for Mobile dostarcza następujące funkcje:

- Dystrybucja wiadomości e-mail w celu połączenia urządzeń mobilnych Android z Kaspersky Security Center za pomocą linków do pobrania aplikacji Kaspersky Endpoint Security for Android z Google Play.

- Dystrybucja wiadomości e-mail w celu połączenia urządzeń mobilnych iOS z Kaspersky Security Center za pomocą linków do pobrania aplikacji Kaspersky Security for iOS z App Store.

- Zdalne połączenie urządzeń mobilnych z Kaspersky Security Center i innymi systemami EMM firm trzecich (na przykład, VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl).

- Zdalna konfiguracja aplikacji mobilnej, a także zdalna konfiguracja usług, aplikacji i funkcji urządzeń mobilnych.
- Zdalna konfiguracja urządzeń mobilnych zgodnie z firmowymi wymaganiami bezpieczeństwa.
- Zapobieganie wyciekowi informacji firmowych przechowywanych na urządzeniach mobilnych w przypadku ich zagubienia lub kradzieży (Anti-Theft). Obsługuje wyłącznie urządzenia z systemem Android.
- Kontrolę zgodności z firmowymi wymaganiami bezpieczeństwa (Kontrola zgodności). Obsługuje wyłącznie urządzenia z systemem Android.
- Sterowanie ochroną przed zagrożeniami internetowymi i sterowanie używania Internetu na urządzeniach mobilnych (Ochrona WWW).
- Konfiguracja powiadomień wyświetlanych użytkownikowi w aplikacjach Kaspersky Endpoint Security for Android i Kaspersky Security for iOS.
- Powiadomienia administratora o stanie i zdarzeniach aplikacji Kaspersky Endpoint Security for Android i Kaspersky Security for iOS mogą być przesyłane w Kaspersky Security Center lub pocztą e-mail.
- Zmiana kontroli ustawień zasady (historia rewizji).

Kaspersky Security for Mobile zawiera następujące komponenty ochrony i zarządzania:

- Antywirus (dla urządzeń z systemem Android)
- Anti-Theft (dla urządzeń z systemem Android)
- Ochrona WWW (dla urządzeń z systemami Android i iOS)
- Kontrola aplikacji (dla urządzeń z systemem Android)
- Kontrola zgodności (dla urządzeń z systemem Android)
- Wykrywanie uprawnień administratora na urządzeniach z systemem Android i wykrywanie zdjęcia zabezpieczeń systemu na urządzeniach iOS.

Informacje o aplikacji Kaspersky Endpoint Security for Android

Aplikacja Kaspersky Endpoint Security for Android zapewnia ochronę urządzeń mobilnych przed zagrożeniami internetowymi, wirusami i innymi programami, które stanowią zagrożenie.

Aplikacja Kaspersky Endpoint Security for Android zawiera następujące komponenty:

- **Anti-Virus**. Ten składnik wykrywa i neutralizuje zagrożenia na Twoim urządzeniu, korzystając z antywirusowych baz danych i usługi chmury Kaspersky Security Network. Antywirus zawiera następujące komponenty:
  - **Ochrona**. Wykrywa zagrożenia w otwieranych plikach, skanuje nowe aplikacje i zapobiega infekcjom urządzenia w czasie rzeczywistym.
  - **Skanowanie**. Jest uruchamiane na żądanie dla całego systemu plików, tylko dla zainstalowanych aplikacji lub wybranego pliku bądź folderu.
  - **Aktualizacja**. Umożliwia pobranie nowych antywirusowych baz danych dla aplikacji.

- **Anti-Theft**. Ten moduł chroni informacje na urządzeniu przed nieautoryzowanym dostępem w przypadku zgubienia lub kradzieży urządzenia. Ten moduł umożliwia wysyłanie następujących poleceń do urządzenia:
  - **Lokalizacja**. Uzyskaj współrzędne lokalizacji urządzenia.
  - **Alarm**. Spraw, aby urządzenie wydało głośny alarm.
  - **Usuń**. Usuń dane firmowe w celu ochrony poufnych informacji firmowych.
- **Ochrona WWW**. Komponent ten blokuje szkodliwe witryny stworzone w celu rozprzestrzeniania się szkodliwego kodu. Ochrona WWW blokuje również fałszywe (phishingowe) strony internetowe stworzone w celu kradzieży poufnych danych użytkownika (na przykład haseł do bankowości elektronicznej bądź systemów płatności elektronicznych) i dostępu do informacji finansowych użytkownika. Ochrona WWW skanuje strony internetowe przed ich otwarciem, korzystając z usługi chmury Kaspersky Security Network. Po skanowaniu, Ochrona WWW zezwala zaufanym stronom internetowym na załadowanie się i blokuje szkodliwe strony internetowe. Ochrona WWW obsługuje również filtrowanie stron internetowych według kategorii zdefiniowanych w usłudze chmury Kaspersky Security Network. To umożliwia administratorowi ograniczenie dostępu użytkownika do pewnych kategorii stron internetowych (na przykład kategorie "Hazard, loterie, zakłady bukmacherskie" lub "Komunikacja przez internet").
- **Kontrola aplikacji.** Komponent ten umożliwia zainstalowanie zalecanych i wymaganych aplikacji na urządzeniu za pośrednictwem bezpośredniego odnośnika do pakietu dystrybucyjnego lub odnośnika do Google Play. Kontrola aplikacji umożliwia usunięcie zablokowanych aplikacji, które naruszają firmowe wymagania bezpieczeństwa.
- **Kontrola zgodności.** Komponent ten umożliwia sprawdzanie zarządzanych urządzeń pod kątem zgodności z firmowymi wymaganiami bezpieczeństwa oraz nakładanie ograniczeń na niektóre funkcje niezgodnych urządzeń.

Możesz skonfigurować komponenty aplikacji Kaspersky Endpoint Security for Android w Kaspersky Security Center Web Console i Cloud Console, definiując ustawienia zasad grupy.

Informacje o aplikacji Kaspersky Security for iOS

Aplikacja Kaspersky Security for iOS chroni urządzenia mobilne przed atakami phishingowymi i złośliwym oprogramowaniem.

Aplikacja Kaspersky Security for iOS dostarcza następujące najważniejsze funkcje:

- **Ochrona WWW**. Komponent ten blokuje szkodliwe witryny stworzone w celu rozprzestrzeniania się szkodliwego kodu. Ochrona WWW blokuje również fałszywe (phishingowe) strony internetowe stworzone w celu kradzieży poufnych danych użytkownika (na przykład haseł do bankowości elektronicznej bądź systemów płatności elektronicznych) i dostępu do informacji finansowych użytkownika. Ochrona WWW skanuje strony internetowe przed ich otwarciem, korzystając z usługi chmury Kaspersky Security Network. Po skanowaniu, Ochrona WWW zezwala zaufanym stronom internetowym na załadowanie się i blokuje szkodliwe strony internetowe. Ten komponent możesz skonfigurować Kaspersky Security Center Web Console, definiując ustawiania zasad grupowych.
- **Wykrywanie zdjęcia zabezpieczeń systemu**. Gdy aplikacja Kaspersky Security for iOS wykryje zdjęcie zabezpieczeń systemu, wyśle komunikat o znaczeniu krytycznym i poinformuje Cię o problemie.

Informacje o wtyczce Kaspersky Security for Mobile (Devices)

Wtyczka Kaspersky Security for Mobile (Devices) dostarcza interfejs do zarządzania urządzeniami mobilnymi i zainstalowanymi na nich aplikacjami mobilnymi za pośrednictwem Kaspersky Security Center Web Console i Cloud Console. Wtyczka Kaspersky Security for Mobile (Devices) umożliwia wykonanie następujących czynności:

- Podłącz urządzenia mobilne do Kaspersky Security Center.
- Zarządzaj certyfikatami urządzeń mobilnych.
- Skonfiguruj Firebase Cloud Messaging (wyłącznie dla urządzeń z systemem Android).
- Wysyłaj polecenia na urządzenia mobilne (wyłącznie dla urządzeń z systemem Android).

Wtyczkę Kaspersky Security for Mobile (Devices) można zainstalować podczas konfigurowania Kaspersky Security Center Web Console. Jeśli korzystasz z Kaspersky Security Center Cloud Console, nie musisz instalować tej wtyczki. Więcej informacji na temat scenariuszy wdrożenia w różnych typach konsol można znaleźć w sekcji "Scenariusze wdrożenia"

Informacje o wtyczce Kaspersky Security for Mobile (Policies)

Wtyczka Kaspersky Security for Mobile (Policies) umożliwia zdefiniowanie ustawień konfiguracyjnych dla urządzeń podłączonych do Kaspersky Security Center przy użyciu zasad grupy. Wtyczka Kaspersky Security for Mobil (Policies) może być używana do wykonywania następujących czynności:

- Utworzenie grupowych zasad zabezpieczających dla urządzeń mobilnych.
- Zdalne skonfigurowanie ustawień działania aplikacji na urządzeniach mobilnych użytkowników.
- Otrzymywanie raportów i statystyk dotyczących działania aplikacji mobilnej na urządzeniach mobilnych użytkowników.

Wtyczkę Kaspersky Security for Mobile (Policies) można zainstalować podczas konfigurowania Kaspersky Security Center Web Console. Jeśli korzystasz z Kaspersky Security Center Cloud Console, nie musisz instalować tej wtyczki. Więcej informacji na temat scenariuszy wdrożenia w różnych typach konsol można znaleźć w sekcji "Scenariusze wdrożenia"

Wymagania sprzętowe i programowe

W tej sekcji znajdują się wymagania sprzętowe i oprogramowaniowe dla komputera administratora, który jest wykorzystywane do instalacji wtyczki Kaspersky Security for Mobile (Devices) oraz wtyczki Kaspersky Security for Mobile (Policies) w Kaspersky Security Center Web Console i Cloud Console, a także wymagania sprzętowe i oprogramowaniowe aplikacji mobilnych.

Wymagania sprzętowe i programowe komputera administratora

Aby zainstalować wtyczkę Kaspersky Security for Mobile (Devices) i wtyczkę Kaspersky Security for Mobile (Policies), komputer administratora musi spełniać wymagania sprzętowe Kaspersky Security Center. Aby uzyskać więcej informacji na temat wymagań sprzętowych i programowych Kaspersky Security Center:

- Jeśli korzystasz z Kaspersky Security Center Web Console, zapoznaj się z *Pomocą Kaspersky Security Center*.
- Jeśli korzystasz z Kaspersky Security Center Cloud Console, zapoznaj się z *Pomocą Kaspersky Security Center Cloud Console*.

Aby korzystać z wtyczki Kaspersky Security for Mobile (Devices) i wtyczki Kaspersky Security for Mobile (Policies) w Kaspersky Security Center Web Console, na komputerze administratora musi być zainstalowany Kaspersky Security Center Web Console.

Aby korzystać z wtyczki Kaspersky Security for Mobile (Devices) i wtyczki Kaspersky Security for Mobile (Policies) w Kaspersky Security Center Cloud Console, musisz utworzyć konto w Kaspersky Security Center Cloud Console. Więcej informacji na temat tworzenia konta znajdziesz w pomocy *Kaspersky Security Center Cloud Console*.

Aplikacja Kaspersky Endpoint Security for Android może działać w obrębie systemów EMM innych firm:

- VMware AirWatch 9.3 lub nowszy
- MobileIron 10.0 lub nowszy
- IBM MaaS360 10.68 lub nowszy
- Microsoft Intune 1908 lub nowszy
- SOTI MobiControl 14.1.4 (1693) lub nowszy

Wymagania sprzętowe i programowe wobec urządzenia mobilnego użytkownika w celu obsługi instalacji aplikacji Kaspersky Endpoint Security for Android

Aplikacja Kaspersky Endpoint Security for Android posiada następujące wymagania sprzętowe i programowe:

- Smartfon lub tablet z ekranem o rozdzielczości 320x480 pikseli lub wyższej
- 65 MB wolnej przestrzeni w głównej pamięci urządzenia
- Android 5.0–12 (w tym Android 12L, za wyjątkiem Go Edition)
- Architektura procesora x86, x86-64, Arm5, Arm6, Arm7 lub Arm8

Aplikację można zainstalować tylko w pamięci głównej urządzenia.

Wymagania sprzętowe i programowe wobec urządzenia mobilnego użytkownika w celu obsługi instalacji aplikacji Kaspersky Security for iOS

Aplikacja Kaspersky Security for iOS ma następujące wymaganie sprzętowe:

- iPhone 6S lub nowszy
- iPad Air 2 lub nowszy

Aplikacja Kaspersky Security for iOS ma następujące wymaganie dotyczące oprogramowania:

- iOS 14.1 lub nowszy
- iPadOS 14.1 lub nowszy

Aplikacja Kaspersky Security for iOS nie może działać poprawnie, kiedy na urządzeniu mobilnym uruchomiony jest klient VPN nawiązujący aktywne połączenie sieci VPN.

Znane problemy i uwagi

Kaspersky Endpoint Security for Android oraz Kaspersky Security for iOS posiadają kilka znanych problemów, które nie mają krytycznego znaczenia dla ich działania.

Znane problemy z aplikacją Kaspersky Security for iOS

- Aplikacja Kaspersky Security for iOS nie może działać poprawnie, kiedy na urządzeniu mobilnym uruchomiony jest klient VPN nawiązujący aktywne połączenie sieci VPN.

Znane problemy z aplikacją Kaspersky Endpoint Security for Android

Znane problemy podczas uruchamiania zarządzania urządzeniami mobilnymi w Kaspersky Security Center Web Console

- Zarządzanie urządzeniami mobilnymi można uruchomić podczas wstępnej konfiguracji Konsoli administracyjnej opartej na MMC programu Kaspersky Security Center (podczas działania Kreatora wstępnej konfiguracji) lub później, wyświetlając w Konsoli administracyjnej folder Zarządzanie urządzeniami mobilnymi.

Znane problemy podczas instalowania aplikacji

- Kaspersky Endpoint Security for Android jest instalowany tylko w pamięci głównej urządzenia.
- Na urządzeniach działających pod kontrolą systemu Android 7.0, podczas prób wyłączenia uprawnień administratora dla Kaspersky Endpoint Security for Android w ustawieniach urządzenia może wystąpić błąd, jeśli dla Kaspersky Endpoint Security for Android nie zezwolono na wyświetlanie nad innymi aplikacjami. Ten problem jest spowodowany przez znany błąd w Android 7.
- Kaspersky Endpoint Security for Android zainstalowany na urządzeniach działających pod kontrolą systemu Android 7.0 lub nowszego nie obsługuje trybu wielu okien.
- Kaspersky Endpoint Security for Android nie działa na urządzeniach Chromebook z systemem operacyjnym Chrome.
- Kaspersky Endpoint Security for Android nie działa na urządzeniach z systemami operacyjnymi Android (Go edition).
- Podczas korzystania z aplikacji Kaspersky Endpoint Security for Android z systemami EMM innych producentów (na przykład VMWare AirWatch) dostępne są tylko składniki Antywirus i Ochrona WWW. Administrator może skonfigurować ustawienia Antywirusa i Ochrony WWW w konsoli systemu EMM. W takim przypadku powiadomienia o działaniu aplikacji są dostępne tylko w interfejsie aplikacji Kaspersky Endpoint Security for Android (Raporty).

Znane problemy podczas aktualizacji wersji aplikacji

- Możesz uaktualnić Kaspersky Endpoint Security for Androida tylko do najnowszej wersji aplikacji. Kaspersky Endpoint Security for Android nie może zostać zmieniony na starszą wersję.

Znane problemy z działaniem antywirusa

- Ze względu na ograniczenia techniczne, Kaspersky Endpoint Security for Android nie może skanować plików o rozmiarze 2 GB lub większym. Podczas skanowania aplikacja pomija takie pliki bez informowania o tym fakcie.
- W celu dodatkowej analizy urządzenia pod kątem nowych zagrożeń, których informacje nie zostały jeszcze dodane do antywirusowych baz danych, należy włączyć korzystanie z Kaspersky Security Network. *Kaspersky Security Network (KSN)* jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Aby korzystać z KSN, urządzenie mobilne musi być połączone z internetem.
- W niektórych przypadkach aktualizacja antywirusowych baz danych z Serwera administracyjnego na urządzeniu mobilnym może się nie powieść. W takim przypadku uruchom zadanie aktualizacji antywirusowych baz danych na Serwerze administracyjnym.
- Na niektórych urządzeniach Kaspersky Endpoint Security for Android nie wykrywa urządzeń podłączonych przez USB OTG. Nie jest możliwe uruchomienie skanowania antywirusowego na takich urządzeniach.
- Na urządzeniach z Androidem 11.0 lub nowszym użytkownik musi przyznać uprawnienie "Zezwól na dostęp do zarządzania wszystkimi plikami".
- W przypadku urządzeń działających pod kontrolą systemu Android 7.0 lub nowszego, okno konfiguracji terminarza uruchamiania skanowania antywirusowego może być wyświetlane niepoprawnie (elementy zarządzania nie są wyświetlane). Ten problem jest spowodowany przez znany błąd w Android 7.
- Na urządzeniach z systemem Android 7.0 ochrona w czasie rzeczywistym w trybie rozszerzonym nie wykrywa zagrożeń w plikach przechowywanych na zewnętrznej karcie SD.
- Na urządzeniach działających pod kontrolą systemu Android 6.0, Kaspersky Endpoint Security for Android nie wykrywa pobierania szkodliwego pliku do pamięci urządzenia. Szkodliwy plik może zostać wykryty przez Antywirusa w momencie uruchomienia pliku lub podczas skanowania antywirusowego urządzenia. Ten problem jest spowodowany przez znany błąd w Android 6.0. Aby zapewnić ochronę urządzenia, zalecane jest skonfigurowane zaplanowanych skanowań antywirusowych.

Znane problemy w działaniu ochrony WWW

- Ochrona WWW na urządzeniach z systemem Android działa tylko w przeglądarkach: Huawei Browser, Google Chrome (włączając funkcję Kart niestandardowych) i Samsung Internet Browser.
- Aby Ochrona WWW działała, musisz włączyć korzystanie z Kaspersky Security Network. Ochrona WWW blokuje strony internetowe na podstawie danych KSN dotyczących reputacji i kategorii stron internetowych.
- Zabronione strony internetowe mogą zostać odblokowane przez Ochronę WWW na urządzeniach z systemem Android 6.0 z zainstalowaną wersją Google Chrome 51 (lub starszą wersją), jeśli witryna jest otwierana w następujący sposób (przyczyną problemu jest dobrze znana wada w Google Chrome):
  - Z wyników wyszukiwania.
  - Z listy zakładek.
  - Z historii wyszukiwania.
  - Przy użyciu funkcji automatycznego uzupełniania adresu internetowego.
  - Poprzez otwarcie strony internetowej na nowej karcie w Google Chrome.

- Zabronione strony internetowe mogą pozostać odblokowane w przeglądarce Google Chrome w wersji 50 (lub dowolnej wcześniejszej), jeśli witryna zostanie otwarta z wyników wyszukiwania Google, gdy w ustawieniach przeglądarki włączono funkcję **Połącz karty i aplikacje**. Ten problem jest spowodowany przez znany błąd w Google Chrome.

- Strony internetowe należące do zablokowanych kategorii mogą pozostać odblokowane w Google Chrome, jeśli użytkownik otworzy je z aplikacji innych firm, na przykład, z aplikacji klienta IM. Ten problem jest związany z działaniem usługi dostępności z funkcją Kart niestandardowych w Chrome.

- Zabronione strony internetowe mogą pozostać odblokowane w przeglądarce internetowej Samsung Internet Browser, jeśli użytkownik otworzy je w tle z poziomu menu kontekstowego lub z poziomu aplikacji innych firm, na przykład, z aplikacji klienta IM.

- Kaspersky Endpoint Security for Android musi być ustawiony jako usługa Ułatwień dostępu w celu zapewnienia poprawnego działania Ochrony WWW.

- Dozwolone strony internetowe mogą być blokowane w przeglądarce Samsung Internet Browser, w trybie Ochrony WWW o nazwie **Dozwolone są jedynie strony internetowe znajdujące się na liście** po odświeżeniu strony. Strony internetowe są blokowane, jeśli wyrażenie regularne zawiera ustawienia zaawansowane (na przykład `^https?:\/\/example\.com\/pictures\/`). Zalecane jest stosowanie wyrażeń regularnych bez dodatkowych ustawień (na przykład `^https?:\/\/example\.com`).

Znane problemy w działaniu funkcji Anti-Theft

- W celu terminowego dostarczania poleceń na urządzenia z systemem Android aplikacja korzysta z usługi Firebase Cloud Messaging (FCM). Jeśli usługa FCM nie jest skonfigurowana, polecenia będą dostarczane do urządzenia tylko podczas synchronizacji z Kaspersky Security Center zgodnie z terminarzem zdefiniowanym w zasadzie, na przykład, co 24 godziny.

- Aby zablokować urządzenie, Kaspersky Endpoint Security for Android musi być ustawiony jako administrator urządzenia.

- Aby zablokować urządzenia z systemem Android 7.0 lub nowszym, Kaspersky Endpoint Security for Android musi być ustawiony jako funkcja dostępności.

- Na niektórych urządzeniach polecenie Anti-Theft może się nie uruchomić, jeśli tryb Oszczędzania baterii jest włączony na urządzeniu. Ten problem został potwierdzony na urządzeniu Alcatel 5080X.

- Aby zlokalizować urządzenia działające pod kontrolą systemu Android 10.0 lub nowszego użytkownik musi nadać uprawnienie "Cały czas".

Znane problemy w działaniu Kontroli aplikacji

- Kaspersky Endpoint Security for Android musi być ustawiony jako usługa Ułatwień dostępu w celu zapewnienia poprawnego działania Kontroli aplikacji.

- Aby Kontrola aplikacji (kategorie aplikacji) działała, musisz włączyć korzystanie z Kaspersky Security Network. Kontrola aplikacji określa kategorię aplikacji na podstawie danych dostępnych w KSN. Aby korzystać z KSN, urządzenie mobilne musi być połączone z internetem. W Kontroli aplikacji możesz dodawać pojedyncze aplikacje do list zablokowanych i dozwolonych aplikacji. W takim przypadku KSN nie jest wymagany.

- Podczas konfigurowania Kontroli aplikacji zalecane jest odznaczenie pola **Blokuj aplikacje systemowe**. Blokowanie aplikacji systemowych może powodować problemy z działaniem urządzenia.

Znane problemy podczas konfigurowania mocy hasła odblokowującego urządzenie

- Na urządzeniach z Androidem 10.0 lub nowszym Kaspersky Endpoint Security przetwarza wymagania dotyczące mocy hasła na jedną z wartości systemowych: średnią lub wysoką.

  Jeśli wymagana długość hasła wynosi od 1 do 4 symboli, aplikacja prosi użytkownika o ustawienie hasła o średniej mocy. Musi być numeryczne (PIN) bez powtarzających się lub uporządkowanych (np. 1234) sekwencji lub alfanumeryczne. Kod PIN lub hasło musi mieć co najmniej 4 znaki.

  Jeśli wymagana długość hasła to 5 lub więcej symboli, aplikacja prosi użytkownika o ustawienie silnego hasła. Musi być numeryczne (PIN) bez powtarzających się lub uporządkowanych sekwencji lub alfanumeryczne (hasło). Kod PIN musi mieć co najmniej 8 cyfr; hasło musi mieć co najmniej 6 znaków.

- Jeśli na urządzeniach działających pod kontrolą systemu Android 7.1.1 hasło odblokowujące nie spełnia firmowych wymagań bezpieczeństwa (Kontrola zgodności), aplikacja systemowa Ustawienia może działać niepoprawnie, gdy zostanie podjęta próba zmiany hasła odblokowującego z poziomu Kaspersky Endpoint Security for Android. Ten problem jest spowodowany przez znany błąd w Android 7.1.1. W tym przypadku, aby zmienić hasło odblokowujące, użyj tylko aplikacji systemowej Ustawienia.

- Na niektórych urządzeniach działających pod kontrolą systemu Android 6.0 lub nowszego może wystąpić błąd podczas wprowadzania hasła odblokowującego ekran, gdy dane na urządzeniu są zaszyfrowane. Ten problem dotyczy określonych funkcji usługi dostępności z oprogramowaniem fabrycznym MIUI.

Znane problemy z ochroną dezinstalacji aplikacji

- Kaspersky Endpoint Security for Android musi być ustawiony jako administrator urządzenia.

- Aby chronić aplikację przed usunięciem na urządzeniach działających pod kontrolą systemu Android 7.0 lub nowszego, Kaspersky Endpoint Security for Android musi być ustawiony jako usługa funkcji Dostępności.

- Na niektórych urządzeniach Xiaomi i Huawei, ochrona przed usunięciem Kaspersky Endpoint Security for Android nie działa. Ten problem jest spowodowany przez specyficzne funkcje oprogramowania fabrycznego MIUI 7 i 8 na urządzeniach Xiaomi i oprogramowania fabrycznego EMUI na urządzeniach Huawei.

Znane problemy podczas konfigurowania ograniczeń urządzenia

- Na urządzeniach z Androidem 10.0 lub nowszym blokowanie korzystania z sieci Wi-Fi nie jest obsługiwane.

- Na urządzeniach z systemem Android 10.0 lub nowszym nie można całkowicie zabronić korzystania z aparatu.

- Na urządzeniach działających pod kontrolą systemu Android 11 lub nowszego, Kaspersky Endpoint Security for Android musi być ustawiony jako funkcja ułatwień dostępu. Kaspersky Endpoint Security for Android wyświetli pytanie o ustawienie aplikacji jako usługę funkcji Dostępności poprzez Kreator wstępnej konfiguracji. Użytkownik może pominąć ten krok lub wyłączyć tę usługę w ustawieniach urządzenia w późniejszym czasie. W takim przypadku nie będzie można ograniczyć korzystania z aparatu.

Znane problemy podczas wysyłania poleceń na urządzenia mobilne

- Na urządzeniach z systemem Android 12 lub nowszym, jeśli użytkownik przyznał uprawnienie "Użyj przybliżonej lokalizacji", aplikacja Kaspersky Endpoint Security for Android najpierw spróbuje uzyskać dokładną lokalizację urządzenia. Jeśli to się nie powiedzie, przybliżona lokalizacja urządzenia zostanie zwrócona tylko wtedy, gdy została odebrana nie więcej niż 30 minut wcześniej. W przeciwnym razie polecenie **Zlokalizuj urządzenie** nie powiedzie się.

Znane problemy z określonymi urządzeniami

- Na niektórych urządzeniach (na przykład Huawei, Meizu i Xiaomi) konieczne jest przyznanie aplikacji Kaspersky Endpoint Security for Android uprawnienia do autostartu lub ręczne dodanie jej do listy aplikacji uruchamianych w momencie uruchamiania systemu operacyjnego. Jeśli aplikacja nie została dodana do listy, Kaspersky Endpoint Security for Android przestaje wykonywać wszystkie swoje funkcje po ponownym uruchomieniu urządzenia mobilnego. Ponadto, jeśli urządzenie zostało zablokowane, nie można użyć polecenia odblokowania urządzenia. Możesz odblokować urządzenie tylko za pomocą jednorazowego kodu odblokowującego.

- Na niektórych urządzeniach (na przykład Meizu i Asus) z Androidem 6.0 lub nowszym, po zaszyfrowaniu danych i ponownym uruchomieniu urządzenia z systemem Android, musisz wprowadzić hasło numeryczne, aby odblokować urządzenie. Jeśli użytkownik używa hasła graficznego do odblokowania urządzenia, należy przekonwertować hasło graficzne na hasło numeryczne. Więcej informacji na temat konwertowania wzoru na hasło numeryczne można znaleźć na stronie działu pomocy technicznej producenta urządzenia mobilnego. Ten problem jest związany z działaniem usługi Ułatwień dostępu.

- Na niektórych urządzeniach Huawei z systemem Android 5.X, po ustawieniu Kaspersky Endpoint Security for Android jako funkcji dostępności może pojawić się niepoprawny komunikat o braku odpowiednich uprawnień. Aby ukryć ten komunikat, włącz aplikację jako aplikację chronioną w ustawieniach urządzenia.

- Na niektórych urządzeniach Huawei z Androidem 5.X lub 6.X, gdy tryb Oszczędzania baterii jest włączony dla Kaspersky Endpoint Security for Android, użytkownik może ręcznie zakończyć aplikację. Urządzenie użytkownika nie będzie już jednak chronione. Ten problem jest spowodowany działaniem niektórych funkcji oprogramowania Huawei. Aby przywrócić ochronę urządzenia, ręcznie uruchom Kaspersky Endpoint Security for Android. Zalecane jest wyłączenie trybu oszczędzania baterii dla Kaspersky Endpoint Security for Android w ustawieniach urządzenia.

- Na urządzeniach Huawei z oprogramowaniem fabrycznym EMUI z systemem Android 7.0 użytkownik może ukryć powiadomienie dotyczące stanu ochrony Kaspersky Endpoint Security for Android. Ten problem jest spowodowany działaniem niektórych funkcji oprogramowania Huawei.

- Na niektórych urządzeniach Xiaomi, podczas ustawiania długości hasła na więcej niż 5 znaków w zasadzie, użytkownik zostanie poproszony o zmianę hasła odblokowania ekranu zamiast kodu PIN. Nie można ustawić kodu PIN, który ma więcej niż 5 znaków. Ten problem jest spowodowany działaniem niektórych funkcji oprogramowania Xiaomi.

- Na urządzeniach Xiaomi z oprogramowaniem fabrycznym MIUI działającym pod kontrolą systemu Android 6.0, ikona programu Kaspersky Endpoint Security for Android może zostać ukryta na pasku stanu. Ten problem jest spowodowany działaniem niektórych funkcji oprogramowania Xiaomi. Zaleca się zezwolenie na wyświetlanie ikon powiadomień w ustawieniach powiadomień.

- Na niektórych urządzeniach Nexus z systemem Android 6.0.1 nie można nadać uprawnień niezbędnych do poprawnego działania z poziomu kreatora wstępnej konfiguracji programu Kaspersky Endpoint Security for Android. Ten problem jest spowodowany przez dobrze znaną wadę poprawki zabezpieczeń dla Androida firmy Google. Aby zapewnić poprawne działanie, wymagane uprawnienia muszą zostać przyznane ręcznie w ustawieniach urządzenia.

- Na pewnych urządzeniach Samsung działających pod kontrolą systemu Android 7.0 lub nowszego, jeśli użytkownik spróbuje skonfigurować nieobsługiwane metody odblokowania urządzenia (na przykład, wzór), urządzenie może zostać zablokowane, gdy spełnione będą następujące warunki: włączona jest ochrona przed dezinstalacją Kaspersky Endpoint Security for Android oraz ustawione są wymagania wobec siły hasła odblokowującego ekran. Aby odblokować urządzenie, należy wysłać specjalne polecenie na urządzenie.

- Na niektórych urządzeniach Samsung niemożliwe jest zablokowanie użycia odcisku palca do odblokowania urządzenia.

- Ochrona WWW nie może zostać włączona na niektórych urządzeniach Samsung, jeśli urządzenie jest połączone z siecią 3G/4G, posiada włączony tryb oszczędzania baterii i ogranicza zużycie danych w tle. Zaleca się

wyłączenie funkcji ograniczającej procesy w tle w ustawieniach oszczędzania baterii.

- Na niektórych urządzeniach Samsung, jeśli hasło odblokowujące nie jest zgodne z firmowymi wymaganiami bezpieczeństwa, Kaspersky Endpoint Security for Android nie blokuje użycia odcisku palca do odblokowania ekranu.

- Na niektórych urządzeniach Honor i Huawei nie można ograniczyć korzystania z Bluetooth. Jeśli Kaspersky Endpoint Security for Android spróbuje ograniczyć korzystanie z Bluetooth, system operacyjny wyświetli powiadomienie zawierające opcje odrzucenia lub zezwolenia na to ograniczenie. Użytkownik może odrzucić to ograniczenie i kontynuować korzystanie z Bluetooth.

- Na urządzeniach Blackview użytkownik może wyczyścić pamięć aplikacji Kaspersky Endpoint Security for Android. W rezultacie ochrona i zarządzanie urządzeniem są wyłączone, wszystkie zdefiniowane ustawienia stają się nieskuteczne, a aplikacja Kaspersky Endpoint Security for Android zostaje usunięta z funkcji ułatwień dostępu. Dzieje się tak, ponieważ urządzenia tego dostawcy zapewniają dostosowaną aplikację Ostatnie ekrany z podwyższonymi uprawnieniami. Ta aplikacja może nadpisać ustawienia Kaspersky Endpoint Security for Android i nie można jej zastąpić, ponieważ jest częścią systemu operacyjnego Android.

- Na niektórych urządzeniach z systemem Android 11 aplikacja Kaspersky Endpoint Security for Android ulega awarii natychmiast po uruchomieniu. Ten problem jest spowodowany przez znany błąd w Android 11.

Wdrażanie rozwiązania do zarządzania urządzeniami mobilnymi w Kaspersky Security Center Web Console lub Cloud Console

Aby zarządzać urządzeniami mobilnymi przy użyciu Kaspersky Security Center Web Console lub Cloud Console, musisz wdrożyć rozwiązanie do zarządzania urządzeniami mobilnymi.

Scenariusze wdrożenia

Instalacja w Kaspersky Security Center Web Console

Instalacja rozwiązania do zarządzania urządzeniami mobilnymi w Kaspersky Security Center Web Console składa się z następujących kroków:

1. Przygotowywanie Kaspersky Security Center Web Console do instalacji
2. Instalowanie wtyczek zarządzających
3. Wdrażania aplikacji mobilnej
4. (Opcjonalnie, wyłacznie dla urządzeń z systemem Android) Konfigurowanie wymiany informacji z Firebase Cloud Messaging

   Zaleca się wykonanie tego kroku, aby zapewnić terminowe dostarczanie poleceń na urządzenia mobilne i wymuszoną synchronizację w przypadku zmiany ustawień zasad.

Instalacja w Kaspersky Security Center Cloud Console

Wdrożenie rozwiązania do zarządzania urządzeniami mobilnymi w Kaspersky Security Center Cloud Console składa się z następujących kroków:

1. Przygotowywanie Kaspersky Security Center Cloud Console do instalacji
2. Wdrażania aplikacji mobilnej
3. (Opcjonalnie, wyłacznie dla urządzeń z systemem Android) Konfigurowanie wymiany informacji z Firebase Cloud Messaging

   Zaleca się wykonanie tego kroku, aby zapewnić terminowe dostarczanie poleceń na urządzenia mobilne i wymuszoną synchronizację w przypadku zmiany ustawień zasad.

Przygotowanie Kaspersky Security Center Web Console i Cloud Console do instalacji

Ta sekcja zawiera instrukcje dotyczące przygotowania Kaspersky Security Center Web Console i Cloud Console do instalacji.

Konfigurowanie Serwera administracyjnego dla podłączenia urządzeń mobilnych

Aby urządzenia mobilne mogły łączyć się z Serwerem administracyjnym, musisz zdefiniować ustawienia połączenia urządzenia mobilnego we właściwościach Serwera administracyjnego przed zainstalowaniem aplikacji Kaspersky Endpoint Security for Android lub Kaspersky Security for iOS na urządzeniach mobilnych.

W celu zdefiniowania ustawień Serwera administracyjnego dla połączenia urządzenia mobilnego:

1. Uruchom zarządzanie urządzeniami mobilnymi na Serwerze administracyjnym.

   Zarządzanie urządzeniami mobilnymi można uruchomić podczas wstępnej konfiguracji Konsoli administracyjnej opartej na MMC programu Kaspersky Security Center (podczas działania Kreatora wstępnej konfiguracji) lub później, wyświetlając w Konsoli administracyjnej folder Zarządzanie urządzeniami mobilnymi.

2. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, kliknij **Ustawienia** ( ).

   Zostanie otwarte okno właściwości Serwera administracyjnego.

3. Skonfiguruj porty Serwera administracyjnego, które będą używane przez urządzenia mobilne:

   a. Wybierz sekcję **Dodatkowe porty**.

   b. Włącz przełącznik **Otwórz port dla urządzeń mobilnych**.

   c. W polu **Port do synchronizacji urządzeń mobilnych** określ port, poprzez który urządzenia mobilne nawiążą połączenie z Serwerem administracyjnym.

      Domyślnie używany jest port 13292.

      Jeśli przełącznik **Otwórz port dla urządzeń mobilnych** jest wyłączony lub określono nieprawidłowy port połączenia, urządzenia mobilne nie będą mogły nawiązać połączenia z Serwerem administracyjnym.

d. W polu **Port do aktywacji urządzenia mobilnego** określ port, który będzie używany przez urządzenia mobilne do nawiązania połączenia z Serwerem administracyjnym w celu aktywacji aplikacji mobilnej.

Domyślnie używany jest port 13292.

Jeśli określisz nieprawidłowy port połączenia, użytkownicy urządzeń mobilnych nie będą mogli aktywować aplikacji przy użyciu Serwera administracyjnego.

4. W razie potrzeby edytuj certyfikat, który będzie używany przez urządzenia mobilne do łączenia się z Serwerem administracyjnym.

Domyślnie Serwer administracyjny używa certyfikatu utworzonego podczas instalacji Serwera administracyjnego. Jeśli chcesz, zastąp certyfikat wydany przez Serwer administracyjny innym certyfikatem lub ponownie wystaw certyfikat wydany przez Serwer administracyjny.

Aby edytować certyfikat*:*

a. Wybierz sekcję **Certyfikaty**.

b. Zdefiniuj wymagane ustawienia.

Aby uzyskać szczegółowe informacje na temat certyfikatów, zapoznaj się z *Pomocą Kaspersky Security Center*.

5. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w ustawieniach i zamknąć okno właściwości Serwera administracyjnego.

Po skonfigurowaniu ustawień połączenia urządzenia mobilnego możesz zainstalować aplikację Kaspersky Endpoint Security for Android lub Kaspersky Security for iOS na urządzeniach mobilnych i połączyć je z Serwerem administracyjnym przy użyciu określonych ustawień.

Tworzenie grupy administracyjnej

Zasady grupy służą do przeprowadzania scentralizowanej konfiguracji aplikacji Kaspersky Endpoint Security for Android i Kaspersky Security for iOS zainstalowanych na urządzeniach mobilnych użytkowników.

Aby zastosować zasadę do grupy urządzeń, przed zainstalowaniem aplikacji mobilnych na urządzeniach użytkowników zalecane jest utworzenie oddzielnej grupy dla tych urządzeń w folderze **Zarządzane urządzenia**.

Po utworzeniu grupy administracyjnej zalecane jest skonfigurowanie opcji automatycznego przydzielania do tej grupy urządzeń, na których chcesz zainstalować aplikacje. Następnie skonfiguruj ustawienia, które są typowe dla wszystkich urządzeń, korzystając z zasad grupy.

W celu utworzenia grupy administracyjnej:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console wybierz **URZĄDZENIA** > **HIERARCHIA GRUP**.

2. W strukturze grupy administracyjnej wybierz grupę administracyjną, która ma zawierać nową grupę administracyjną.

3. Kliknij przycisk **Dodaj**.

4. W otwartym oknie **Nazwa nowej grupy administracyjnej** wprowadź nazwę grupy, a następnie kliknij przycisk **Dodaj**.

W hierarchii grup administracyjnych pojawi się nowa grupa administracyjna o określonej nazwie.

Tworzenie reguły automatycznego przydzielania urządzenia do grup administracyjnych

Gdy aplikacja Kaspersky Endpoint Security for Android lub Kaspersky Security for iOS jest zainstalowana na urządzeniach mobilnych, są one wyświetlane na stronie **WYKRYWANIE I WDRAŻANIE** > **NIEPRZYPISANE URZĄDZENIA** w Kaspersky Security Center Web Console lub Cloud Console. Aby zarządzać nowo podłączonymi urządzeniami, możesz ręcznie przenieść je do grupy administracyjnej lub utworzyć regułę automatycznego przydzielania ich do grup administracyjnych.

Aby utworzyć regułę automatycznego przydzielania urządzeń mobilnych do grup administracyjnych:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console wybierz **WYKRYWANIE I WDRAŻANIE** > **WDRAŻANIE I PRZYPISANIE** > **REGUŁY PRZENOSZENIA**.
2. W otwartym oknie **Nowa reguła** kliknij przycisk **Dodaj**.
3. W polu **Nazwa reguły** określ nazwę reguły.
4. W polu **Grupa administracyjna** wybierz grupę administracyjną, do której zostaną przydzielone urządzenia mobilne po zainstalowaniu na nich aplikacji.
5. W sekcji **Zastosuj regułę** wybierz **Uruchom raz dla każdego urządzenia**.
6. Zaznacz pole **Przenieś tylko urządzenia, które nie są dodane do grupy administracyjnej**, aby zapobiec przenoszeniu urządzeń mobilnych przydzielonych do innych grup administracyjnych podczas stosowania reguły.
7. Zaznacz pole **Włącz regułę**, aby zastosować regułę natychmiast po jej utworzeniu.

   Regułę możesz włączyć w dowolnym momencie później, używając przycisku przełączania na stronie **REGUŁY PRZENOSZENIA**.
8. Wybierz **WARUNKI REGUŁY** > **Aplikacje** i wykonaj następujące czynności:

   a. Włącz przycisk przełącznika **Wersja systemu operacyjnego**.

   b. Z listy systemów operacyjnych, która się otworzy, wybierz **Android** lub **iOS**.

   Reguła zostanie zastosowana na odpowiednich urządzeniach. Aby utworzyć regułę, musisz określić co najmniej jeden warunek.
9. Kliknij **Zapisz**, aby utworzyć regułę.

Nowo utworzona reguła jest wyświetlana na stronie **REGUŁY PRZENOSZENIA**. Zgodnie z tą regułą Kaspersky Security Center przydzieli wszystkie nowo podłączone urządzenia do wybranej grupy administracyjnej.

Szczegółowe informacje o zarządzaniu grupami administracyjnymi i akcjach na nieprzypisanych urządzeniach:

- Jeśli korzystasz z Kaspersky Security Center Web Console, zapoznaj się z *Pomocą Kaspersky Security Center*.
- Jeśli korzystasz z Kaspersky Security Center Cloud Console, zapoznaj się z *Pomocą Kaspersky Security Center Cloud Console*.

Instalowanie wtyczek zarządzających

Aby zarządzać urządzeniami mobilnymi w Kaspersky Security Center Web Console, należy zainstalować następujące wtyczki administracyjne:

- Wtyczka Kaspersky Security for Mobile (Devices)
- Wtyczka Kaspersky Security for Mobile (Policies)

> Jeśli korzystasz z Kaspersky Security Center Cloud Console, nie musisz instalować wtyczek administracyjnych. Wystarczy utworzyć konto w Kaspersky Security Center Cloud Console. Więcej informacji na temat tworzenia konta znajdziesz w pomocy *Kaspersky Security Center Cloud Console*.

Aby zainstalować wtyczki administracyjne, możesz skorzystać z następujących metod:

- Poprzez użycie Kreatora szybkiego uruchamiania Kaspersky Security Center Web Console.

  Kaspersky Security Center Web Console automatycznie wyświetli pytanie o uruchomienie Kreatora wstępnej konfiguracji po zainstalowaniu Serwera administracyjnego, przy pierwszym nawiązaniu połączenia z nim. Możesz także ręcznie uruchomić Kreator wstępnej konfiguracji w dowolnym momencie.

  Więcej informacji dotyczących Kreatora wstępnej konfiguracji dla Kaspersky Security Center można znaleźć w *Pomocy do Kaspersky Security Center*.

- Poprzez użycie listy dostępnych pakietów dystrybucyjnych w Kaspersky Security Center Web Console.

  Lista dostępnych pakietów dystrybucyjnych jest aktualizowana automatycznie po opublikowaniu nowych wersji aplikacji firmy Kaspersky.

- Pobierz pakiety dystrybucyjne z zewnętrznego źródła i dodaj wtyczki administracyjne do Kaspersky Security Center Web Console.

  Na przykład pakiety dystrybucyjne wtyczek administracyjnych można pobrać ze strony internetowej Kaspersky.

Instalowanie wtyczek administracyjnych z listy dostępnych pakietów dystrybucyjnych

W celu zainstalowania wtyczek zarządzających:

1. W oknie głównym Kaspersky Security Center Web Console wybierz **USTAWIENIA KONSOLI** > **WTYCZKI SIECIOWE**.
2. Kliknij przycisk **Dodaj**.

   Spowoduje to otwarcie listy aktualnych wersji aplikacji firmy Kaspersky.
3. Zainstaluj wtyczki administracyjne:

   a. Na liście dostępnych aplikacji kliknij sekcję **Urządzenia mobilne**, aby ją rozwinąć.

   b. Wybierz wtyczkę **Kaspersky Security for Mobile (Devices)**, a następnie kliknij **Zainstaluj wtyczkę**.

   c. Wybierz wtyczkę **Kaspersky Security for Mobile (Policies)**, a następnie kliknij **Zainstaluj wtyczkę**.

Pakiety dystrybucyjne zostaną pobrane, a wtyczki zainstalowane. Po zainstalowaniu każdej wtyczki i dodaniu jej do Kaspersky Security Center Web Console wyświetlane jest okno potwierdzenia.

Instalowanie wtyczek zarządzających z pakietu dystrybucyjnego

Pakiet dystrybucyjny możesz pobrać ze strony internetowej Kaspersky.

W celu zainstalowania wtyczki Kaspersky Security for Mobile (Devices) z pakietu dystrybucyjnego:

1. Skopiuj pliki `plugin.zip` i `signature.txt` z archiwum pakietu dystrybucyjnego `on_prem_ksm_devices_xx.x.x.x.zip` na stację roboczą administratora.
2. W oknie głównym Kaspersky Security Center Web Console wybierz **USTAWIENIA KONSOLI** > **WTYCZKI SIECIOWE**.
3. Kliknij **Dodaj z pliku**.
4. W otwartym oknie **Dodaj z pliku** kliknij **Prześlij plik ZIP**, a następnie wyszukaj plik `plugin.zip`.
5. Kliknij **Prześlij podpis**, a następnie wyszukaj plik `signature.txt`.
6. Kliknij przycisk **Dodaj**.

Wtyczka Kaspersky Security for Mobile (Devices) jest instalowana i dodawana do Kaspersky Security Center Web Console.

W celu zainstalowania wtyczki Kaspersky Security for Mobile (Policies) z pakietu dystrybucyjnego:

1. Skopiuj pliki `plugin.zip` i `signature.txt` z archiwum pakietu dystrybucyjnego `on_prem_ksm_policies_xx.x.x.x.zip` na stację roboczą administratora.
2. W oknie głównym Kaspersky Security Center Web Console wybierz **USTAWIENIA KONSOLI** > **WTYCZKI SIECIOWE**.
3. Kliknij **Dodaj z pliku**.
4. W otwartym oknie **Dodaj z pliku** kliknij **Prześlij plik ZIP**, a następnie wyszukaj plik `plugin.zip`.
5. Kliknij **Prześlij podpis**, a następnie wyszukaj plik `signature.txt`.
6. Kliknij przycisk **Dodaj**.

Wtyczka Kaspersky Security for Mobile (Policies) jest instalowana i dodawana do Kaspersky Security Center Web Console.

Możesz upewnić się, że wtyczki administracyjne zostały zainstalowane, przeglądając listę zainstalowanych wtyczek na stronie **USTAWIENIA KONSOLI** > **WTYCZKI SIECIOWE**.

Wdrażania aplikacji mobilnej

Aby zarządzać urządzeniami mobilnymi poprzez Kaspersky Security Center Web Console lub Cloud Console, musisz wdrożyć aplikację Kaspersky Endpoint Security for Android lub Kaspersky Security for iOS na urządzeniach mobilnych. Aplikacje możesz wdrażać na urządzeniach mobilnych za pomocą Kaspersky Security Center Web Console lub Cloud Console.

Wdrażanie aplikacji mobilnej za pomocą Kaspersky Security Center Web Console lub Cloud Console.

Aplikacja mobilna jest wdrażana na urządzeniach mobilnych użytkowników, których konta zostały dodane do Kaspersky Security Center. Aby uzyskać więcej informacji o kontach użytkowników w Kaspersky Security Center:

- Jeśli korzystasz z Kaspersky Security Center Web Console, zapoznaj się z *Pomocą Kaspersky Security Center*.
- Jeśli korzystasz z Kaspersky Security Center Cloud Console, zapoznaj się z *Pomocą Kaspersky Security Center Cloud Console*.

Możesz użyć wtyczki Kaspersky Security for Mobile (Devices), aby zainstalować aplikację z Kaspersky Security Center Web Console lub Cloud Console, wysyłając link instalacyjny na urządzenie mobilne.

- Na urządzeniu z systemem Android użytkownik otrzymuje link Google Play do pobrania aplikacji Kaspersky Endpoint Security for Android. Aplikacja może zostać zainstalowana zgodnie ze standardową procedurą instalacji na platformie Android. Po zainstalowaniu aplikacji użytkownik musi zapewnić wymagane uprawnienia.

  Niektóre urządzenia Huawei i Honor nie mają usług Google, a zatem nie mają dostępu do aplikacji w Google Play. Jeśli niektórzy użytkownicy urządzeń Huawei i Honor nie mogą zainstalować aplikacji z Google Play, powinni otrzymać propozycję zainstalowania aplikacji z Huawei App Gallery.

- Na urządzeniu iOS użytkownik otrzymuje link do App Store do pobrania aplikacji Kaspersky Security for iOS. Aplikacja może zostać zainstalowana zgodnie ze standardową procedurą instalacji na platformie iOS.

  Przed połączeniem urządzenia z systemem iOS wyślij adres Kaspersky Security Center na urządzenie użytkownika w celu poprawy bezpieczeństwa połączenia. Użytkownik zobaczy ten adres w trakcie instalacji aplikacji i będzie mógł anulować połączenie, jeśli wyświetlony adres nie będzie taki sam jak wysłany przez Ciebie adres.

Odnośnik zawiera następujące dane:

- Ustawienia synchronizacji Kaspersky Security Center
- Certyfikat ogólny

Aby wdrożyć aplikację na urządzeniu mobilnym:

1. Uruchom Kreatora podłączania urządzenia mobilnego:
   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**, a następnie kliknij **Dodaj**.
   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console wybierz **UŻYTKOWNICY I ROLE** > **UŻYTKOWNICY**. Kliknij nazwę użytkownika lub grupy użytkowników, do której chcesz wysłać

odnośnik umożliwiający podłączenie urządzenia mobilnego, a następnie wybierz **URZĄDZENIA.** Kliknij **Dodaj urządzenie mobilne**. W tym przypadku pomiń krok 3.

Kontynuuj pracę Kreatora, używając przycisku **Dalej.**

2. Wybierz system operacyjny urządzeń, które chcesz dodać:

   - **Android**
   - **iOS i iPadOS**

3. Wybierz użytkowników i grupy użytkowników, do których chcesz wysłać link do podłączenia urządzenia mobilnego.

4. Wybierz adresy e-mail, na jakie wysłać link:

   - **Wszystkie adresy e-mail**
   - **Główny adres e-mail**
   - **Alternatywny adres e-mail**
   - **Inny adres e-mail**

     Jeśli wybierzesz tę opcję, podaj poniżej adres e-mail.

5. Wyświetlone zostanie podsumowanie odnośnika.

   Upewnij się, że wszystkie parametry linku są poprawne, a następnie kliknij **Wyślij**.

6. Otworzy się okno z potwierdzeniem wysłania odnośnika do dodania urządzenia mobilnego.

   Kliknij **OK**, aby zakończyć działania Kreatora.

Kiedy użytkownik instaluje aplikację Kaspersky Endpoint Security for Android lub Kaspersky Security for iOS, jego urządzenie zostanie wyświetlone na zakładce **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA** w Web Console lub Cloud Console. Po zainstalowaniu aplikacji na urządzeniach mobilnych użytkowników, możliwa będzie konfiguracja ustawień urządzeń i aplikacji za pomocą zasad grup. Możliwe będzie także wysłanie poleceń na urządzenia mobilne (wyłącznie dla urządzeń z systemem Android) w celu ochrony danych w przypadku, gdy urządzenia zostaną zagubione bądź skradzione.

Aktywowanie aplikacji mobilnej

W Kaspersky Security Center licencja może obejmować różne grupy funkcji. Aby mieć pewność, że aplikacja Kaspersky Endpoint Security for Android oraz Kaspersky Security for iOS jest w pełni funkcjonalna, licencja dla Kaspersky Security Center zakupiona przez organizację musi oferować funkcję **Zarządzanie urządzeniami mobilnymi**. Funkcja **Zarządzanie urządzeniami mobilnymi** jest przeznaczona do łączenia urządzeń mobilnych z Kaspersky Security Center i zarządzania nimi.

Aby uzyskać szczegółowe informacje na temat licencjonowania Kaspersky Security Center i opcji licencjonowania:

- Jeśli korzystasz z Kaspersky Security Center Web Console, zapoznaj się z *Pomocą Kaspersky Security Center*.
- Jeśli korzystasz z Kaspersky Security Center Cloud Console, zapoznaj się z *Pomocą Kaspersky Security Center Cloud Console*.

Aktywacja aplikacji Kaspersky Endpoint Security for Android lub Kaspersky Security for iOS na urządzeniu mobilnym odbywa się poprzez dostarczenie aplikacji informacji o aktywnej licencji. Informacje o licencji są dostarczane na urządzenie mobilne wraz z zasadą, gdy urządzenie zostaje zsynchronizowane z Kaspersky Security Center.

Jeśli aktywacja aplikacji mobilnej nie zostanie zakończona w przeciągu 30 dni od zainstalowania aplikacji na urządzeniu mobilnym, aplikacja zostanie automatycznie przełączona w tryb ograniczonej funkcjonalności. W tym trybie większość komponentów aplikacji nie działa. Po przełączeniu w tryb ograniczonej funkcjonalności aplikacja przestanie wykonywać automatyczną synchronizację z Kaspersky Security Center. Dlatego też, jeśli z jakiegoś powodu aktywacja aplikacji nie zakończyła się w przeciągu 30 dni od zainstalowania aplikacji, użytkownik musi ręcznie zsynchronizować urządzenie z Kaspersky Security Center.

Jeśli Kaspersky Security Center nie jest wdrożony w Twojej organizacji lub nie jest dostępny dla urządzeń mobilnych, użytkownicy mogą ręcznie aktywować aplikację na swoich urządzeniach mobilnych.

Aby akywować aplikację mobilną:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **Licencje**.

3. Użyj listy rozwijanej, aby wybrać wymagany klucz licencyjny z magazynu kluczy Serwera administracyjnego.

   Szczegóły klucza licencyjnego są wyświetlane w poniższych polach.

   Możesz zastąpić istniejący klucz aktywacyjny na urządzeniu mobilnym, jeśli różni się od klucza wybranego z powyższej listy rozwijalnej. Aby to zrobić, zaznacz pole wyboru **Jeśli klucz na urządzeniu jest inny, zastąp go tym kluczem**.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Zapewnianie wymaganych uprawnień dla aplikacji Kaspersky Endpoint Security for Android

Niektóre funkcje aplikacji Kaspersky Endpoint Security for Android wymagają uprawnień. Kaspersky Endpoint Security for Android prosi o obowiązkowe uprawnienia podczas instalacji, a także po instalacji i przed użyciem poszczególnych funkcji aplikacji. Jeśli nie zostaną nadane uprawnienia obowiązkowe, nie będzie można zainstalować Kaspersky Endpoint Security for Android.

Na niektórych urządzeniach (na przykład, Huawei, Meizu i Xiaomi) należy ręcznie dodać Kaspersky Endpoint Security for Android do listy aplikacji uruchamianych w momencie uruchamiania systemu operacyjnego. Jeśli aplikacja nie została dodana do listy, Kaspersky Endpoint Security for Android przestaje wykonywać wszystkie swoje funkcje po ponownym uruchomieniu urządzenia mobilnego.

Na urządzeniach z systemem Android 11 lub nowszym musisz **wyłączyć uprawnienia do usuwania, jeśli aplikacja nie jest używana** w ustawieniach systemowych. W przeciwnym razie, gdy aplikacja nie będzie używana przez kilka miesięcy, system automatycznie zresetuje uprawnienia przyznane aplikacji przez użytkownika.

Uprawnienia wymagane przez aplikację Kaspersky Endpoint Security for Android

Uprawnienie	Funkcja aplikacji
Telefon (wymagane tylko dla systemu Android 5.0 – 9.X)	Nawiązanie połączenia z Kaspersky Security Center (ID urządzenia)
Pamięć (wymagane)	Antywirus
Dostęp do zarządzania wszystkimi plikami	Antywirus (tylko dla systemu Android 11 lub nowszego)
Urządzenia Bluetooth w pobliżu (dla Androida w wersji 12 lub nowszej)	Ogranicz korzystanie z Bluetooth
Administrator urządzenia (obowiązkowe)	Anti-Theft – blokada urządzenia (tylko dla systemu Android 5.0 – 6.X)
	Anti-Theft – zrób zdjęcie złodziejowi przy użyciu przedniego aparatu Chociaż robienie zdjęć nie jest obsługiwane w Kaspersky Security Center Web Console i Cloud Console, aplikacja Kaspersky Endpoint Security for Android wymaga tego uprawnienia, aby mogła być zarządzana przez wszystkie konsole Kaspersky Security Center.
	Anti-Theft – włączenie alarmu
	Anti-Theft – pełny reset
	Ochrona hasłem
	Ochrona przed odinstalowaniem aplikacji
	Instalowanie certyfikatu bezpieczeństwa
	Kontrola aplikacji
	Ograniczenie korzystania z aparatu, Bluetooth i Wi-Fi
Aparat	Anti-Theft – zrób zdjęcie złodziejowi przy użyciu przedniego aparatu

	Chociaż robienie zdjęć nie jest obsługiwane w Kaspersky Security Center Web Console i Cloud Console, aplikacja Kaspersky Endpoint Security for Android wymaga tego uprawnienia, aby mogła być zarządzana przez wszystkie konsole Kaspersky Security Center. Na urządzeniach działających pod kontrolą systemu Android 11.0 lub nowszego użytkownik musi nadać uprawnienie "Podczas używania aplikacji", gdy zostanie o to poproszony.
Lokalizacja	Anti-Theft – lokalizacja urządzenia Na urządzeniach działających pod kontrolą systemu Android 10.0 lub nowszego użytkownik musi nadać uprawnienie "Cały czas", gdy zostanie o to poproszony.
Dostępność	Anti-Theft – blokada urządzenia (tylko dla systemu Android 7.0 lub nowszego)
	Ochrona WWW
	Kontrola aplikacji
	Ochrona przed odinstalowaniem aplikacji (tylko dla systemu Android 7.0 lub nowszego)
	Wyświetlanie ostrzeżeń Kaspersky Endpoint Security for Android (tylko dla systemu Android 10.0 lub nowszego)
	Ograniczenie korzystania z aparatu (tylko Android 11 lub nowszy)

Zarządzanie certyfikatami

Certyfikaty mobilne są używane w celu identyfikacji użytkowników urządzeń mobilnych na Serwerze administracyjnym.

Kaspersky Security Center Web Console i Cloud Console umożliwiają wykonywanie następujących akcji z użyciem certyfikatów mobilnych użytkownika:

- Zobacz certyfikaty i ich statusy.
- Utwórz nowe certyfikaty.
- Odnów wygasające certyfikaty.
- Usuń certyfikaty.

Aby uzyskać więcej informacji o certyfikatach Kaspersky Security Center:

- Jeśli korzystasz z Kaspersky Security Center Web Console, zapoznaj się z *Pomocą Kaspersky Security Center*.
- Jeśli korzystasz z Kaspersky Security Center Cloud Console, zapoznaj się z *Pomocą Kaspersky Security Center Cloud Console*.

Przeglądanie listy certyfikatów

Kaspersky Security Center Web Console i Cloud Console umożliwiają przeglądanie zastosowanych certyfikatów mobilnych użytkowników, ich stanów i właściwości.

Aby wyświetlić listę zastosowanych certyfikatów mobilnych użytkowników:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **URZĄDZENIA MOBILNE** > **URZĄDZENIA**.

2. Wybierz **Zarządzaj certyfikatami**.

   Zostanie otwarta strona **Certyfikaty mobilne** z informacjami o zastosowanych certyfikatach mobilnych użytkowników. Możesz wyświetlić szczegóły certyfikatu, klikając go w kolumnie **Nazwa użytkownika**.

Definiowanie ustawień certyfikatu

Możesz użyć Kaspersky Security Center Web Console lub Cloud Console do skonfigurowania ważności, automatycznych aktualizacji i ochrony hasłem certyfikatów mobilnych.

Aby zdefiniować ustawienia certyfikatu mobilnego:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **URZĄDZENIA MOBILNE** > **URZĄDZENIA**.

2. Wybierz **Zarządzaj certyfikatami**.

3. Wybierz **Ustawienia certyfikatu**.

4. W otwartym oknie **Wygeneruj certyfikaty mobilne** możesz skonfigurować następujące elementy:

   - **Okres ważności certyfikatu (liczba dni)**

     Okres ważności certyfikatu w dniach. Domyślny okres ważności certyfikatu to 365 dni. Po upływie tego okresu urządzenie mobilne nie będzie mogło połączyć się z Serwerem administracyjnym.

   - **Wystaw ponownie, gdy certyfikat wygaśnie za (liczba dni)**

     Liczba dni pozostałych do wygaśnięcia bieżącego certyfikatu, podczas których Serwer administracyjny powinien wydać nowy certyfikat. Na przykład, jeśli wartość tego pola wynosi 4, Serwer administracyjny wystawia nowy certyfikat na cztery dni przed wygaśnięciem bieżącego certyfikatu. Domyślną wartością jest 1.

   - **Jeśli to możliwe, wystaw certyfikat automatycznie**

     Jeśli to możliwe, certyfikaty zostaną ponownie wydane automatycznie. Jeśli ta opcja jest wyłączona, certyfikaty muszą być ponownie wystawiane ręcznie po ich wygaśnięciu. Domyślnie ta opcja jest wyłączona.

   - **Pytaj o hasło podczas instalacji certyfikatu**

     Użytkownik zostanie poproszony o podanie hasła, gdy certyfikat zostanie zainstalowany na urządzeniu mobilnym. Hasło jest używane tylko raz – podczas instalacji certyfikatu na urządzeniu mobilnym. Hasło zostanie automatycznie wygenerowane przez Serwer administracyjny i wysłane do użytkownika pocztą elektroniczną. Długość hasła można określić w polu **Długość hasła**.

5. Kliknij **Zapisz**, aby zastosować zmiany i zamknąć okno.

Określone ustawienia będą używane przez Kaspersky Security Center do tworzenia, aktualizowania i ochrony certyfikatów mobilnych.

Tworzenie certyfikatu

Możesz tworzyć certyfikaty mobilne w Kaspersky Security Center Web Console i Cloud Console w celu identyfikacji użytkowników urządzeń mobilnych.

Aby utworzyć certyfikat mobilny:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **URZĄDZENIA MOBILNE** > **URZĄDZENIA**.

2. Wybierz **Zarządzaj certyfikatami**.

3. W otwartym oknie **Certyfikaty mobilne** kliknij **Dodaj**, aby uruchomić **Kreator tworzenia certyfikatów mobilnych**. Kontynuuj pracę Kreatora, używając przycisku **Dalej**.

4. Wybierz użytkowników lub grupy użytkowników, których urządzeniami mobilnymi chcesz zarządzać za pomocą nowego certyfikatu.

5. Określ **Parametry publikacji**:

   - Jeśli chcesz powiadomić użytkowników o nowym certyfikacie, zaznacz pole **Powiadom użytkownika o nowym certyfikacie**.

   - Jeśli chcesz zezwolić na wielokrotne używanie jednego certyfikatu na tym samym urządzeniu, zaznacz pole **Zezwalaj na wielokrotne używanie jednego certyfikatu na tym samym urządzeniu (tylko dla urządzeń z zainstalowanym Kaspersky Endpoint Security for Android)**.

6. Wybierz **Typ uwierzytelniania**:

   - Wybierz **Poświadczenia (login domeny lub nazwa użytkownika)**, jeśli chcesz, aby użytkownicy uzyskiwali dostęp do certyfikatu przy użyciu swoich poświadczeń.

   - Wybierz **Hasło jednorazowe**, jeśli chcesz, aby użytkownicy uzyskiwali dostęp do certyfikatu przy użyciu hasła jednorazowego.

     Ta opcja jest dostępna, jeśli nie zaznaczyłeś w poprzednim kroku pola **Zezwalaj na wielokrotne używanie jednego certyfikatu na tym samym urządzeniu (tylko dla urządzeń z zainstalowanym Kaspersky Endpoint Security for Android)**.

   - Wybierz opcję **Hasło**, jeśli chcesz, aby użytkownicy uzyskiwali dostęp do certyfikatu przy użyciu hasła.

     Ta opcja jest dostępna, jeśli w poprzednim kroku zaznaczyłeś pole **Zezwalaj na wielokrotne używanie jednego certyfikatu na tym samym urządzeniu (tylko dla urządzeń z zainstalowanym Kaspersky Endpoint Security for Android)**.

7. Określ sposób dostarczenia certyfikatu w polu **Dostarczenie certyfikatu**:

   - Jeśli w poprzednim kroku wybrałeś **Hasło jednorazowe**, wybierz jedną z następujących opcji:

     - Jeśli chcesz wysłać hasło e-mailem, wybierz **Powiadom użytkownika przez e-mail**.

Następnie wybierz, którego adresu e-mail chcesz użyć lub wybierz **Inny adres e-mail**, aby określić inny adres e-mail.

- Jeśli chcesz powiadomić użytkowników o haśle w inny sposób, wybierz **Pokaż hasło po zakończeniu działania kreatora**.

- Jeśli w poprzednim kroku wybrałeś **Poświadczenia (login domeny lub nazwa użytkownika)**, wybierz adres e-mail, którego chcesz użyć lub skorzystaj z opcji **Inny adres e-mail**, aby określić inny adres e-mail.

8. Wyświetlone zostanie podsumowanie certyfikatu.

   Upewnij się, że wszystkie parametry są poprawne, a następnie kliknij **Utwórz**.

W rezultacie **Kreator tworzenia certyfikatów mobilnych** tworzy certyfikat, który użytkownicy mogą instalować na swoich urządzeniach mobilnych. Certyfikat staje się dostępny po następnej synchronizacji urządzeń mobilnych z Kaspersky Security Center.

Więcej informacji o tworzeniu certyfikatów i konfigurowaniu reguł ich wydawania:

- Jeśli korzystasz z Kaspersky Security Center Web Console, zapoznaj się z *Pomocą Kaspersky Security Center*.
- Jeśli korzystasz z Kaspersky Security Center Cloud Console, zapoznaj się z *Pomocą Kaspersky Security Center Cloud Console*.

Odnawianie certyfikatu

Jeśli którykolwiek z zastosowanych certyfikatów mobilnych wkrótce wygaśnie, możesz go odnowić za pomocą Kaspersky Security Center Web Console lub Cloud Console.

Aby odnowić certyfikat mobilny:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **URZĄDZENIA MOBILNE** > **URZĄDZENIA**.
2. Wybierz **Zarządzaj certyfikatami**.
3. Wybierz certyfikat, który chcesz odnowić, a następnie kliknij **Wystaw ponownie**.

   Status certyfikatu zmieni się na **Certyfikat został ponownie wydany**.

Usuwanie certyfikatu

Certyfikaty mobilne możesz usunąć za pomocą Kaspersky Security Center Web Console lub Cloud Console.

Jeśli usuniesz certyfikat mobilny, urządzenie nie będzie mogło dłużej synchronizować się z Serwerem administracyjnym i nie będzie można nim zarządzać za pomocą Kaspersky Security Center. Aby ponownie rozpocząć zarządzanie urządzeniem mobilnym, musisz ponownie zainstalować na nim aplikację Kaspersky Endpoint Security for Android.

Aby usunąć certyfikat mobilny:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **URZĄDZENIA MOBILNE** > **URZĄDZENIA**.

2. Wybierz **Zarządzaj certyfikatami**.

3. Wybierz certyfikat, który chcesz usunąć, a następnie kliknij **Usuń**.

   Certyfikat jest usuwany i przestaje być widoczny na liście certyfikatów.

Wymiana informacji z Firebase Cloud Messaging

Kaspersky Endpoint Security for Android używa usługi Firebase Cloud Messaging (FCM) do zapewnienia dostarczenia poleceń na urządzenia mobilne i wymuszonej synchronizacji, gdy ustawienia zasady zostaną zmienione, w odpowiednim czasie.

Aby korzystać z usługi Firebase Cloud Messaging, należy skonfigurować ustawienia usługi w Kaspersky Security Center Web Console lub Cloud Console.

W celu włączenia Firebase Cloud Messaging w Kaspersky Security Center Web Console lub Cloud Console:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **SYNCHRONIZACJA URZĄDZEŃ ANDROID**.

   Otworzy się okno **Synchronizacja urządzeń Android**.

2. W polach **ID nadawcy** i **Klucz serwera** określ ustawienia Firebase Cloud Messaging: SENDER_ID i API Key.

   Usługa Firebase Cloud Messaging jest włączona.

Aby uzyskać ID nadawcy i klucz serwera:

1. Zarejestruj się w portalu Google.

2. Przejdź do Google Cloud Platform.

3. Utwórz nowy projekt.

   Poczekaj na utworzenie projektu.

4. Znajdź odpowiedni SENDER_ID projektu.

5. Włącz Google Firebase Cloud Messaging for Android.

6. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby utworzyć poświadczenia.

7. Pobierz klucz API z właściwości nowo utworzonych poświadczeń.

   Szczegółowe informacje o operacjach w Google Cloud Platform znajdziesz w jej dokumentacji.

   Posiadasz teraz **ID nadawcy** i **Klucz serwera** aby skonfigurować ustawienia Firebase Cloud Messaging.

Jeśli ustawienia Firebase Cloud Messaging nie zostały skonfigurowane, polecenia na urządzeniu mobilnym i ustawienia zasady zostaną dostarczone po zsynchronizowaniu urządzenia z Kaspersky Security Center zgodnie z terminarzem ustawionym w zasadzie (na przykład, co 24 godziny). Innymi słowy, polecenia i ustawienia zasady zostaną dostarczone z opóźnieniem.

W celu zapewnienia obsługi głównej funkcjonalności produktu, wyrażasz zgodę na automatyczne dostarczenie do usługi Firebase Cloud Messaging unikatowego numeru ID instalacji aplikacji (ID instancji) oraz następujących danych:

- Informacji o zainstalowanym oprogramowaniu: wersji aplikacji, ID aplikacji, wersji kompilacji aplikacji i nazwy pakietu aplikacji.
- Informacji o komputerze, na którym jest zainstalowane oprogramowanie: wersję systemu operacyjnego, ID urządzenia, wersję usług Google.
- Informacji o FCM: ID aplikacji w FCM, ID użytkownika FCM, wersji protokołu.

Dane są przesyłane do usług Firebase poprzez bezpieczne połączenie. Dostęp i ochronę informacji regulują odpowiednie warunki korzystania z usług Firebase: Warunki przetwarzania i bezpieczeństwa danych Firebase, Prywatność i bezpieczeństwo w Firebase.

Aby zapobiec wymianie informacji z usługą Firebase Cloud Messaging:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **SYNCHRONIZACJA URZĄDZEŃ ANDROID**.

   Otworzy się okno **Synchronizacja urządzeń Android**.

2. Kliknij **Resetuj**.
3. W oknie, które zostanie otwarte, kliknij przycisk **OK**, aby potwierdzić resetowanie.

Ustawienia Firebase Cloud Messaging zostaną wyczyszczone.

Zarządzanie urządzeniami mobilnymi w Kaspersky Security Center Web Console i Cloud Console

Możesz zarządzać urządzeniami mobilnymi w Kaspersky Security Center Web Console i Cloud Console, korzystając z zasad grupy i wysyłając polecenia na urządzenia mobilne (wyłączenie dla urządzeń z systemem Android).

Aby zarządzać urządzeniami mobilnymi w Kaspersky Security Center Web Console, musisz zainstalować wtyczki administracyjne.

Podłączanie urządzeń mobilnych do Kaspersky Security Center

Aby zarządzać urządzeniem mobilnym przy użyciu Kaspersky Security Center Web Console lub Cloud Console, urządzenie musi być połączone z Kaspersky Security Center. Listę urządzeń mobilnych podłączonych do Kaspersky Security Center możesz wyświetlić na zakładce **URZĄDZENIA** > **URZĄDZENIA MOBILNE** > **URZĄDZENIA** w Web Console lub Cloud Console.

Przed połączeniem urządzenia z systemem iOS wyślij adres Kaspersky Security Center na urządzenie użytkownika w celu poprawy bezpieczeństwa połączenia. Użytkownik zobaczy ten adres w trakcie instalacji aplikacji i będzie mógł anulować połączenie, jeśli wyświetlony adres nie będzie taki sam jak wysłany przez Ciebie adres.

W celu podłączenia urządzenia mobilnego do Kaspersky Security Center:

1. Uruchom Kreatora podłączania urządzenia mobilnego:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**, a następnie kliknij **Dodaj**.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console wybierz **UŻYTKOWNICY I ROLE** > **UŻYTKOWNICY**. Kliknij nazwę użytkownika lub grupy użytkowników, do której chcesz wysłać odnośnik umożliwiający podłączenie urządzenia mobilnego, a następnie wybierz **URZĄDZENIA.** Kliknij **Dodaj urządzenie mobilne**. W tym przypadku pomiń krok 3.

   Kontynuuj pracę Kreatora, używając przycisku **Dalej.**

2. Wybierz system operacyjny urządzeń, które chcesz dodać:

   - **Android**

   - **iOS i iPadOS**

3. Wybierz użytkowników i grupy użytkowników, do których chcesz wysłać link do podłączenia urządzenia mobilnego.

4. Wybierz adresy e-mail, na jakie wysłać link:

   - **Wszystkie adresy e-mail**

   - **Główny adres e-mail**

   - **Alternatywny adres e-mail**

   - **Inny adres e-mail**

     Jeśli wybierzesz tę opcję, podaj poniżej adres e-mail.

5. Wyświetlone zostanie podsumowanie odnośnika.

   Upewnij się, że wszystkie parametry linku są poprawne, a następnie kliknij **Wyślij**.

6. Otworzy się okno z potwierdzeniem wysłania odnośnika do dodania urządzenia mobilnego.

   Kliknij **OK**, aby zakończyć działania Kreatora.

Gdy użytkownik zainstaluje aplikację Kaspersky Endpoint Security for Android lub Kaspersky Security for iOS, urządzenie użytkownika zostanie wyświetlone na zakładce **URZĄDZENIA** > **URZĄDZENIA MOBILNE** > **URZĄDZENIA** w Web Console lub Cloud Console.

Przenoszenie nieprzypisanych urządzeń mobilnych do grup administracyjnych

Gdy aplikacja Kaspersky Endpoint Security for Android lub Kaspersky Security for iOS jest zainstalowana na urządzeniach mobilnych, są one wyświetlane na stronie **WYKRYWANIE I WDRAŻANIE** > **NIEPRZYPISANE URZĄDZENIA** w Kaspersky Security Center Web Console lub Cloud Console. Aby zarządzać nowo podłączonymi urządzeniami, możesz utworzyć regułę ich automatycznego przydzielania do grup administracyjnych lub ręcznie przenieść je do grupy administracyjnej.

Aby przenieść nieprzypisane urządzenie mobilne do grupy administracyjnej:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console wybierz **WYKRYWANIE I WDRAŻANIE** > **NIEPRZYPISANE URZĄDZENIA**.

2. Wybierz urządzenie, które chcesz przenieść do grupy administracyjnej, a następnie kliknij **Przenieś do grupy**.

3. Z drzewa grup administracyjnych, które się otworzy, wybierz grupę docelową, do której chcesz przenieść urządzenie.

   Możesz utworzyć nową grupę administracyjną, wybierając istniejącą grupę, a następnie klikając **Dodaj grupę podrzędną**.

4. Kliknij **Przenieś**.

Urządzenie zostanie przeniesione do określonej grupy administracyjnej i zostaną do niego zastosowane zasady grupy.

Wysyłanie poleceń na urządzenia mobilne

Możesz wysyłać polecenia na urządzenia mobilne z systemem Android, aby chronić dane na urządzeniu mobilnym, które zostało zgubione lub skradzione lub aby wykonać wymuszoną synchronizację urządzenia mobilnego z Kaspersky Security Center.

Nie możesz wysłać poleceń na urządzenia z systemem iOS.

Obsługiwane są następujące polecenia:

- **Zablokuj urządzenie**

  Urządzenie mobilne zostanie zablokowane.

- **Odblokuj urządzenie**

  Urządzenie mobilne zostanie odblokowane. Po odblokowaniu urządzenia mobilnego działającego pod kontrolą systemu Android 5.0 – 6.X, hasło odblokowujące ekran (kod PIN) zostaje zresetowane do wartości "1234". Po odblokowaniu urządzenia działającego pod kontrolą systemu Android 7.0 lub nowszego, hasło odblokowujące ekran nie zostaje zmienione.

- **Przywróć ustawienia fabryczne**

  Wszystkie dane zostaną usunięte z urządzenia mobilnego i zostaną przywrócone ustawienia domyślne.

- **Usuń dane firmowe**

  Skonteneryzowane dane i firmowe konto e-mail są usuwane z urządzenia mobilnego.

- **Zlokalizuj urządzenie**

  Urządzenie zostanie zlokalizowane i wyświetlone na Google Maps. Operator telefonii komórkowej może pobierać opłatę za dostęp do internetu.

  Na urządzeniach z systemem Android 12 lub nowszym, jeśli użytkownik przyznał uprawnienie "Użyj przybliżonej lokalizacji", aplikacja Kaspersky Endpoint Security for Android najpierw spróbuje uzyskać dokładną lokalizację urządzenia. Jeśli to się nie powiedzie, przybliżona lokalizacja urządzenia zostanie zwrócona tylko wtedy, gdy została odebrana nie więcej niż 30 minut wcześniej. W przeciwnym razie polecenie **Zlokalizuj urządzenie** nie powiedzie się.

- **Alarm dźwiękowy**

  Urządzenie mobilne włączy alarm. Alarm będzie włączony przez 5 minut (lub przez 1 minutę, jeśli bateria urządzenia jest słaba).

- **Synchronizuj urządzenie**

  Urządzenie mobilne jest synchronizowane z Kaspersky Security Center.

Aplikacja Kaspersky Endpoint Security for Android wymaga określonych uprawnień do wykonywania poleceń. Jeśli Kreator wstępnej konfiguracji jest uruchomiony, Kaspersky Endpoint Security for Android wyświetli pytanie o nadanie aplikacji wszystkich wymaganych uprawnień. Użytkownik może pominąć te kroki lub wyłączyć te uprawnienia w ustawieniach urządzenia w późniejszym czasie. W takiej sytuacji niemożliwe będzie wykonywanie poleceń.

Na urządzeniach działających pod kontrolą systemu Android 10.0 lub nowszego użytkownik musi nadać uprawnienie "Cały czas", aby uzyskać dostęp do lokalizacji Na urządzeniach działających pod kontrolą systemu Android 11.0 lub nowszego użytkownik musi nadać uprawnienie "Podczas używania aplikacji", aby uzyskać dostęp do aparatu. W przeciwnym razie polecenia anti-theft nie będą działały. Użytkownik zostanie powiadomiony o tym ograniczeniu i ponownie poproszony o nadanie wymaganego poziomu uprawnień. Jeśli użytkownik wybierze opcję "Tylko teraz" dla uprawnienia dostępu do aparatu, aplikacja uzna, że dostęp został nadany. Jeśli ponownie zostanie wyświetlona prośba o nadanie uprawnienia dostępu do aparatu, zalecane jest bezpośrednie skontaktowanie się z użytkownikiem.

Aby wysłać polecenie na urządzenie mobilne:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**.
2. Wybierz urządzenie, do którego chcesz wysłać polecenie, a następnie kliknij opcję **Kontrola** lub **Zarządzaj**.
3. Wybierz żądane polecenie z listy **Dostępne polecenia**, a następnie kliknij przycisk **OK**.
4. Kliknij **OK**, jeśli pojawi się monit o potwierdzenie operacji.

Określone polecenie jest wysyłane na urządzenie mobilne i wyświetlane jest okno potwierdzenia.

Usuwanie urządzeń mobilnych z Kaspersky Security Center

Jeśli nie potrzebujesz już zarządzać urządzeniem mobilnym, możesz usunąć je z Kaspersky Security Center przy użyciu Web Console lub Cloud Console.

W celu usunięcia urządzenia mobilnego z Kaspersky Security Center:

1. Usuń aplikację mobilną z urządzenia lub sprawdź, czy użytkownik usunął aplikację z wymaganego urządzenia.
2. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**.
3. Wybierz urządzenie mobilne, które chcesz usunąć, a następnie kliknij **Usuń**.
4. Kliknij **OK**, aby potwierdzić operację.

Urządzenie zostanie usunięte z Kaspersky Security Center.

Zarządzanie zasadami grupy

W tej sekcji opisano, jak zarządzać zasadami grupy w Kaspersky Security Center Web Console i Cloud Console.

Profile grupowe do zarządzania urządzeniami mobilnymi

Zasada grupy to pakiet ustawień do zarządzania urządzeniami mobilnymi, które należą do grupy administracyjnej, oraz do zarządzania aplikacjami mobilnymi zainstalowanymi na urządzeniach.

Możesz użyć zasady do skonfigurowania ustawień pojedynczych urządzeń oraz grupy urządzeń. Dla grupy urządzeń ustawienia administracyjne można skonfigurować w oknie właściwości zasady grupowej.

Każdy parametr odzwierciedlony w zasadzie posiada atrybut "zablokowany", co pokazuje, czy możliwe jest modyfikowanie ustawienia w zasadach zagnieżdżonych poziomów hierarchii (dla grup zagnieżdżonych i podrzędnych Serwerów administracyjnych), w lokalnych ustawieniach aplikacji.

Wartości ustawień skonfigurowane w zasadzie i lokalnych ustawieniach aplikacji są zapisywane na Serwerze administracyjnym, rozsyłane na urządzenia mobilne podczas synchronizacji i zapisywane na urządzeniach jako bieżące ustawienia. Jeśli użytkownik określił inne wartości ustawień, które nie zostały "zablokowane", podczas kolejnej synchronizacji urządzenia z Serwerem administracyjnym nowe wartości ustawień są przesyłane do Serwera administracyjnego i zapisywane w lokalnych ustawieniach aplikacji zamiast wartości, które zostały wcześniej określone przez administratora.

Aby zapewnić aktualność ochrony urządzeń mobilnych z systemem Android, możesz monitorować urządzenia użytkowników pod kątem zgodności z firmowymi wymogami bezpieczeństwa.

Aby uzyskać więcej informacji na temat zarządzania zasadami i grupami administracyjnymi w Kaspersky Security Center Web Console i Cloud Console:

- Jeśli korzystasz z Kaspersky Security Center Web Console, zapoznaj się z *Pomocą Kaspersky Security Center*.
- Jeśli korzystasz z Kaspersky Security Center Cloud Console, zapoznaj się z *Pomocą Kaspersky Security Center Cloud Console*.

Przeglądanie listy zasad grupy

Kaspersky Security Center Web Console i Cloud Console umożliwiają przeglądanie zasad grupy, ich stanów i właściwości.

W celu wyświetlenia listy zasad grupy,

W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**.

Lista zasad grupy otwiera się z krótkimi informacjami na temat zasad grupy. Na tej stronie możesz tworzyć, modyfikować, kopiować, przenosić i usuwać zasady grupy.

Przeglądanie wyników dystrybucji zasad

Kaspersky Security Center Web Console i Cloud Console umożliwiają przeglądanie wykresu dystrybucji zasady grupy oraz informacji o wszystkich urządzeniach objętych tą zasadą.

Aby wyświetlić wyniki dystrybucji zasady grupy:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**.

2. Na wyświetlonej liście zasad grupy zaznacz pole wyboru obok nazwy zasady, dla której chcesz wyświetlić wyniki dystrybucji, a następnie kliknij **Dystrybucja**.

   Otworzy się strona wyników dystrybucji zasad. Ta strona zawiera podsumowanie zasad, schemat dystrybucji zasad oraz tabelę z informacjami o wszystkich urządzeniach objętych tymi zasadami. Możesz otworzyć okno właściwości zasady, klikając przycisk **Konfiguruj zasadę**.

Tworzenie zasady grupy

Kaspersky Security Center Web Console i Cloud Console umożliwiają tworzenie zasad grupy w celu zarządzania urządzeniami mobilnymi.

W celu usunięcia zasady grupy:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**.

2. Na wyświetlonej liście zasad grupy Kaspersky Security Center kliknij **Bieżąca ścieżka**, aby wybrać grupę administracyjną, dla której chcesz utworzyć zasadę.

   Domyślnie nowe zasady grupy są stosowane do grupy **Zarządzane urządzenia**.

3. Kliknij przycisk **Dodaj**, aby uruchomić Kreatora tworzenia zasad. Kontynuuj pracę Kreatora, używając przycisku **Dalej.**

4. Wybierz aplikację w zależności od platformy:

   - **Kaspersky Endpoint Security for Android**
   - **Kaspersky Security for iOS**

5. Wpisz nazwę nowej zasady w polu **Nazwa**. Jeśli określisz nazwę istniejącej zasady, do jego nazwy automatycznie zostanie dodany przyrostek (1).

6. Wybierz stan zasady:

   - **Aktywny**

     Kreator zapisze utworzoną zasadę na Serwerze administracyjnym. Przy kolejnej synchronizacji urządzenia mobilnego z Serwerem administracyjnym zasada zostanie użyta na urządzeniu jako zasada aktywna.

   - **Nieaktywny**

Kreator zapisze utworzoną zasadę na Serwerze administracyjnym jako zapasową zasadę. Ta zasada może być aktywowana w późniejszym czasie, po wystąpieniu określonego zdarzenia. Jeśli to konieczne, zasada nieaktywna może zostać przełączona w stan aktywny.

Dla jednej aplikacji w grupie może zostać utworzonych wiele różnych zasad, ale tylko jedna z nich może być aktywna. Po utworzeniu nowej aktywnej zasady, poprzednia aktywna zasada automatycznie staje się nieaktywna.

7. Możesz włączyć lub wyłączyć dwie opcje dziedziczenia, **Dziedzicz ustawienia z zasady nadrzędnej** i **Wymuś dziedziczenie ustawień w zasadach podrzędnych**:

   - Jeśli włączysz **Dziedzicz ustawienia z zasady nadrzędnej** dla podrzędnej grupy administracyjnej i zablokujesz niektóre ustawienia w zasadzie nadrzędnej, nie możesz zmienić tych ustawień w zasadzie dla grupy podrzędnej. Możesz jednak zmienić ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

   - Jeśli wyłączysz **Dziedzicz ustawienia z zasady nadrzędnej** dla podrzędnej grupy administracyjnej, możesz zmienić wszystkie ustawienia w grupie podrzędnej, nawet jeśli niektóre ustawienia są zablokowane w zasadzie nadrzędnej.

   - Włączenie opcji **Wymuś dziedziczenie ustawień w zasadach podrzędnych** w nadrzędnej grupie administracyjnej powoduje włączenie opcji **Dziedzicz ustawienia z zasady nadrzędnej** dla każdej zasady podrzędnej. W takim przypadku nie można wyłączyć tej opcji dla żadnej zasady podrzędnej. Wszystkie ustawienia zablokowane w zasadzie nadrzędnej są dziedziczone przymusowo w grupach podrzędnych i nie można zmienić tych ustawień w grupach podrzędnych.

   - W zasadach grupy **Zarządzane urządzenia** opcja **Dziedzicz ustawienia z zasady nadrzędnej** nie wpływa na żadne ustawienia, ponieważ grupa **Zarządzane urządzenia** nie ma żadnych grup nadrzędnych i dlatego nie dziedziczy żadnych zasad.

   Domyślnie opcja **Dziedzicz ustawienia z zasady nadrzędnej** jest włączona, a opcja **Wymuś dziedziczenie ustawień w zasadach podrzędnych** jest wyłączona.

8. Jeśli chcesz, możesz zdefiniować ustawienia nowo utworzonej zasady. W tym celu wybierz zakładkę **USTAWIENIA APLIKACJI**, a następnie postępuj zgodnie z opisem w sekcji "Definiowanie ustawień zasady".

   Alternatywnie możesz to zrobić później.

9. Kliknij **Zapisz**, aby utworzyć zasadę.

Utworzona zostanie nowa zasada grupy do zarządzania urządzeniami mobilnymi.

Modyfikacja zasady grupy

Kaspersky Security Center Web Console i Cloud Console umożliwiają modyfikowanie ustawień zasad grupy.

W celu zmodyfikowania zasady grupy:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. W oknie właściwości zasady wybierz **USTAWIENIA APLIKACJI**, a następnie zdefiniuj ustawienia zasady zgodnie z opisem w sekcji "Definiowanie ustawień zasady".

   Możesz także skonfigurować ustawienia ogólne, dziedziczenie ustawień, rejestrowanie zdarzeń i powiadomienia, profile zasad oraz przeglądać historię rewizji. W celu uzyskania więcej informacji, odwiedź stronę *Pomocy Kaspersky Security Center*.

3. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Kopiowanie zasady grupy

Kaspersky Security Center Web Console i Cloud Console umożliwiają utworzenie kopii zasady grupy.

Aby utworzyć kopię zasady grupy:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**.
2. Na wyświetlonej liście zasad grupy zaznacz pole wyboru obok nazwy zasady, dla której chcesz utworzyć kopię, a następnie kliknij **Kopiuj**.
3. Z drzewa grup administracyjnych, które zostanie otwarte, wybierz grupę docelową, w której chcesz utworzyć kopię zasady.

   Możesz utworzyć nową grupę administracyjną, wybierając istniejącą grupę, a następnie klikając **Dodaj grupę podrzędną**.

4. Kliknij **Kopiuj**.
5. Kliknij **OK**, aby potwierdzić operację.

W grupie docelowej o tej samej nazwie zostanie utworzona kopia zasady. Stan każdej skopiowanej lub przeniesionej zasady w grupie docelowej będzie **Nieaktywny**. W każdej chwili możesz zmienić stan na **Aktywny**.

Jeżeli w grupie docelowej istnieje już zasada o nazwie identycznej z nazwą nowo utworzonej lub przeniesionej zasady, do nazwy nowo utworzonej lub przeniesionej zasady dodawany jest indeks (<następny numer sekwencyjny>), na przykład: (1).

Przenoszenie zasady do innej grupy administracyjnej

Kaspersky Security Center Web Console i Cloud Console umożliwiają przeniesienie zasady do innej grupy administracyjnej.

Aby przenieść zasadę do innej grupy administracyjnej:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**.

2. Na otwartej liście zasad grupy zaznacz pole wyboru obok nazwy zasady, którą chcesz przenieść do innej grupy administracyjnej, a następnie kliknij **Przenieś**.

3. Z drzewa grup administracyjnych, które zostanie otwarte, wybierz grupę docelową, do której chcesz przenieść zasadę.

   Możesz utworzyć nową grupę administracyjną, wybierając istniejącą grupę, a następnie klikając **Dodaj grupę podrzędną**.

4. Kliknij **Przenieś**.

5. Kliknij **OK**, aby potwierdzić operację.

Wynik zależy od właściwości dziedziczenia zasady:

- Jeśli zasada nie jest dziedziczona w grupie źródłowej, zostanie przeniesiona do grupy docelowej.
- Jeśli zasada jest dziedziczona w grupie źródłowej, nie zostanie przeniesiona. Zamiast tego w grupie docelowej zostanie utworzona kopia tej zasady.

Stan każdej skopiowanej lub przeniesionej zasady w grupie docelowej będzie **Nieaktywny**. W każdej chwili możesz zmienić stan na **Aktywny**.

Jeżeli w grupie docelowej istnieje już zasada o nazwie identycznej z nazwą nowo utworzonej lub przeniesionej zasady, do nazwy nowo utworzonej lub przeniesionej zasady dodawany jest indeks (<następny numer sekwencyjny>), na przykład: (1).

Usunięcie zasady grupy

Kaspersky Security Center Web Console i Cloud Console umożliwiają usuwanie zasad grupy.

Możesz usunąć tylko zasadę, która nie jest dziedziczona w bieżącej grupie administracyjnej. Jeśli zasada jest dziedziczona, możesz ją usunąć tylko w grupie wyższego poziomu, dla której została utworzona.

W celu usunięcia zasady grupy:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**.

2. Na wyświetlonej liście zasad grupy zaznacz pole wyboru obok nazwy zasady, którą chcesz usunąć, a następnie kliknij **Usuń**.

3. Kliknij **OK**, aby potwierdzić operację.

Zasada grupy zostanie usunięta.

Definiowanie ustawień zasady

W tej sekcji opisano, jak zdefiniować ustawienia zasad Kaspersky Security Center do zarządzania urządzeniami mobilnymi.

Ustawienia zasady można zdefiniować podczas tworzenia lub modyfikowania zasady.

Konfigurowanie ochrony antywirusowej

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Aby natychmiast wykrywać zagrożenia, wirusy i inne szkodliwe aplikacje, należy skonfigurować ochronę w czasie rzeczywistym i automatyczne uruchamianie skanowania antywirusowego.

Kaspersky Endpoint Security for Android wykrywa następujące typy obiektów:

- Wirusy, robaki, trojany i złośliwe narzędzia
- Adware
- Aplikacje, które mogą być wykorzystywane przez cyberprzestępców w celu wyrządzenia szkody na Twoim urządzeniu lub kradzieży danych osobowych

Ze względu na ograniczenia techniczne, Kaspersky Endpoint Security for Android nie może skanować plików o rozmiarze 2 GB lub większym. Podczas skanowania aplikacja pomija duże pliki i nie powiadamia o pominięciu takich plików.

Konfigurowanie ochrony w czasie rzeczywistym

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

W celu skonfigurowania ochrony w czasie rzeczywistym:

1. Otwórz okno właściwości zasady:
   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.
   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.
2. W oknie właściwości zasady wybierz **USTAWIENIA APLIKACJI** > **Ochrona podstawowa**.
3. W sekcji **Antywirus** skonfiguruj ochronę systemu plików urządzenia mobilnego:
   - Aby włączyć ochronę w czasie rzeczywistym urządzenia mobilnego przed zagrożeniami, zaznacz pole **Włącz ochronę antywirusową w czasie rzeczywistym**.

- Określ poziom ochrony:
  - Jeśli chcesz, aby Kaspersky Endpoint Security for Android skanował tylko nowe aplikacje i pliki z folderu Pobrane, wybierz **Skanuj tylko nowe aplikacje**.
  - Aby włączyć rozszerzoną ochronę urządzenia mobilnego przed zagrożeniami, wybierz **Skanuj wszystkie aplikacje i monitoruj działania dotyczące plików**.

    Kaspersky Endpoint Security for Android skanuje wszystkie pliki otwierane, modyfikowane, przenoszone, kopiowane, instalowane lub zapisywane przez użytkownika na urządzeniu, a także nowo zainstalowane aplikacje mobilne.

    Na urządzeniach z systemem Android 8.0 lub nowszym Kaspersky Endpoint Security for Android skanuje pliki, które użytkownik modyfikuje, przenosi, instaluje i zapisuje, a także kopie plików. Kaspersky Endpoint Security for Android nie skanuje plików po ich otwarciu lub plików źródłowych po ich skopiowaniu.
- Aby włączyć dodatkowe skanowanie nowych aplikacji przed ich pierwszym uruchomieniem na urządzeniu użytkownika za pomocą usługi chmury Kaspersky Security Network, zaznacz pole **Dodatkowa ochrona zapewniana przez Kaspersky Security Network**.
- Aby zablokować oprogramowanie reklamowe i aplikacje, które mogą zostać wykorzystane przez przestępców w celu uszkodzenia urządzenia lub danych użytkownika, zaznacz pole wyboru **Wykrywaj adware, autodialery i aplikacje, które mogą być wykorzystywane przez cyberprzestępców do uszkodzenia urządzenia i danych użytkownika**.

4. W sekcji **Ustawienia antywirusa** wybierz akcję, która zostanie wykonana po wykryciu zagrożenia:
   - **Usuń i zapisz kopię zapasową pliku w kwarantannie**

     Wykryte obiekty zostaną automatycznie usunięte. Użytkownik nie musi podejmować żadnych dodatkowych działań. Przed usunięciem obiektu Kaspersky Endpoint Security for Android utworzy kopię zapasową pliku i zapisze ją w kwarantannie.
   - **Usuń**

     Wykryte obiekty zostaną automatycznie usunięte. Użytkownik nie musi podejmować żadnych dodatkowych działań. Przed usunięciem obiektu, Kaspersky Endpoint Security for Android wyświetli tymczasowe powiadomienie o wykryciu obiektu.
   - **Pomiń**

     Jeśli wykryte obiekty zostaną pominięte, Kaspersky Endpoint Security for Android ostrzeże użytkownika o problemach z ochroną urządzenia. Informacja na temat pominiętych obiektów jest wyświetlana w sekcji aplikacji **Stan**. Dla każdego pominiętego zagrożenia, aplikacja udostępnia działania użytkownikowi, które może wykonać w celu eliminacji zagrożenia. Lista pominiętych obiektów może ulec zmianie, na przykład, jeśli szkodliwy plik został usunięty lub przeniesiony. Aby uzyskać aktualną listę zagrożeń, uruchom pełne skanowanie urządzenia. Aby zapewnić solidną ochronę danych, wyeliminuj wszystkie wykryte obiekty.

5. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie automatycznego uruchamiania skanowania antywirusowego na urządzeniu mobilnym

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

W celu skonfigurowania automatycznego uruchamiania skanowania antywirusowego na urządzeniu mobilnym:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. W oknie właściwości zasady wybierz **USTAWIENIA APLIKACJI** > **Ochrona podstawowa**.

3. Aby zablokować oprogramowanie reklamowe i aplikacje, które mogą zostać wykorzystane przez przestępców do uszkodzenia urządzenia lub danych użytkownika, zaznacz pole wyboru **Wykrywaj adware, autodialery i aplikacje, które mogą być wykorzystywane przez cyberprzestępców do uszkodzenia urządzenia i danych użytkownika** w sekcji **Skanowanie urządzenia**.

4. Na liście **Akcja po wykryciu zagrożenia** wybierz jedną z następujących opcji:

   - **Usuń i zapisz kopię zapasową pliku w kwarantannie**

     Wykryte obiekty zostaną automatycznie usunięte. Użytkownik nie musi podejmować żadnych dodatkowych działań. Przed usunięciem obiektu Kaspersky Endpoint Security for Android utworzy kopię zapasową pliku i zapisze ją w kwarantannie.

   - **Usuń**

     Wykryte obiekty zostaną automatycznie usunięte. Użytkownik nie musi podejmować żadnych dodatkowych działań. Przed usunięciem obiektu, Kaspersky Endpoint Security for Android wyświetli tymczasowe powiadomienie o wykryciu obiektu.

   - **Pomiń**

     Jeśli wykryte obiekty zostaną pominięte, Kaspersky Endpoint Security for Android ostrzeże użytkownika o problemach z ochroną urządzenia. Informacja na temat pominiętych obiektów jest wyświetlana w sekcji aplikacji **Stan**. Dla każdego pominiętego zagrożenia, aplikacja udostępnia działania użytkownikowi, które może wykonać w celu eliminacji zagrożenia. Lista pominiętych obiektów może ulec zmianie, na przykład, jeśli szkodliwy plik został usunięty lub przeniesiony. Aby uzyskać aktualną listę zagrożeń, uruchom pełne skanowanie urządzenia. Aby zapewnić solidną ochronę danych, wyeliminuj wszystkie wykryte obiekty.

   - **Pytaj użytkownika**

     Aplikacja Kaspersky Endpoint Security for Android wyświetla powiadomienie z monitem o wybranie akcji, która ma zostać podjęta wobec wykrytego obiektu: **Pomiń** lub **Usuń**.

     Jeśli aplikacja wykryje kilka zagrożeń, opcja **Pytaj użytkownika** umożliwi użytkownikowi urządzenia zastosowanie wybranej akcji do każdego pliku poprzez użycie opcji **Zastosuj do wszystkich**.

Program Kaspersky Endpoint Security for Android musi zostać ustawiony jako usługa dostępności w celu zapewnienia wyświetlania powiadomień na urządzeniach mobilnych działających pod kontrolą systemu Android 10.0 lub nowszego. Kaspersky Endpoint Security for Android wyświetli pytanie o ustawienie aplikacji jako usługę funkcji Dostępności poprzez Kreator wstępnej konfiguracji. Użytkownik może pominąć ten krok lub wyłączyć tę usługę w ustawieniach urządzenia w późniejszym czasie. W tym przypadku aplikacja Kaspersky Endpoint Security for Android wyświetla okno systemowe z monitem o wybranie akcji, która ma zostać podjęta na wykrytym obiekcie: Pomiń lub Usuń. Aby zastosować akcję na kilku obiektach, musisz otworzyć Kaspersky Endpoint Security.

5. W sekcji **Zaplanowane skanowanie** możesz skonfigurować automatyczne pełne skanowanie systemu plików urządzenia.

   Wybierz jedną z następujących opcji:

   - **Wyłączono**

     Skanowanie systemu plików urządzenia nie zostanie uruchomione automatycznie.

   - **Po aktualizacji baz danych**

     System plików urządzenia będzie automatycznie skanowany przy każdej aktualizacji antywirusowej bazy danych.

   - **Codziennie**

     System plików urządzenia będzie codziennie automatycznie skanowany.

     Jeśli wybierzesz tę opcję, możesz również określić czas skanowania w polu **Czas uruchomienia**.

   - **Co tydzień**

     System plików urządzenia będzie skanowany automatycznie raz w tygodniu.

     Jeśli wybierzesz tę opcję, możesz również wybrać dzień tygodnia, w którym chcesz uruchomić skanowanie, korzystając z listy rozwijanej i określając czas skanowania w polu **Czas uruchomienia**.

W systemie Android 12 lub nowszych aplikacja może wykonać to zadanie później niż określono, jeśli urządzenie jest w trybie oszczędzania baterii.

6. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie aktualizacji antywirusowych baz danych

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

W celu skonfigurowania aktualizacji antywirusowych baz danych:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

- W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. W oknie właściwości zasady wybierz **USTAWIENIA APLIKACJI** > **Aktualizacja baz danych**.

3. W sekcji **Aktualizacja baz danych** skonfiguruj terminarz automatycznej aktualizacji baz danych na urządzeniu użytkownika.

   Wybierz jedną z następujących opcji:

   - **Wyłączono**

     Automatyczne aktualizacje antywirusowych baz danych zostaną wyłączone.

   - **Codziennie**

     Antywirusowe bazy danych będą aktualizowane codziennie.

     Jeśli wybierzesz tę opcję, możesz również określić czas aktualizacji w polu **Czas aktualizacji**.

   - **Co tydzień**

     Antywirusowe bazy danych będą aktualizowane raz w tygodniu.

     Jeśli wybierzesz tę opcję, możesz również określić czas aktualizacji w polu **Czas aktualizacji** oraz dzień tygodnia, w którym chcesz uruchomić aktualizację na liście rozwijanej **Dzień tygodnia**.

   W systemie Android 12 lub nowszych aplikacja może wykonać to zadanie później niż określono, jeśli urządzenie jest w trybie oszczędzania baterii.

4. W sekcji **Źródło uaktualnień baz danych** wybierz źródło uaktualnień, z którego Kaspersky Endpoint Security for Android będzie pobierał i instalował uaktualnienia antywirusowych baz danych aplikacji:

   - **Serwery Kaspersky**

     Kaspersky Endpoint Security for Android użyje serwera aktualizacji Kaspersky jako źródła aktualizacji do pobierania antywirusowych baz danych na urządzenie użytkownika.

   - **Serwer administracyjny**

     Dostępne tylko wtedy, gdy korzystasz z Kaspersky Security Center Web Console.

     Kaspersky Endpoint Security for Android użyje repozytorium Serwera administracyjnego Kaspersky Security Center jako źródła aktualizacji do pobierania antywirusowych baz danych na urządzenie użytkownika.

   - **Inne źródło**

     Kaspersky Endpoint Security for Android użyje serwera innej firmy jako źródła aktualizacji do pobierania antywirusowych baz danych na urządzenie użytkownika.

     W przypadku wybrania tej opcji należy określić adres serwera HTTP w polu **Użyj innego serwera jako źródła aktualizacji antywirusowych baz danych**.

5. Jeśli chcesz, aby Kaspersky Endpoint Security for Android pobierał uaktualnienia antywirusowych baz danych zgodnie z terminarzem, gdy urządzenie użytkownika jest w roamingu, w sekcji **Aktualizuj antywirusowe bazy danych podczas roamingu** zaznacz pole **Zezwól na aktualizację baz danych podczas roamingu**.

6. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Definiowanie ustawień odblokowania urządzenia

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Aby zabezpieczyć urządzenie mobilne, należy skonfigurować używanie hasła, o którego wprowadzenie użytkownik będzie proszony, gdy urządzenie przejdzie w tryb uśpienia.

Możesz nałożyć ograniczenia dotyczące aktywności użytkownika w przypadku, gdy hasło odblokowujące jest słabe (na przykład, zablokować urządzenie). Ograniczenia można nałożyć przy użyciu komponentu Kontrola zgodności.

Na pewnych urządzeniach Samsung działających pod kontrolą systemu Android 7.0 lub nowszego, jeśli użytkownik spróbuje skonfigurować nieobsługiwane metody odblokowania urządzenia (na przykład, wzór), urządzenie może zostać zablokowane, gdy spełnione będą następujące warunki: włączona jest ochrona przed dezinstalacją Kaspersky Endpoint Security for Android oraz ustawione są wymagania wobec siły hasła odblokowującego ekran. Aby odblokować urządzenie, należy wysłać specjalne polecenie na urządzenie.

W celu skonfigurowania siły hasła odblokowującego urządzenie:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. W oknie właściwości zasady wybierz **USTAWIENIA APLIKACJI** > **Ochrona podstawowa**.

3. Jeśli chcesz, żeby aplikacja sprawdzała, czy ustawiono hasło odblokowujące, w sekcji **Ochrona hasłem** zaznacz pole **Wymagaj ustawienia hasła odblokowującego ekran**.

   Jeśli aplikacja wykryje, że na urządzeniu nie określono hasła systemowego, zapyta użytkownika o jego ustawienie. Hasło zostanie ustawione zgodnie z parametrami zdefiniowanymi przez administratora

4. Określ minimalną liczbę znaków w haśle użytkownika.

   Możliwe wartości: od 4 do 16 znaków.

   Domyślnie, hasło użytkownika powinno zawierać 4 znaki.

   Na urządzeniach z Androidem 10.0 lub nowszym Kaspersky Endpoint Security przetwarza wymagania dotyczące mocy hasła na jedną z wartości systemowych: średnią lub wysoką.

   Wartości dla urządzeń z systemem Android 10.0 lub nowszym są określane przez następujące reguły:

   - Jeśli wymagana długość hasła wynosi od 1 do 4 symboli, aplikacja prosi użytkownika o ustawienie hasła o średniej mocy. Musi być numeryczne (PIN) bez powtarzających się lub uporządkowanych (np. 1234) sekwencji albo alfanumeryczne. Kod PIN lub hasło musi mieć co najmniej 4 znaki.

- Jeśli wymagana długość hasła to 5 lub więcej symboli, aplikacja prosi użytkownika o ustawienie silnego hasła. Musi być numeryczne (PIN) bez powtarzających się lub uporządkowanych sekwencji albo alfanumeryczne (hasło). Kod PIN musi mieć co najmniej 8 cyfr; hasło musi mieć co najmniej 6 znaków.

5. Jeśli chcesz, aby użytkownik miał możliwość używania odcisków palców do odblokowywania ekranu, zaznacz pole wyboru **Zezwalaj na używanie odcisków palców (w przypadku urządzeń z systemem Android 9 lub starszym)**. Jeśli hasło odblokowujące nie jest zgodne z firmowymi wymaganiami bezpieczeństwa, nie możesz użyć czytnika linii papilarnych do odblokowania ekranu.

   Na urządzeniach z Androidem 10.0 lub nowszym odblokowywanie ekranu odciskiem palca nie jest obsługiwane.

   Kaspersky Endpoint Security for Android nie ogranicza korzystania z czytnika linii papilarnych do logowania do aplikacji lub potwierdzania zakupów.

   Na niektórych urządzeniach Samsung niemożliwe jest zablokowanie użycia odcisku palca do odblokowania urządzenia.

   Na niektórych urządzeniach Samsung, jeśli hasło odblokowujące nie jest zgodne z firmowymi wymaganiami bezpieczeństwa, Kaspersky Endpoint Security for Android nie blokuje użycia odcisku palca do odblokowania ekranu.

   Po dodaniu odcisku palca w ustawieniach urządzenia, użytkownik może odblokować ekran przy użyciu następujących metod:

   - Przyłóż palec do czytnika linii papilarnych (główna metoda).
   - Wprowadź hasło odblokowujące (metoda zapasowa).

6. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie ochrony danych na skradzionym lub zagubionym urządzeniu

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Aby chronić dane firmowe w przypadku zgubienia lub kradzieży urządzenia mobilnego, należy skonfigurować ochronę przed nieautoryzowanym dostępem.

Aby zapewnić ochronę skradzionych lub utraconych danych urządzenia, Kaspersky Endpoint Security for Android musi być ustawiony jako funkcja ułatwień dostępu. Kaspersky Endpoint Security for Android wyświetli pytanie o ustawienie aplikacji jako usługę funkcji Dostępności poprzez Kreator wstępnej konfiguracji. Użytkownik może pominąć ten krok lub wyłączyć tę usługę w ustawieniach urządzenia w późniejszym czasie.

W celu skonfigurowania ochrony na skradzionym lub zagubionym urządzeniu:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. W oknie właściwości zasady wybierz **USTAWIENIA APLIKACJI** > **Ochrona podstawowa**.

3. W sekcji **Anti-Theft** skonfiguruj blokowanie urządzenia:

   - Określ liczbę znaków w kodzie odblokowującym.

   - Określ tekst, który ma być wyświetlany, gdy urządzenie jest zablokowane.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie kontroli aplikacji

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Kontrola aplikacji sprawdza, czy aplikacje zainstalowane na urządzeniu mobilnym odpowiadają firmowym wymaganiom bezpieczeństwa. W Kaspersky Security Center administrator tworzy listy dozwolonych, blokowanych, obowiązkowych i zalecanych aplikacji zgodnie z firmowymi wymaganiami bezpieczeństwa. W wyniku działania Kontroli aplikacji program Kaspersky Endpoint Security wyświetli pytanie użytkownikowi o zainstalowanie obowiązkowych i zalecanych aplikacji, a także o usunięcie blokowanych aplikacji. Nie można uruchomić zablokowanych aplikacji na urządzeniu mobilnym użytkownika.

W Kaspersky Security Center Web Console i Cloud Console możesz zarządzać aplikacjami na urządzeniach użytkowników, stosując predefiniowane reguły. Możesz skonfigurować dwa typy reguł **Kontrola aplikacji**: reguły aplikacji i reguły kategorii.

Reguła aplikacji jest stosowana do określonej aplikacji, a **Reguła kategorii** jest stosowana do dowolnej aplikacji należącej do wstępnie zdefiniowanej kategorii. Kategorie aplikacji są określane przez ekspertów firmy Kaspersky.

*Aby skonfigurować **Kontrola aplikacji**:*

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **Sterowanie zabezpieczeniami**.

3. W tabeli w sekcji **Kontrola aplikacji** dodaj reguły, które określą, jakie aplikacje będą kontrolowane.

   - Aby dodać regułę dla określonej aplikacji:

     a. W tabeli kliknij **Reguła aplikacji**.

     b. W otwartym oknie **Reguła aplikacji** wybierz akcję, która zostanie wykonana na aplikacjach objętych utworzoną regułą.

     c. Określ aplikację, która będzie podlegać regule, wypełniając **Odnośnik do pakietu instalacyjnego (np. https://play.google.com/store/apps/details?id=com.kaspersky.kes)**, **Nazwa pakietu (na przykład katana.facebook.com)** i **Nazwa aplikacji**.

     d. Kliknij **Zapisz**.

     Reguła zostanie dodana do listy reguł **Kontrola aplikacji**.

   - Aby dodać regułę dla kategorii aplikacji:

     a. W tabeli w sekcji **Kontrola aplikacji** kliknij **Reguła kategorii**.

     b. W otwartym oknie **Reguła kategorii** wybierz kategorię aplikacji z listy rozwijanej.

     Aplikacje w wybranej kategorii będą podlegać utworzonej regule.

     c. W sekcji **Tryb działania** wybierz akcję, która zostanie wykonana, gdy dowolne aplikacje z wybranej kategorii spróbują się uruchomić: **Zabronione aplikacje** lub **Dozwolone aplikacje**.

     d. W razie potrzeby wypełnij **Dodatkowy komentarz wyświetlany na urządzeniu użytkownika po wykryciu aplikacji z określonej kategorii**.

     e. Kliknij **Zapisz**.

     Reguła zostanie dodana do listy reguł **Kontrola aplikacji**.

4. W sekcji **Akcje z zabronionymi aplikacjami** wybierz czynność wykonywaną dla zabronionych aplikacji:

   - Jeśli chcesz, aby Kaspersky Endpoint Security for Android blokował uruchamianie zabronionych aplikacji na urządzeniu mobilnym użytkownika, wybierz **Blokuj uruchamianie aplikacji**.

   - Jeśli chcesz, żeby Kaspersky Endpoint Security for Android wysyłał dane dotyczące zabronionych aplikacji do dziennika zdarzeń bez ich blokowania, zaznacz pole **Nie blokuj zabronionych aplikacji, tylko raportuj**.

5. W sekcji **Tryb działania** wybierz, czy dodane reguły będą definiować aplikacje dozwolone, czy aplikacje zabronione:

   - Jeśli chcesz, aby reguły określały, które aplikacje są dozwolone, wybierz **Zabronione aplikacje**.

     Jeśli chcesz, żeby Kaspersky Endpoint Security for Android blokował uruchamianie aplikacji systemowych na urządzeniu mobilnym użytkownika (np. Kalendarz, Aparat i Ustawienia) w trybie **Zabronione aplikacje**, zaznacz pole **Blokuj aplikacje systemowe**.

     Eksperci z Kaspersky zalecają włączenie blokowania uruchamiania aplikacji systemowych.

- Jeśli chcesz, aby reguły określały, które aplikacje są zabronione, wybierz **Dozwolone aplikacje**.

6. Aby otrzymywać informacje o wszystkich aplikacjach zainstalowanych na urządzeniach mobilnych, w sekcji **Raport aplikacji** zaznacz pole **Wyślij listę zainstalowanych aplikacji na wszystkich urządzeniach mobilnych**.

   Kaspersky Endpoint Security for Android wysyła dane do dziennika zdarzeń za każdym razem, gdy aplikacja zostaje zainstalowana lub usunięta z urządzenia.

7. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie kontroli zgodności urządzeń mobilnych z firmowymi wymaganiami bezpieczeństwa

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Kontrola zgodności pozwala monitorować urządzenia z systemem Android pod kątem zgodności z firmowymi wymaganiami bezpieczeństwa i podejmować działania w przypadku niezgodności. Firmowe wymagania bezpieczeństwa regulują sposób pracy użytkownika z urządzeniem. Na przykład, ochrona w czasie rzeczywistym musi być włączona na urządzeniu, antywirusowe bazy danych muszą być aktualne, a hasło do urządzenia musi być wystarczająco silne. Kontrola zgodności opiera się na liście reguł. Reguła zgodności obejmuje następujące komponenty:

- Kryterium niezgodności urządzenia.
- Działanie, jakie zostanie podjęte na urządzeniu, jeśli użytkownik nie wyeliminuje niezgodności w określonym przedziale czasu.
- Czas, jaki użytkownik ma na wyeliminowanie braku zgodności (na przykład 24 godziny).

  Po upływie określonego czasu wybrane działanie zostanie wykonane na urządzeniu użytkownika.

  W systemie Android 12 lub nowszych aplikacja może wykonać to zadanie później niż określono, jeśli urządzenie jest w trybie oszczędzania baterii.

Aby skonfigurować kontrolę zgodności, możesz wykonać następujące czynności:

- Włącz lub wyłącz istniejące reguły zgodności.
- Edytuj istniejącą regułę zgodności.
- Dodaj nową regułę.
- Usuń regułę.

Włączanie i wyłączanie reguł zgodności

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Aby włączyć lub wyłączyć istniejące reguły kontroli zgodności urządzeń mobilnych z firmowymi wymaganiami bezpieczeństwa:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **Sterowanie zabezpieczeniami**.

3. W sekcji **Kontrola zgodności** włącz lub wyłącz istniejące reguły zgodności za pomocą przycisków przełączania w kolumnie **Stan**.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Edytowanie reguł zgodności

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Aby edytować regułę kontroli zgodności urządzeń mobilnych z firmowymi wymaganiami bezpieczeństwa:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **Sterowanie zabezpieczeniami**.

3. W sekcji **Kontrola zgodności** wybierz regułę, którą chcesz edytować, a następnie kliknij **Edytuj**.

4. W otwartym oknie **Reguła** edytuj regułę w następujący sposób:

   a. W kolumnie **Akcja** skonfiguruj listę akcji, które zostaną wykonane w przypadku niezgodności z regułą, dodając nowe akcje, edytując istniejące lub usuwając je.

   b. Opcjonalnie określ okres czasu, w którym użytkownik może naprawić niezgodność, używając kolumny **Czas do korekty** dla każdej akcji.

c. Kliknij przycisk **Zapisz**, aby zapisać regułę.

5. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Dodawanie reguł zgodności

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Aby dodać regułę kontrolowania zgodności urządzeń mobilnych z firmowymi wymaganiami bezpieczeństwa:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.
   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **Sterowanie zabezpieczeniami**.

3. W sekcji **Kontrola zgodności** kliknij **Reguła**.

4. W otwartym oknie **Reguła** zdefiniuj regułę w następujący sposób:

   a. Wybierz kryterium niezgodności reguły.

   b. Kliknij **Dodaj**, a następnie w kolumnie **Akcja** wybierz akcję, która zostanie wykonana w przypadku niezgodności z regułą.

   Możesz dodać kilka akcji.

   c. Określ okres czasu, w którym użytkownik może naprawić niezgodność, używając kolumny **Czas do korekty** dla każdej akcji.

   d. Kliknij przycisk **Zapisz**, aby zapisać regułę.

5. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Usuwanie reguł zgodności

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Aby usunąć regułę kontroli zgodności urządzeń mobilnych z firmowymi wymaganiami bezpieczeństwa:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **Sterowanie zabezpieczeniami**.

3. W sekcji **Kontrola zgodności** wybierz regułę, którą chcesz usunąć, a następnie kliknij **Usuń**.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Lista kryteriów niezgodności

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Aby upewnić się, że urządzenie z systemem Android jest zgodne z firmowymi wymaganiami bezpieczeństwa, Kaspersky Endpoint Security for Android może sprawdzić urządzenie pod kątem następujących kryteriów:

- **Ochrona w czasie rzeczywistym jest wyłączona**.

  Ochrona w czasie rzeczywistym musi być włączona.

  Aby uzyskać więcej informacji na temat konfigurowania ochrony w czasie rzeczywistym, zobacz sekcję "Konfigurowanie ochrony w czasie rzeczywistym".

- **Antywirusowe bazy danych są nieaktualne**.

  Antywirusowa baza danych Kaspersky Endpoint Security for Android musi być regularnie aktualizowana.

  Więcej informacji na temat definiowania ustawień aktualizacji antywirusowych baz danych znajduje się w sekcji "Konfigurowanie ochrony antywirusowej".

- **Zainstalowane są zabronione aplikacje**.

  Na urządzeniu nie mogą być zainstalowane aplikacje sklasyfikowane jako **Zablokuj uruchomienie**, jak określono w sekcji **Kontrola aplikacji**.

  Aby uzyskać więcej informacji na temat tworzenia reguł dla aplikacji, zobacz sekcję "Konfigurowanie Kontroli aplikacji".

- **Aplikacje z zabronionych kategorii są zainstalowane**.

  Na urządzeniu nie mogą być zainstalowane aplikacje należące do kategorii sklasyfikowanej jako **Zablokuj uruchomienie**, jak określono w sekcji **Kontrola aplikacji**.

  Aby uzyskać więcej informacji na temat tworzenia reguł dla kategorii aplikacji, zobacz sekcję "Konfigurowanie Kontroli aplikacji".

- **Nie wszystkie wymagane aplikacje są zainstalowane**.

  Na urządzeniu muszą być zainstalowane określone aplikacje sklasyfikowane jako **Wymuś instalację**, zgodnie z opisem w sekcji **Kontrola aplikacji**.

  Aby uzyskać więcej informacji na temat tworzenia reguł dla aplikacji, zobacz sekcję "Konfigurowanie Kontroli aplikacji".

- **Wersja systemu operacyjnego jest nieaktualna**.

  Urządzenie musi posiadać dozwoloną wersję systemu operacyjnego.

  Aby skorzystać z tego kryterium niezgodności, należy określić zakres dozwolonych wersji systemu operacyjnego na listach rozwijanych **Najniższa wersja systemu operacyjnego** i **Najwyższa wersja systemu operacyjnego**.

- **Urządzenie od dłuższego czasu nie było synchronizowane**.

  Urządzenie musi być regularnie synchronizowane z Serwerem administracyjnym.

  Aby skorzystać z tego kryterium niezgodności, należy określić maksymalny odstęp czasu między synchronizacjami urządzeń na liście rozwijanej **Okres synchronizacji**.

- **Urządzenie zostało zrootowane**.

  Urządzenie nie może być zrootowane.

  Aby uzyskać więcej informacji, zobacz sekcję "Wykrywanie hackowania urządzenia (root)".

- **Hasło odblokowujące nie spełnia wymagań bezpieczeństwa**.

  Urządzenie musi być chronione hasłem odblokowującym, które jest zgodne z wymaganiami dotyczącymi siły hasła odblokowującego.

Lista działań w przypadku niezgodności

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Jeśli użytkownik nie wyeliminuje problemu braku zgodności w ciągu określonego czasu, dostępne będą następujące działania:

- **Blokuj wszystkie aplikacje poza systemowymi**.

  Zablokowane jest uruchamianie wszystkich aplikacji na urządzeniu mobilnym użytkownika, za wyjątkiem aplikacji systemowych.

- **Zablokuj urządzenie**.

  Urządzenie mobilne jest zablokowane. Aby uzyskać dostęp do danych, należy odblokować urządzenie. Jeśli przyczyna zablokowania urządzenia nie zostanie usunięta po odblokowaniu urządzenia, urządzenie zostanie zablokowane ponownie po określonym czasie.

- **Usuń dane firmowe**.

  Wyczyść skonteneryzowane dane, firmowe konto e-mail, ustawienia połączenia z firmową siecią Wi-Fi i VPN oraz nazwę punktu dostępu (APN).

- **Pełny reset urządzenia do ustawień fabrycznych**.

  Wszystkie dane zostają usunięte z urządzenia mobilnego i zostają przywrócone ustawienia fabryczne.

Konfigurowanie dostępu użytkownika do stron internetowych

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android i iOS.

Aby chronić dane osobiste i firmowe przechowywane na urządzeniach mobilnych podczas przeglądania internetu, możesz skonfigurować dostęp użytkowników do stron internetowych przy użyciu Ochrony WWW. Ochrona WWW skanuje strony internetowe, zanim użytkownik je otworzy, a następnie blokuje strony rozpowszechniające szkodliwy kod oraz strony służące do wyłudzania informacji, które mają na celu kradzież poufnych danych i uzyskanie dostępu do kont finansowych.

Na urządzeniach z systemem Android funkcja ta obsługuje filtrowanie stron internetowych według kategorii zdefiniowanych w usłudze chmury Kaspersky Security Network. Filtrowanie umożliwia ograniczenie dostępu do pewnych stron internetowych lub kategorii stron internetowych (na przykład do stron z kategorii "**Hazard, loterie, zakłady bukmacherskie**" lub "**Komunikacja przez internet**").

Na urządzeniach z systemem Andoid Ochrona WWW działa tylko w przeglądarkach: Google Chrome, Huawei Browser i Samsung Internet Browser.

Aby zapewnić prawidłowe działanie Ochrony WWW, Kaspersky Endpoint Security for Android musi być ustawiony jako funkcja ułatwień dostępu. Kaspersky Endpoint Security for Android wyświetli pytanie o ustawienie aplikacji jako usługę funkcji Dostępności poprzez Kreator wstępnej konfiguracji. Użytkownik może pominąć ten krok lub wyłączyć tę usługę w ustawieniach urządzenia w późniejszym czasie.

Na urządzeniach z systemem iOS użytkownik musi zezwolić aplikacji Kaspersky Security for iOS na dodanie konfiguracji VPN, aby Ochrona WWW mogła działać.

W celu skonfigurowania dostępu użytkownika do stron internetowych:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **Sterowanie zabezpieczeniami**.

3. W sekcji **Ochrona WWW** zaznacz pole **Włącz Ochronę WWW**, aby włączyć tę funkcję.

4. Na urządzeniach z systemem Andoid możesz ustawić jedną z następujących opcji:

   - Aby ograniczyć dostęp użytkownika do stron internetowych na podstawie ich zawartości:

     a. Wybierz **Blokuj strony z określonych kategorii**.

     b. Zaznacz pola obok kategorii stron internetowych, do których Kaspersky Endpoint Security for Android będzie blokować dostęp.

Jeśli Ochrona WWW jest włączona, dostęp użytkownika do stron internetowych z kategorii **Phishing** i **Strony internetowe ze szkodliwym oprogramowaniem** jest zablokowany.

- Aby określić listę dozwolonych stron internetowych:

  a. Wybierz **Zezwalaj tylko na określone strony internetowe**.

  b. Utwórz listę stron internetowych, dodając adresy stron internetowych, do których aplikacja nie będzie blokowała dostępu. Kaspersky Endpoint Security for Android obsługuje tylko wyrażenia regularne. Podczas wprowadzania adresu dozwolonej strony internetowej należy skorzystać z następującego szablonu:

  - `http:\/\/www\.example\.com.*` — wszystkie strony potomne strony internetowej są dozwolone (na przykład: `http://www.example.com/about`).
  - `https:\/\/.*example\.com` — wszystkie poddomeny strony internetowej są dozwolone (na przykład: `https://pictures.example.com`).

  c. Możesz także użyć wyrażenia `https?`, aby wybrać HTTP i HTTPS. Więcej informacji na temat wyrażeń regularnych można znaleźć na stronie asysty technicznej Oracle.

- Aby zablokować użytkownikom dostęp do wszystkich stron internetowych, wybierz **Blokuj wszystkie strony internetowe**.

5. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie ograniczeń funkcji

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Kaspersky Security Center Web Console umożliwia skonfigurowanie dostępu użytkownika do następujących funkcji urządzeń mobilnych:

- Wi-Fi
- Aparat
- Bluetooth

Domyślnie, użytkownik może korzystać z Wi-Fi, aparatu i Bluetooth na urządzeniu bez ograniczeń.

W celu skonfigurowania ograniczeń korzystania z Wi-Fi, aparatu i Bluetooth na urządzeniu:

1. Otwórz okno właściwości zasady:

- W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

- W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **Sterowanie zabezpieczeniami**.

3. W sekcji **Zarządzanie funkcjami** skonfiguruj korzystanie z Wi-Fi, aparatu i Bluetooth:

   - Aby na urządzeniu mobilnym użytkownika wyłączyć moduł Wi-Fi, zaznacz pole **Zabroń korzystania z Wi-Fi**.

     Na urządzeniach z Androidem 10.0 lub nowszym blokowanie korzystania z sieci Wi-Fi nie jest obsługiwane.

   - Aby na urządzeniu mobilnym użytkownika wyłączyć aparat, zaznacz pole **Zabroń korzystania z aparatu**.

     Na urządzeniach z systemem Android 10.0 lub nowszym nie można całkowicie zabronić korzystania z aparatu.

     Na urządzeniach działających pod kontrolą systemu Android 11 lub nowszego, Kaspersky Endpoint Security for Android musi być ustawiony jako funkcja ułatwień dostępu. Kaspersky Endpoint Security for Android wyświetli pytanie o ustawienie aplikacji jako usługę funkcji Dostępności poprzez Kreator wstępnej konfiguracji. Użytkownik może pominąć ten krok lub wyłączyć tę usługę w ustawieniach urządzenia w późniejszym czasie. W takim przypadku nie będzie można ograniczyć korzystania z aparatu.

   - Aby na urządzeniu mobilnym użytkownika wyłączyć Bluetooth, zaznacz pole **Zabroń korzystania z Bluetooth**.

     Na urządzeniach z systemem Andoid w wersji 12 lub nowszej korzystanie z Bluetooth można wyłączyć tylko, jeśli użytkownik urządzenia przydzielił uprawnienie **Urządzenia Bluetooth w pobliżu**. Użytkownik może przyznać to uprawnienie w trakcie działania Kreatora wstępnej konfiguracji lub później.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Ochrona Kaspersky Endpoint Security for Android przed odinstalowaniem

Aby urządzenie mobilne było chronione i zgodne z firmowymi wymaganiami bezpieczeństwa, możesz włączyć ochronę przed usunięciem Kaspersky Endpoint Security for Android. W tej sytuacji użytkownik nie będzie mógł usunąć aplikacji z poziomu interfejsu Kaspersky Endpoint Security for Android. Podczas dezinstalacji aplikacji przy pomocy narzędzi systemu operacyjnego Android, użytkownikowi zostanie wyświetlone pytanie o wyłączenie uprawnień administratora dla Kaspersky Endpoint Security for Android. Po wyłączeniu uprawnień, urządzenie mobilne zostanie zablokowane.

W celu włączenia ochrony przed odinstalowaniem Kaspersky Endpoint Security for Android:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **Sterowanie zabezpieczeniami**.

3. W sekcji **Zarządzaj aplikacją na urządzeniu mobilnym** usuń zaznaczenie pola **Zezwól na usuwanie z urządzenia Kaspersky Endpoint Security for Android**.

   Aby chronić aplikację przed usunięciem na urządzeniach działających pod kontrolą systemu Android 7.0 lub nowszego, Kaspersky Endpoint Security for Android musi być ustawiony jako usługa funkcji Dostępności. Jeśli Kreator wstępnej konfiguracji jest uruchomiony, Kaspersky Endpoint Security for Android wyświetli pytanie o nadanie aplikacji wszystkich wymaganych uprawnień. Użytkownik może pominąć te kroki lub wyłączyć te uprawnienia w ustawieniach urządzenia w późniejszym czasie. W takim przypadku aplikacja nie jest chroniona przed dezinstalacją.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Jeśli zostanie podjęta próba usunięcia aplikacji, urządzenie mobilne zostanie zablokowane.

Konfigurowanie synchronizacji urządzeń mobilnych z Kaspersky Security Center

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android i iOS.

Aby zarządzać urządzeniami mobilnymi i otrzymywać raporty lub statystyki z urządzeń mobilnych użytkowników, należy zdefiniować ustawienia synchronizacji. Synchronizacja urządzeń mobilnych z Kaspersky Security Center może odbywać się w następujące sposoby:

- **Zgodnie z terminarzem**. Synchronizacja zgodnie z terminarzem odbywa się przy użyciu protokołu HTTP. Terminarz synchronizacji można skonfigurować w ustawieniach zasady. Modyfikacje w ustawieniach zasady, polecenia i zadania będą wykonywane, gdy urządzenia mobilne zostaną zsynchronizowane z Kaspersky Security Center zgodnie z terminarzem, czyli z opóźnieniem. Domyślnie urządzenia mobilne są synchronizowane z Kaspersky Security Center automatycznie co sześć godzin.

  W systemie Android 12 lub nowszych aplikacja może wykonać to zadanie później niż określono, jeśli urządzenie jest w trybie oszczędzania baterii.

- **Wymuszone** (dla urządzeń z systemem Android). Wymuszona synchronizacja odbywa się przy użyciu powiadomień typu push usługi FCM (Firebase Cloud Messaging). Wymuszona synchronizacja jest przeznaczona przede wszystkim do dostarczania w odpowiednim momencie poleceń na urządzenie mobilne. Jeśli chcesz

używać wymuszonej synchronizacji, upewnij się, że ustawienia FCM są skonfigurowane w Kaspersky Security Center.

W celu skonfigurowania synchronizacji urządzenia mobilnego z Kaspersky Security Center:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **Synchronizacja**.

3. W sekcji **Synchronizacja z Serwerem administracyjnym** użyj listy rozwijanej **Okres synchronizacji**, aby wybrać okres synchronizacji.

   Domyślnie synchronizacja jest wykonywana co sześć godzin.

4. Dla urządzeń z systemem Android synchronizację można wyłączyć, gdy urządzenie jest w roamingu. W tym celu zaznacz pole wyboru **Nie synchronizuj podczas roamingu**.

   Domyślnie synchronizacja w roamingu jest włączona.

5. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Kaspersky Security Network

W celu zapewnienia bardziej efektywnej ochrony, Kaspersky Endpoint Security for Android i Kaspersky Security for iOS używają danych zebranych od użytkowników na całym świecie. Usługa *Kaspersky Security Network* została zaprojektowana do przetwarzania tych danych.

Kaspersky Security Network (KSN) jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacjom Kaspersky na zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów.

Uczestnictwo użytkownika w Kaspersky Security Network pomaga firmie Kaspersky uzyskać informacje o typach i źródłach nowych zagrożeń w czasie rzeczywistym, rozwijać metody ich neutralizacji, a także zmniejszyć liczbę fałszywych alarmów. Uczestnictwo w Kaspersky Security Network pozwala również uzyskać dostęp do statystyk reputacji dla aplikacji i stron internetowych.

Jeżeli uczestniczysz w Kaspersky Security Network, zbierane są pewne statystyki w trakcie działania aplikacji, które następnie są automatycznie wysyłane do Kaspersky. Te informacje umożliwiają śledzenie zagrożeń w czasie rzeczywistym. Pliki lub ich części, które mogą zostać wykorzystane przez cyberprzestępców w celu wyrządzenia szkody komputerowi lub zawartości użytkownika, mogą również zostać przesłane do firmy Kaspersky w celu dodatkowego zbadania.

Następujące komponenty aplikacji korzystają z usługi chmurowej Kaspersky Security Network:

- Komponenty antywirus, Ochrona WWW i Kontrola aplikacji w aplikacji Kaspersky Endpoint Security for Android.
- Komponent Ochrona WWW w aplikacji Kaspersky Security for iOS.

Aby rozpocząć używanie KSN, musisz zaakceptować regulamin Umowy licencyjnej z użytkownikiem końcowym. Aby uzyskać więcej informacji o przesyłaniu danych do KSN, sprawdź Wymiana informacji z Kaspersky Security Network.

Odrzucenie możliwości uczestniczenia w KSN zmniejsza poziom ochrony urządzenia, co może doprowadzić do infekcji urządzenia i utraty danych.

Aby udoskonalić działanie aplikacji mobilnej, możesz także przesłać dane statystyczne do Kaspersky Security Network.

Przesyłanie informacji do Kaspersky Security Network jest dobrowolne.

Wymiana informacji z Kaspersky Security Network

Wymiana informacji w Kaspersky Endpoint Security for Android

W celu udoskonalenia ochrony w czasie rzeczywistym, Kaspersky Endpoint Security for Android wykorzystuje usługę chmury Kaspersky Security Network podczas działania następujących komponentów:

- **Anti-Virus.** Aplikacja uzyska dostęp do internetowej bazy wiedzy firmy Kaspersky, zawierającej reputację plików i aplikacji. Skanowanie wyszukuje zagrożenia, o których informacje nie zostały jeszcze dodane do antywirusowych baz danych, ale są już dostępne w KSN. Usługa chmury Kaspersky Security Network zapewnia pełne działanie Antywirusa i zmniejsza prawdopodobieństwo fałszywych alarmów.
- **Ochrona WWW.** Aplikacja wykorzystuje dane pobrane z KSN do skanowania stron internetowych przed ich otwarciem. Aplikacja określa także kategorię strony internetowej do kontrolowania dostępu użytkowników do internetu w oparciu o listy dozwolonych i blokowanych kategorii (na przykład, kategoria "Komunikacja przez internet").
- **Kontrola aplikacji.** Aplikacja określa kategorię aplikacji do ograniczenia uruchamiania aplikacji, które nie spełniają firmowych wymagań bezpieczeństwa, w oparciu o listy dozwolonych i blokowanych kategorii (na przykład, kategoria "Gry").

Informacje dotyczące typu danych wysyłanych do Kaspersky podczas korzystania z KSN w trakcie działania Antywirusa i Kontroli aplikacji są dostępne w Umowie licencyjnej. Akceptując warunki i postanowienia Umowy licencyjnej, wyrażasz zgodę na wysyłanie tych informacji.

Informacje o typie danych przesyłanych do Kaspersky podczas korzystania z KSN w trakcie działania Ochrony WWW są dostępne w Oświadczeniu dotyczącym przetwarzania danych w ramach Ochrony WWW. Akceptując warunki i postanowienia Oświadczenia, wyrażasz zgodę na wysyłanie tych informacji.

Aby uzyskać więcej informacji o przesyłaniu danych do KSN, sprawdź Przesyłanie danych w Kaspersky Endpoint Security for Android.

Podanie danych do KSN jest dobrowolne. Jeśli chcesz, możesz wyłączyć wymianę danych z KSN.

Wymiana informacji w Kaspersky Security for iOS

W celu udoskonalenia ochrony w czasie rzeczywistym, Kaspersky Security for iOS wykorzystuje usługę chmury Kaspersky Security Network podczas działania komponentu **Ochrona WWW**. Aplikacja wykorzystuje dane pobrane z KSN do skanowania zasobów internetowych przed ich otwarciem.

Informacje dotyczące typu danych wysyłanych do Kaspersky podczas korzystania z KSN w trakcie działania Ochrony WWW są dostępne w Umowie licencyjnej użytkownika końcowego. Akceptując warunki i postanowienia Umowy licencyjnej, wyrażasz zgodę na wysyłanie tych informacji.

Aby uzyskać więcej informacji o przesyłaniu danych do KSN, sprawdź Przesyłanie danych w Kaspersky Security for iOS.

Podanie danych do KSN jest dobrowolne. Jeśli chcesz, możesz wyłączyć wymianę danych z KSN.

Wysyłanie statystyk do KSN z aplikacji na Androida i iOS

W celu wymiany danych z KSN w celu udoskonalenia działania aplikacji, muszą być spełnione następujące warunki:

- Użytkownik urządzenia musi przeczytać i zaakceptować warunki Oświadczenia Kaspersky Security Network.
- Musisz skonfigurować ustawienia zasady grupy, aby zezwolić na wysłanie statystyk do KSN.

Możesz zakończyć wysyłanie danych statystycznych do Kaspersky Security Network w dowolnym momencie. Informacje dotyczące typu danych statystycznych wysyłanych do Kaspersky podczas korzystania z KSN w trakcie działania aplikacji mobilnej są dostępne w Oświadczeniu Kaspersky Security Network.

Włączanie i wyłączanie Kaspersky Security Network

Domyślnie korzystanie z Kaspersky Security Network jest włączone.

Jeśli korzystanie z Kaspersky Security Network jest wyłączone, Ochrona WWW, Kontrola aplikacji i dodatkowe zabezpieczenia w Kaspersky Security Network są automatycznie wyłączone, a ich ustawienia stają się niedostępne.

W celu włączenia lub wyłączenia korzystania z Kaspersky Security Network:

1. Otwórz okno właściwości zasady:
   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.
   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.
2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **KSN i statystyki**.
3. Aby włączyć lub wyłączyć korzystanie z Kaspersky Security Network, zaznacz lub odznacz pole **Używaj Kaspersky Security Network**.
4. Jeśli korzystanie z Kaspersky Security Network jest włączone i jeśli zgadzasz się na przesyłanie danych do Kaspersky, zaznacz pole **Zezwól na wysyłanie statystyk do Kaspersky Security Network**. Te dane pomogą aplikacji mobilnej szybciej reagować na zagrożenia, poprawiać wydajność komponentów ochrony i zmniejszać prawdopodobieństwo fałszywych alarmów.

5. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Wymiana informacji z Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Kaspersky Endpoint Security for Android wymienia dane z usługami Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics w celu poprawy jakości, wyglądu i wydajności oprogramowania, produktów, usług i infrastruktury firmy Kaspersky poprzez analizę doświadczenia użytkowników, funkcji, stanu i używanych ustawień urządzenia.

Domyślnie, wymiana informacji z usługami Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics jest wyłączona.

W celu włączenia wymiany danych:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **KSN i statystyki**.

3. W sekcji **Wysyłanie statystyk** zaznacz pole wyboru **Zezwól na przesyłanie danych, aby poprawić jakość, wygląd i wydajność aplikacji**.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie powiadomień na urządzeniach mobilnych

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android.

Jeśli nie chcesz, aby powiadomienia Kaspersky Endpoint Security for Android rozpraszały użytkownika urządzenia mobilnego, możesz wyłączyć pewne powiadomienia.

Kaspersky Endpoint Security używa następujących narzędzi do wyświetlania stanu ochrony urządzenia:

- **Powiadomienie o stanie ochrony**. To powiadomienie jest przypięte do paska powiadomień. Powiadomienie o stanie ochrony nie może zostać usunięte. Powiadomienie wyświetla stan ochrony urządzenia (na przykład:) oraz liczbę problemów (jeśli jakiekolwiek występują). Użytkownik urządzenia może dotknąć stan ochrony urządzenia i wyświetlić listę problemów w aplikacji.

- **Powiadomienia aplikacji**. Te powiadomienia informują użytkownika urządzenia o aplikacji (na przykład: wykryciu zagrożenia).

- **Komunikaty wyskakujące**. Wiadomości wyskakujące wymagają działania ze strony użytkownika urządzenia (na przykład, działanie, jakie należy wykonać po wykryciu zagrożenia).

Domyślnie włączone są wszystkie powiadomienia Kaspersky Endpoint Security for Android.

Użytkownik urządzenia z systemem Android może wyłączyć wszystkie powiadomienia z Kaspersky Endpoint Security for Android w ustawieniach na pasku powiadomień. Jeśli powiadomienia są wyłączone, użytkownik nie monitoruje działania aplikacji i może zignorować ważne informacje (na przykład informacje o błędach podczas synchronizacji urządzenia z Kaspersky Security Center). W takim przypadku, aby sprawdzić stan działania aplikacji, użytkownik musi otworzyć Kaspersky Endpoint Security for Android.

W celu skonfigurowania wyświetlania powiadomień dotyczących działania Kaspersky Endpoint Security for Android na urządzeniu mobilnym:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **Powiadomienia i raporty**.

3. W sekcji **Powiadomienia** skonfiguruj wyświetlanie powiadomień:

   - Aby ukryć wszystkie powiadomienia i wyskakujące wiadomości, wyłącz opcję **Wyświetlaj powiadomienia, gdy Kaspersky Endpoint Security działa w tle**.

     Program Kaspersky Endpoint Security for Android będzie wyświetlał tylko powiadomienia dotyczące stanu ochrony. Powiadomienie wyświetla stan ochrony urządzenia (na przykład,) oraz liczbę problemów. Aplikacja wyświetla również powiadomienia, gdy użytkownik pracuje z aplikacją (na przykład użytkownik ręcznie aktualizuje antywirusowe bazy danych).

     Eksperci z Kaspersky zalecają włączenie powiadomień i powiadomień wyskakujących. Jeśli wyłączysz powiadomienia i wiadomości wyskakujące, gdy aplikacja działa w tle, aplikacja nie ostrzeże użytkowników o zagrożeniach w czasie rzeczywistym. Użytkownicy urządzeń mobilnych mogą poznać stan ochrony urządzenia tylko wtedy, gdy otworzą aplikację.

   - W sekcji **Lista problemów z bezpieczeństwem wyświetlanych na urządzeniach użytkowników** wybierz problemy Kaspersky Endpoint Security for Android, które mają być wyświetlane na urządzeniu mobilnym użytkownika.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Wykrywanie hackowania urządzenia

Kaspersky Security Center Web Console umożliwia wykrywanie hakowania urządzenia (root) na urządzeniach z systemem Android i wykrywania zdjęcia zabezpieczeń systemu na urządzeniach z systemem iOS. Pliki systemowe są niezabezpieczone na zhackowanym urządzeniu i dlatego mogą być modyfikowane. Ponadto aplikacje firm trzecich z nieznanych źródeł mogą być instalowane na zhakowanych urządzeniach. Po wykryciu próby włamania, zalecamy natychmiastowe przywrócenie normalnego działania urządzenia.

Kaspersky Endpoint Security for Android korzysta z następujących usług, aby wykryć sytuację, gdy użytkownik otrzymuje uprawnienia administratora.

- *Wbudowana usługa Kaspersky Endpoint Security for Android.* Usługa firmy Kaspersky, która sprawdza, czy użytkownik urządzenia mobilnego uzyskał uprawnienia roota (Kaspersky Mobile Security SDK).

- *Usługa zaświadczania SafetyNet Attestation.* Jest to usługa Google, która sprawdza integralność systemu operacyjnego, analizuje sprzęt i oprogramowanie urządzenia oraz identyfikuje inne problemy z bezpieczeństwem. Więcej informacji na temat usługi zaświadczania SafetyNet Attestation można znaleźć na stronie Centrum pomocy produktu Android.

Kaspersky Security for iOS korzysta z następujących usług, aby wykryć zdjęcie zabezpieczeń systemu:

- *Wbudowana usługa Kaspersky Security for iOS.* Usługa firmy Kaspersky, która sprawdza, czy na urządzeniu mobilnych nie zniesiono zdjęcia zabezpieczeń systemu (Kaspersky Mobile Security SDK).

Jeśli urządzenie zostało zhakowane, otrzymasz powiadomienie. Powiadomienia o włamaniu możesz przeglądać w Kaspersky Security Center Web Console na zakładce **MONITOROWANIE I RAPORTOWANIE** > **PULPIT.** Możesz także wyłączyć powiadomienia dotyczące włamań w ustawieniach powiadomień o zdarzeniach.

Na urządzeniach Android można nałożyć ograniczenia dotyczące aktywności użytkownika w przypadku, gdy urządzenie zostanie zhakowane (na przykład, zablokować urządzenie). Ograniczenia można nałożyć przy użyciu komponentu Kontrola zgodności. Aby to zrobić, utwórz regułę zgodności z kryterium **Urządzenie zostało zrootowane**

Definiowanie ustawień licencjonowania

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android i iOS.

Aby zarządzać urządzeniami mobilnymi poprzez Kaspersky Security Center Web Console lub Cloud Console, musisz aktywować aplikację mobilną na urządzeniach mobilnych. Aktywacja aplikacji Kaspersky Endpoint Security for Android lub Kaspersky Security for iOS na urządzeniu mobilnym odbywa się poprzez dostarczenie aplikacji informacji o aktualnej licencji. Informacje o licencji są dostarczane na urządzenie mobilne wraz z zasadą, gdy urządzenie zostaje zsynchronizowane z Kaspersky Security Center.

Jeśli aktywacja aplikacji mobilnej nie zostanie zakończona w przeciągu 30 dni od zainstalowania aplikacji na urządzeniu mobilnym, aplikacja zostanie automatycznie przełączona w tryb ograniczonej funkcjonalności. W tym trybie większość komponentów aplikacji nie działa. Po przełączeniu w tryb ograniczonej funkcjonalności aplikacja przestanie wykonywać automatyczną synchronizację z Kaspersky Security Center. Dlatego też, jeśli z jakiegoś powodu aktywacja aplikacji nie zakończyła się w przeciągu 30 dni od zainstalowania aplikacji, użytkownik musi ręcznie zsynchronizować urządzenie z Kaspersky Security Center.

Aby zdefiniować ustawienia licencjonowania zasady grupy:

1. Otwórz okno właściwości zasady:

   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **ZASADY I PROFILE**. Na otwartej liście zasad grupy kliknij nazwę zasady, którą chcesz skonfigurować.
   - W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, wybierz **URZĄDZENIA** > **MOBILNE** > **URZĄDZENIA**. Kliknij urządzenie mobilne objęte zasadą, którą chcesz skonfigurować, a następnie wybierz zasadę na karcie **AKTYWNE ZASADY I PROFILE ZASAD**.

2. Na stronie właściwości zasad wybierz **USTAWIENIA APLIKACJI** > **Licencje**.

3. Użyj listy rozwijanej, aby wybrać wymagany klucz licencyjny z magazynu kluczy Serwera administracyjnego.

   Szczegóły klucza licencyjnego są wyświetlane w poniższych polach.

   > Możesz zastąpić istniejący klucz aktywacyjny na urządzeniu mobilnym, jeśli różni się od klucza wybranego z powyższej listy rozwijalnej. Aby to zrobić, zaznacz pole wyboru **Jeśli klucz na urządzeniu jest inny, zastąp go tym kluczem**.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany wprowadzone w zasadzie i wyjść z okna właściwości zasady.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfiguracja zdarzeń

> Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android i iOS.

Możesz określić ustawienia przechowywania i powiadamiania o zdarzeniach występujących na urządzeniach użytkowników i wysyłanych do Kaspersky Security Center.

> Zdarzenia można konfigurować tylko podczas modyfikowania zasady.

Zdarzenia są podzielone według istotności na następujących kartach:

- **Krytyczne**

  Zdarzenie krytyczne wskazuje na problem, który może prowadzić do utraty danych, nieprawidłowego działania lub błędu krytycznego.

- **Awaria funkcjonalna**

Awaria działania wskazuje na poważny problem, błąd lub awarię, która wystąpiła podczas działania aplikacji.

- **Ostrzeżenie**

  Ostrzeżenie niekoniecznie jest poważne, ale wskazuje na potencjalny problem w przyszłości.

- **Informacyjne**

  Zdarzenie informacyjne informuje o pomyślnym zakończeniu operacji lub procedury lub o prawidłowym działaniu aplikacji.

W każdej sekcji lista zawiera typy zdarzeń i domyślny okres przechowywania zdarzeń w Kaspersky Security Center (w dniach).

Z listy zdarzeń możesz wykonać następujące czynności:

- Dodaj lub usuń typ zdarzenia z listy typów zdarzeń wysyłanych do Kaspersky Security Center.
- Zdefiniuj ustawienia przechowywania i powiadamiania dla każdego typu zdarzenia, na przykład: jak długo zdarzenia tego typu muszą być przechowywane w bazie danych Serwera administracyjnego lub czy będziesz powiadamiany o zdarzeniach tego typu przez e-mail.

Aby uzyskać więcej informacji na temat konfiguracji zdarzeń w Kaspersky Security Center Web Console i Cloud Console:

- Jeśli korzystasz z Kaspersky Security Center Web Console, zapoznaj się z *Pomocą Kaspersky Security Center*.
- Jeśli korzystasz z Kaspersky Security Center Cloud Console, zapoznaj się z *Pomocą Kaspersky Security Center Cloud Console*.

Konfiguracja zdarzeń dotyczących instalacji, aktualizacji i usuwania aplikacji na urządzeniach użytkowników

Te ustawienia zasad możesz zdefiniować wyłącznie dla urządzeń z systemem Android i iOS.

Jeśli korzystasz z Kaspersky Security Center Cloud Console, lista typów zdarzeń występujących na urządzeniach użytkowników i wysyłanych do Kaspersky Security Center nie obejmuje instalacji, aktualizacji ani usuwania aplikacji na urządzeniach. Dzieje się tak, ponieważ takie zdarzenia występują bardzo często i mogą zastąpić inne ważne zdarzenia w bazie danych Kaspersky Security Center po osiągnięciu limitu liczby zdarzeń. Mogą również wpływać na wydajność Serwera administracyjnego lub DBMS oraz przepustowość połączenia internetowego z Kaspersky Security Center Cloud Console.

Jeśli mimo wszystko chcesz przechowywać zdarzenia tego typu i otrzymywać o nich powiadomienia, postępuj zgodnie z opisem w tej sekcji.

W celu skonfigurowania zdarzeń dotyczących instalacji, aktualizacji i usuwania aplikacji na urządzeniach użytkowników:

1. W ustawieniach zasady, w zakładce **KONFIGURACJA ZDARZEŃ**, dodaj typ zdarzenia informacyjnego **Aplikacja została zainstalowana lub usunięta (lista zainstalowanych aplikacji)** do listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.

Więcej informacji na temat konfiguracji zdarzeń znajdziesz w pomocy *Kaspersky Security Center Cloud Console*.

2. Włącz opcję **Wyślij listę zainstalowanych aplikacji na wszystkich urządzeniach mobilnych**.

Zdarzenia dotyczące instalacji, aktualizacji i usuwania aplikacji na urządzeniach użytkowników są przechowywane w bazie danych Kaspersky Security Center. Otrzymasz powiadomienie o tych zdarzeniach.

Obciążenie sieci

Ta sekcja zawiera informacje na temat natężenia ruchu sieciowego wymienianego między urządzeniami mobilnymi i Kaspersky Security Center.

Natężenie ruchu

Zadanie	Wychodzący ruch sieciowy	Przychodzący ruch sieciowy	Całkowity ruch
Początkowe wdrożenie aplikacji, MB	0.08	17.76	17.84
Początkowa aktualizacja antywirusowych baz danych (wielkość ruchu może się różnić ze względu na rozmiar antywirusowych baz danych), MB	0.04	2.21	2.25
Synchronizacja urządzenia mobilnego z Kaspersky Security Center, MB	0.03	0.02	0.05
Regularna aktualizacja antywirusowych baz danych (wielkość ruchu może się różnić ze względu na rozmiar antywirusowych baz danych), MB	0.08	3.06	3.14
Wykonywanie poleceń Anti-Theft. Lokalizacja urządzenia (natężenie ruchu może się różnić ze względu na specyfikację wbudowanej kamery i jakość zdjęć), MB	0.09	0.8	0.17
Wykonywanie poleceń Anti-Theft. Zrób zdjęcie (mugshot), MB	1.0	0.02	1.02
Wykonywanie poleceń Anti-Theft. Blokada urządzenia, MB	0.06	0.05	0.11
Średnia dzienna liczba, MB	0.22	6.96	7.18

Praca w Konsoli administracyjnej opartej na MMC

W tej sekcji Pomocy opisano ochronę i zarządzanie urządzeniami mobilnymi przy użyciu Konsoli administracyjnej opartej na konsoli MMC programu Kaspersky Security Center.

Kluczowe przypadki użycia

INSTALACJA

W jaki sposób zdalnie zainstalować Kaspersky Endpoint Security for Android?

W jaki sposób zablokować możliwość usunięcia Kaspersky Endpoint Security for Android?

W jaki sposób aktywować Kaspersky Endpoint Security for Android?

OCHRONA

W jaki sposób zablokować urządzenie, które zostało skradzione lub zagubione?

W jaki sposób zapewnić sobie ochronę przed zagrożeniami internetowymi?

Jak zabronić używania pustego hasła?

KORZYSTANIE Z ROZWIĄZAŃ FIRM TRZECICH

Android Enterprise (Aplikacje z ikoną teczki, Konfigurowanie profilu roboczego Android)

VMware AirWatch, MobileIron, IBM Maas360, SOTI MobiControl

KONTROLA

W jaki sposób zablokować możliwość grania w gry na urządzeniu?

W jaki sposób skonfigurować dostęp do stron internetowych na urządzeniu?

W jaki sposób wykryć root?

ZARZĄDZANIE

W jaki sposób skonfigurować skrzynkę odbiorczą na urządzeniu?

W jaki sposób połączyć urządzenie mobilne z Wi-Fi?

W jaki sposób zainstalować aplikację korporacyjną?

Informacje o Kaspersky Security for Mobile

Kaspersky Security for Mobile jest zintegorwanym rozwiązaniem do ochrony i zarządzania firmowymi urządzeniami mobilnymi, a także osobistymi urządzeniami mobilnymi używanymi przez pracowników firmy do celów firmowych.

Kaspersky Security for Mobile zawiera następujące moduły:

- Aplikację mobilną Kaspersky Endpoint Security for Android

  Aplikacja Kaspersky Endpoint Security for Android zapewnia ochronę urządzeń mobilnych przed zagrożeniami internetowymi, wirusami i innymi programami, które stanowią zagrożenie.

- Wtyczkę zarządzająca Kaspersky Endpoint Security for Android

  Wtyczka zarządzająca Kaspersky Endpoint Security for Android dostarcza interfejs zarządzania urządzeniami mobilnymi i aplikacjami mobilnymi zainstalowanymi na tych urządzeniach za pośrednictwem Konsoli administracyjnej Kaspersky Security Center.

- Wtyczka zarządzająca Kaspersky Device Management for iOS

  Wtyczka zarządzająca Kaspersky Device Management for iOS umożliwia zdefiniowanie ustawień konfiguracji urządzeń połączonych z Kaspersky Security Center za pośrednictwem protokołu iOS MDM (zwane dalej "urządzenia iOS MDM") oraz za pośrednictwem protokołu Exchange ActiveSync (zwane dalej "urządzenia EAS"), bez korzystania z narzędzia iPhone Configuration Utility lub konsoli Exchange Management Console.

Wtyczki zarządzające są zintegrowane z *systemem zdalnego zarządzania Kaspersky Security Center*. Administrator może używać jednej Konsoli administracyjnej Kaspersky Security Center w celu zarządzania wszystkimi urządzeniami mobilnymi w sieci firmowej, jak również komputerami klienckimi i systemami wirtualnymi. Po podłączeniu urządzeń mobilnych do Serwera administracyjnego jest możliwość zarządzania nimi. Administrator może zdalnie monitorować zarządzane urządzenia.

Aplikacja mobilna Kaspersky Endpoint Security for Android może także działać jako część *systemu zdalnego zarządzania Kaspersky Endpoint Security Cloud*. Więcej informacji na temat pracy z aplikacjami poprzez Kaspersky Endpoint Security Cloud można znaleźć w internetowym systemie *pomocy programu Kaspersky Endpoint Security Cloud*.

Aplikacja mobilna Kaspersky Endpoint Security for Android może także działać jako część rozwiązań EMM firm trzecich uczestniczących w AppConfig Community.

Najważniejsze funkcje zarządzania urządzeniami mobilnymi w Konsoli administracyjnej opartej na MMC

Kaspersky Security for Mobile dostarcza następujące funkcje:

- Rozsyłanie wiadomości e-mail informujących o podłączeniu urządzeń Android z Kaspersky Security Center przy użyciu odnośników Google Play.
- Zdalne połączenie urządzeń mobilnych z Kaspersky Security Center i innymi systemami EMM firm trzecich (na przykład, VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl).
- Zdalna konfiguracja aplikacji Kaspersky Endpoint Security for Android, a także zdalna konfiguracji usług, aplikacji i funkcji urządzeń Android.
- Zdalna konfiguracja urządzeń mobilnych zgodnie z firmowymi wymaganiami bezpieczeństwa.
- Zapobieganie wyciekowi informacji firmowych przechowywanych na urządzeniach mobilnych w przypadku ich zagubienia lub kradzieży (Anti-Theft).
- Kontrolę zgodności z firmowymi wymaganiami bezpieczeństwa (Kontrola zgodności).
- Kontrola korzystania z internetu na urządzeniach mobilnych (Ochrona WWW).
- Konfiguracja poczty firmowej na urządzeniach mobilnych, w tym organizacji z wdrożonym w firmie serwerem pocztowym Microsoft Exchange (tylko dla urządzeń iOS i Samsung).
- Konfiguracja sieci firmowej (Wi-Fi, VPN) umożliwiająca korzystanie z VPN na urządzeniach mobilnych. VPN można skonfigurować tylko na urządzeniach iOS i Samsung.

- Konfigurację stanu urządzenia mobilnego, jaki będzie wyświetlany w Kaspersky Security Center, gdy naruszone zostaną reguły zasady: Krytyczne, Ostrzeżenie, OK.
- Konfiguracja powiadomień wyświetlanych użytkownikowi w aplikacji Kaspersky Endpoint Security for Android.
- Konfigurację ustawień na urządzeniach obsługujących Samsung KNOX 2.6 lub nowszy.
- Konfiguracja ustawień na urządzeniach obsługujących profile robocze Androida.
- Instalowanie Kaspersky Endpoint Security for Android poprzez konsolę Samsung KNOX Mobile Enrollment. Samsung KNOX Mobile Enrollment służy do instalacji wsadowej i wstępnej konfiguracji aplikacji na nowych urządzeniach Samsung zakupionych od oficjalnych dostawców.
- Aktualizacja Kaspersky Endpoint Security for Android do określonej wersji przy użyciu zasad Kaspersky Security Center.
- Powiadomienia administratora o stanie i zdarzeniach aplikacji Kaspersky Endpoint Security for Android mogą być przesyłane w Kaspersky Security Center lub pocztą e-mail.
- Zmiana kontroli ustawień zasady (historia rewizji).

Kaspersky Security for Mobile zawiera następujące komponenty ochrony i zarządzania:

- Antywirus (dla urządzeń z systemem Android)
- Anti-Theft (dla urządzeń z systemem Android)
- Ochrona WWW (dla urządzeń z systemami Android i iOS)
- Kontrola aplikacji (dla urządzeń z systemem Android)
- Kontrola zgodności (dla urządzeń z systemem Android)
- Wykrywanie uprawnień administratora (root) na urządzeniach (dla urządzeń z systemem Android)

Informacje o Kaspersky Endpoint Security for Android

Aplikacja Kaspersky Endpoint Security for Android zapewnia ochronę urządzeń mobilnych przed zagrożeniami internetowymi, wirusami i innymi programami, które stanowią zagrożenie.

Aplikacja Kaspersky Endpoint Security for Android zawiera następujące komponenty:

- **Anti-Virus**. Umożliwia wykrycie i zneutralizowanie zagrożeń na urządzeniu użytkownika przy użyciu antywirusowych baz danych i usługi chmury Kaspersky Security Network. Antywirus zawiera następujące komponenty:
  - Ochrona. Wykrywa zagrożenia w otwieranych plikach, skanuje nowe aplikacje i zapobiega infekcjom urządzenia w czasie rzeczywistym.
  - Skanowanie. Jest uruchamiane na żądanie dla całego systemu plików, tylko dla zainstalowanych aplikacji lub wybranego pliku bądź folderu.
  - Aktualizacja. Aktualizacja umożliwia pobranie nowych antywirusowych baz danych dla aplikacji.

- **Anti-Theft.** Ten moduł chroni informacje na urządzeniu przed nieautoryzowanym dostępem w przypadku zgubienia lub kradzieży urządzenia. Ten moduł umożliwia wysyłanie następujących poleceń do urządzenia:
  - **Zlokalizuj**, aby uzyskać współrzędne lokalizacji urządzenia.
  - **Alarm**, aby urządzenie wydawało głośny alarm.
  - **Mugshot**, aby urządzenie zrobiło zdjęcia przednim aparatem, jeśli ktoś spróbuje je odblokować.
  - **Wyczyść** dane firmowe w celu ochrony poufnych informacji firmowych.
- **Ochrona WWW.** Komponent ten blokuje szkodliwe strony stworzone w celu rozprzestrzeniania się szkodliwego kodu. Ochrona WWW blokuje również fałszywe (phishingowe) strony internetowe stworzone w celu kradzieży poufnych danych użytkownika (na przykład haseł do bankowości elektronicznej bądź systemów płatności elektronicznych) i dostępu do informacji finansowych użytkownika. Ochrona WWW skanuje strony internetowe przed ich otwarciem, korzystając z usługi chmury Kaspersky Security Network. Po skanowaniu, Ochrona WWW zezwala zaufanym stronom internetowym na załadowanie się i blokuje szkodliwe strony internetowe. Ochrona WWW obsługuje również filtrowanie stron internetowych według kategorii zdefiniowanych w usłudze chmury Kaspersky Security Network. To umożliwia administratorowi ograniczenie dostępu użytkownika do pewnych kategorii stron internetowych (na przykład kategorie "Hazard, loterie, zakłady bukmacherskie" lub "Komunikacja przez internet").
- **Kontrola aplikacji.** Komponent ten umożliwia zainstalowanie zalecanych i wymaganych aplikacji na urządzeniu za pośrednictwem bezpośredniego odnośnika do pakietu dystrybucyjnego lub odnośnika do Google Play. Kontrola aplikacji umożliwia usunięcie zablokowanych aplikacji, które naruszają firmowe wymagania bezpieczeństwa.
- **Kontrola zgodności.** Komponent ten umożliwia sprawdzanie zarządzanych urządzeń pod kątem zgodności z firmowymi wymaganiami bezpieczeństwa oraz nakładanie ograniczeń na niektóre funkcje niezgodnych urządzeń.

Informacje o Kaspersky Device Management for iOS

Kaspersky Device Management for iOS zapewnia ochronę i kontrolę urządzeń mobilnych podłączonych do Kaspersky Security Center i obejmuje funkcje zarządzania urządzeniami, takie jak:

- **Ochrona hasłem**. Ta funkcja umożliwia ustawienie wymagań dotyczących złożoności haseł, tak aby użytkownicy używali złożonych haseł zgodnych z firmową polityką haseł.
- **Zarządzanie siecią**. Ta funkcja umożliwia dodawanie zatwierdzonych sieci VPN i Wi-Fi lub ograniczanie dostępu innym osobom.
- **Wyczyść dane firmowe**. W przypadku zgubienia lub kradzieży urządzenia możesz wysłać na to urządzenie polecenie usunięcia danych, aby chronić poufne informacje firmowe.
- **Ochrona WWW**. Komponent ten blokuje szkodliwe strony stworzone w celu rozprzestrzeniania się szkodliwego kodu. Ochrona WWW blokuje również fałszywe (phishingowe) strony internetowe stworzone w celu kradzieży poufnych danych użytkownika (na przykład haseł do bankowości elektronicznej bądź systemów płatności elektronicznych) i dostępu do informacji finansowych użytkownika. Ochrona WWW skanuje strony internetowe przed ich otwarciem, korzystając z usługi chmury Kaspersky Security Network. Po skanowaniu, Ochrona WWW zezwala zaufanym stronom internetowym na załadowanie się i blokuje szkodliwe strony internetowe. Ochrona WWW obsługuje również filtrowanie stron internetowych według kategorii zdefiniowanych w usłudze chmury Kaspersky Security Network. To umożliwia administratorowi ograniczenie dostępu użytkownika do pewnych kategorii stron internetowych (na przykład kategorie "Hazard, loterie, zakłady bukmacherskie" lub "Komunikacja przez internet").

- **Ograniczenia aplikacji.** Ten składnik pozwala kontrolować, czy aplikacje natywne urządzenia, takie jak iTunes, Safari lub Game Center, mogą być używane na nadzorowanym urządzeniu.

- **Ograniczenia funkcji.** Komponent ten umożliwia sprawdzanie zarządzanych urządzeń pod kątem zgodności z firmowymi wymaganiami bezpieczeństwa oraz nakładanie ograniczeń na niektóre funkcje niezgodnych urządzeń.

Informacje o skrzynce pocztowej Exchange

Skrzynka pocztowa Exchange to aplikacja kliencka usługi Exchange ActiveSync. Aplikacja jest przeznaczona do pomocy użytkownikom korporacyjnym w pracy z pocztą, kalendarzem, kontaktami i zadaniami. Skrzynka pocztowa Exchange umożliwia połączenie urządzenia mobilnego z serwerem Microsoft Exchange. Więcej informacji o usłudze Exchange ActiveSync można znaleźć na *stronie pomocy technicznej firmy Microsoft*.

Aby zarządzać urządzeniami mobilnymi przy użyciu protokołu Exchange ActiveSync, serwer Exchange musi być wdrożony na serwerze Microsoft Exchange. Więcej informacji na temat instalowania serwera Exchange można znaleźć pod adresem *pomocy Kaspersky Security Center*. Na urządzeniach mobilnych nie jest wymagana żadna dodatkowa konfiguracja.

Przy pomocy skrzynki pocztowej Exchange możesz zdalnie konfigurować urządzenia EAS, korzystając z zasad grupowych, oraz możesz wysłać polecenie usunięcia danych. Protokół Exchange ActiveSync jest obsługiwany przez następujące systemy operacyjne:

- Windows Mobile
- Windows CE
- Windows Phone
- Android
- Bada
- BlackBerry 10
- iOS
- Symbian

Zestaw ustawień zarządzania dostępny dla urządzenia Exchange ActiveSync zależy od systemu operacyjnego, który jest zainstalowany na urządzeniu mobilnym. Więcej informacji o funkcjach pomocniczych protokołu Exchange ActiveSync dla określonego systemu operacyjnego można znaleźć w dokumentacji dla danego systemu operacyjnego.

Informacje o wtyczce zarządzającej Kaspersky Endpoint Security for Android

Wtyczka zarządzająca Kaspersky Endpoint Security for Android dostarcza interfejs zarządzania urządzeniami mobilnymi i aplikacjami mobilnymi zainstalowanymi na tych urządzeniach za pośrednictwem Konsoli administracyjnej Kaspersky Security Center. Wtyczka zarządzająca Kaspersky Endpoint Security for Android może być używana do:

- Utworzenia grupowych zasad zabezpieczeń dla urządzeń mobilnych.

- Zdalnego skonfigurowania ustawień działania aplikacji Kaspersky Endpoint Security for Android na urządzeniach mobilnych użytkowników.
- Otrzymywania raportów i statystyk dotyczących działania aplikacji mobilnej Kaspersky Endpoint Security for Android na urządzeniach użytkowników.

Wtyczka zarządzająca Kaspersky Endpoint Security for Android jest instalowana domyślnie podczas instalacji Kaspersky Security Center. Wtyczka nie wymaga odrębnej instalacji.

Informacje o wtyczce zarządzającej Kaspersky Device Management for iOS

Wtyczka zarządzająca Kaspersky Device Management for iOS dostarcza interfejs zarządzania urządzeniami mobilnymi podłączonymi przy użyciu protokołu iOS MDM i Exchange ActiveSync za pośrednictwem Konsoli administracyjnej Kaspersky Security Center. Wtyczka zarządzająca Kaspersky Device Management for iOS może zostać użyta do:

- Utworzenia grupowych zasad zabezpieczeń dla urządzeń mobilnych.
- Zdalnego skonfigurowania urządzeń podłączonych przy użyciu protokołu Exchange ActiveSync (zwane dalej również "urządzenia EAS").
- Zdalnego skonfigurowania urządzeń podłączonych przy użyciu protokołu iOS MDM (zwane dalej również "urządzenia iOS MDM").
- Otrzymywania raportów i statystyk dotyczących działania urządzeń mobilnych użytkowników.

Więcej informacji dotyczących podłączenia urządzeń mobilnych do Kaspersky Security Center przy użyciu protokołów iOS MDM i Exchange ActiveSync można znaleźć na stronie *pomocy Kaspersky Security Center*.

Wtyczka zarządzająca Kaspersky Device Management for iOS jest instalowana domyślnie podczas instalacji Kaspersky Security Center. Wtyczka nie wymaga odrębnej instalacji.

Wymagania sprzętowe i programowe

Ta sekcja zawiera wymagania sprzętowe i programowe komputera administratora, który jest używany do instalowania aplikacji na urządzeniach mobilnych, a także systemy operacyjne urządzeń mobilnych, obsługiwane przez Kaspersky Security for Mobile.

Wymagania sprzętowe i programowe komputera administratora

Aby zainstalować kompleksowe rozwiązanie Kaspersky Security for Mobile, komputer administratora musi spełniać wymagania sprzętowe Kaspersky Security Center. Więcej informacji na temat wymagań sprzętowych Kaspersky Security Center można znaleźć w *pomocy Kaspersky Security Center*.

Aby możliwa była praca z wtyczką zarządzającą Kaspersky Endpoint Security for Android, na komputerze administratora musi być zainstalowana Konsola administracyjna Kaspersky Security Center w wersji 12 lub nowszej.

Aby możliwa była praca z wtyczką zarządzającą Kaspersky Device Management for iOS, komputer administratora musi spełniać następujące wymagania programowe:

- Konsola administracyjna Kaspersky Security Center 12 lub nowsza wersja.

- Komponent Serwer Exchange Server.
- Komponent Serwer iOS MDM Server.
- Zestaw instrukcji wersji SSE2 lub bardziej aktualna wersja.

Aby zainstalować aplikację mobilną Kaspersky Endpoint Security for Android z poziomu Serwera administracyjnego, komputer administratora musi spełniać następujące wymagania programowe:

- Kaspersky Security Center 12 lub nowsza wersja
- Wtyczka zarządzająca dla Kaspersky Endpoint Security for Android

Nie ma żadnych wymagań programowych dla instalacji aplikacji mobilnych Kaspersky Endpoint Security for Android z odpowiednich sklepów internetowych.

Aplikacja mobilna Kaspersky Endpoint Security for Android może być także używana jako część systemu zdalnego zarządzania Kaspersky Endpoint Security Cloud (wersja 6.0 i nowsze). Więcej informacji na temat pracy z aplikacjami poprzez Kaspersky Endpoint Security Cloud można znaleźć w *pomocy Kaspersky Endpoint Security Cloud*.

Aplikacja mobilna Kaspersky Endpoint Security for Android może działać w obrębie systemów EMM innych firm:

- VMware AirWatch 9.3 lub nowszy
- MobileIron 10.0 lub nowszy
- IBM MaaS360 10.68 lub nowszy
- Microsoft Intune 1908 lub nowszy
- SOTI MobiControl 14.1.4 (1693) lub nowszy

Wymagania sprzętowe i programowe wobec urządzenia mobilnego użytkownika w celu obsługi instalacji aplikacji Kaspersky Endpoint Security for Android

Aplikacja Kaspersky Endpoint Security for Android posiada następujące wymagania sprzętowe i programowe:

- Smartfon lub tablet z ekranem o rozdzielczości 320x480 pikseli lub wyższej
- 65 MB wolnej przestrzeni w głównej pamięci urządzenia
- Android 5.0–12 (w tym Android 12L, za wyjątkiem Go Edition)
- Architektura procesora x86, x86-64, Arm5, Arm6, Arm7 lub Arm8

Aplikację można zainstalować tylko w pamięci głównej urządzenia.

Wymagania sprzętowe i programowe dla profilu iOS MDM

Dla profilu iOS MDM urządzenie musi spełniać następujące wymagania sprzętowe i programowe:

- iOS 10.0–15.0 lub iPadOS 13–15

- Połączenie z internetem

Znane problemy i uwagi

W Kaspersky Endpoint Security for Android występuje szereg znanych problemów, które nie są krytyczne dla działania aplikacji.

Znane problemy podczas instalowania aplikacji

- Kaspersky Endpoint Security for Android jest instalowany tylko w pamięci głównej urządzenia.
- Na urządzeniach działających pod kontrolą systemu Android 7.0, podczas prób wyłączenia uprawnień administratora dla Kaspersky Endpoint Security for Android w ustawieniach urządzenia może wystąpić błąd, jeśli dla Kaspersky Endpoint Security for Android nie zezwolono na wyświetlanie nad innymi aplikacjami. Ten problem jest spowodowany przez znany błąd w Android 7.
- Kaspersky Endpoint Security for Android zainstalowany na urządzeniach działających pod kontrolą systemu Android 7.0 lub nowszego nie obsługuje trybu wielu okien.
- Kaspersky Endpoint Security for Android nie działa na urządzeniach Chromebook z systemem operacyjnym Chrome.
- Kaspersky Endpoint Security for Android nie działa na urządzeniach z systemami operacyjnymi Android (Go edition).
- Podczas korzystania z aplikacji Kaspersky Endpoint Security for Android z systemami EMM innych producentów (na przykład VMWare AirWatch) dostępne są tylko składniki Antywirus i Ochrona WWW. Administrator może skonfigurować ustawienia Antywirusa i Ochrony WWW w konsoli systemu EMM. W takim przypadku powiadomienia o działaniu aplikacji są dostępne tylko w interfejsie aplikacji Kaspersky Endpoint Security for Android (Raporty).

Znane problemy podczas aktualizacji wersji aplikacji

- Możesz uaktualnić Kaspersky Endpoint Security for Androida tylko do najnowszej wersji aplikacji. Kaspersky Endpoint Security for Android nie może zostać zmieniony na starszą wersję.
- Aby zaktualizować Kaspersky Endpoint Security for Android przy użyciu autonomicznego pakietu instalacyjnego, instalacja aplikacji z nieznanych źródeł musi być dozwolona na urządzeniu mobilnym użytkownika.
- Możesz dokonać aktualizacji za pośrednictwem Google Play, jeśli program Kaspersky Endpoint Security for Android został zainstalowany z poziomu Google Play. Jeśli aplikacja została zainstalowana przy użyciu innej metody, nie możesz przeprowadzić aktualizacji poprzez Google Play.
- Aktualizację można przeprowadzić za pośrednictwem Kaspersky Security Center, jeśli Kaspersky Endpoint Security for Android został zainstalowany za pośrednictwem Kaspersky Security Center. Jeśli aplikacja została zainstalowana z poziomu Google Play, nie możesz jej zaktualizować poprzez Kaspersky Security Center.
- Po uaktualnieniu wtyczek administracyjnych do wersji technicznej 33, aplikacja Kaspersky Endpoint Security for Android musi również zostać zaktualizowana do wersji technicznej 33. W przeciwnym razie nie będzie można aktywować Samsung KNOX na niektórych urządzeniach użytkowników.

Znane problemy z działaniem antywirusa

- Ze względu na ograniczenia techniczne, Kaspersky Endpoint Security for Android nie może skanować plików o rozmiarze 2 GB lub większym. Podczas skanowania aplikacja pomija takie pliki bez informowania o tym fakcie.
- W celu dodatkowej analizy urządzenia pod kątem nowych zagrożeń, których informacje nie zostały jeszcze dodane do antywirusowych baz danych, należy włączyć korzystanie z Kaspersky Security Network. *Kaspersky Security Network (KSN)* jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Aby korzystać z KSN, urządzenie mobilne musi być połączone z internetem.
- W niektórych przypadkach aktualizacja antywirusowych baz danych z Serwera administracyjnego na urządzeniu mobilnym może się nie powieść. W takim przypadku uruchom zadanie aktualizacji antywirusowych baz danych na Serwerze administracyjnym.
- Na niektórych urządzeniach Kaspersky Endpoint Security for Android nie wykrywa urządzeń podłączonych przez USB OTG. Nie jest możliwe uruchomienie skanowania antywirusowego na takich urządzeniach.
- Na urządzeniach z Androidem 11.0 lub nowszym użytkownik musi przyznać uprawnienie "Zezwól na dostęp do zarządzania wszystkimi plikami".
- W przypadku urządzeń działających pod kontrolą systemu Android 7.0 lub nowszego, okno konfiguracji terminarza uruchamiania skanowania antywirusowego może być wyświetlane niepoprawnie (elementy zarządzania nie są wyświetlane). Ten problem jest spowodowany przez znany błąd w Android 7.
- Na urządzeniach z systemem Android 7.0 ochrona w czasie rzeczywistym w trybie rozszerzonym nie wykrywa zagrożeń w plikach przechowywanych na zewnętrznej karcie SD.
- Na urządzeniach działających pod kontrolą systemu Android 6.0, Kaspersky Endpoint Security for Android nie wykrywa pobierania szkodliwego pliku do pamięci urządzenia. Szkodliwy plik może zostać wykryty przez Antywirusa w momencie uruchomienia pliku lub podczas skanowania antywirusowego urządzenia. Ten problem jest spowodowany przez znany błąd w Android 6.0. Aby zapewnić ochronę urządzenia, zalecane jest skonfigurowane zaplanowanych skanowań antywirusowych.

Znane problemy w działaniu ochrony WWW

- Ochrona WWW na urządzeniach z systemem Android działa tylko w przeglądarkach: Huawei Browser, Google Chrome (włączając funkcję Kart niestandardowych) i Samsung Internet Browser. Ochrona WWW dla przeglądarki Samsung Internet Browser nie blokuje stron na urządzeniu mobilnym, jeśli profil roboczy jest używany, a Ochrona WWW jest włączona tylko dla profilu roboczego.
- Kaspersky Endpoint Security w profilu roboczym skanuje tylko domenę strony internetowej w ruchu HTTPS. Szkodliwe i phishingowe strony internetowe mogą pozostać niezablokowane, jeśli aplikacja została zainstalowana w profilu roboczym. Jeśli domena jest zaufana, Ochrona WWW może pominąć zagrożenie (na przykład: `https://trusted.domain.com/phishing/`). Jeśli domena jest niezaufana, Ochrona WWW zablokuje szkodliwe i phishingowe strony internetowe.
- Aby Ochrona WWW działała, musisz włączyć korzystanie z Kaspersky Security Network. Ochrona WWW blokuje strony internetowe na podstawie danych KSN dotyczących reputacji i kategorii stron internetowych.
- Zabronione strony internetowe mogą zostać odblokowane przez Ochronę WWW na urządzeniach z systemem Android 6.0 z zainstalowaną wersją Google Chrome 51 (lub starszą wersją), jeśli witryna jest otwierana w następujący sposób (przyczyną problemu jest dobrze znana wada w Google Chrome):
  - Z wyników wyszukiwania.

- Z listy zakładek.
- Z historii wyszukiwania.
- Przy użyciu funkcji automatycznego uzupełniania adresu internetowego.
- Poprzez otwarcie strony internetowej na nowej karcie w Google Chrome.

- Zabronione strony internetowe mogą pozostać odblokowane w przeglądarce Google Chrome w wersji 50 (lub dowolnej wcześniejszej), jeśli witryna zostanie otwarta z wyników wyszukiwania Google, gdy w ustawieniach przeglądarki włączono funkcję **Połącz karty i aplikacje**. Ten problem jest spowodowany przez znany błąd w Google Chrome.

- Strony internetowe należące do zablokowanych kategorii mogą pozostać odblokowane w Google Chrome, jeśli użytkownik otworzy je z aplikacji innych firm, na przykład, z aplikacji klienta IM. Ten problem jest związany z działaniem usługi dostępności z funkcją Kart niestandardowych w Chrome.

- Zabronione strony internetowe mogą pozostać odblokowane w przeglądarce internetowej Samsung Internet Browser, jeśli użytkownik otworzy je w tle z poziomu menu kontekstowego lub z poziomu aplikacji innych firm, na przykład, z aplikacji klienta IM.

- Kaspersky Endpoint Security for Android musi być ustawiony jako usługa Ułatwień dostępu w celu zapewnienia poprawnego działania Ochrony WWW.

- Podczas wprowadzania adresu strony internetowej w ustawieniach Ochrony WWW miej na uwadze następujące zasady:
  - W przypadku urządzeń z systemem Android określ adres w formacie wyrażeń regularnych (na przykład `http:\/\/www\.przyklad\.com.*`).
  - W przypadku urządzeń iOS MDM określ protokół przesyłania danych HTTP lub HTTPS (na przykład: `http://www.example.com`).

- Dozwolone strony internetowe mogą być blokowane w przeglądarce Samsung Internet Browser, w trybie Ochrony WWW o nazwie **Dozwolone są jedynie strony internetowe znajdujące się na liście** po odświeżeniu strony. Strony internetowe są blokowane, jeśli wyrażenie regularne zawiera ustawienia zaawansowane (na przykład `^https?:\/\/example\.com\/pictures\/`). Zalecane jest stosowanie wyrażeń regularnych bez dodatkowych ustawień (na przykład `^https?:\/\/example\.com`).

Znane problemy w działaniu funkcji Anti-Theft

- W celu terminowego dostarczania poleceń na urządzenia z systemem Android aplikacja korzysta z usługi Firebase Cloud Messaging (FCM). Jeśli usługa FCM nie jest skonfigurowana, polecenia będą dostarczane do urządzenia tylko podczas synchronizacji z Kaspersky Security Center zgodnie z terminarzem zdefiniowanym w zasadzie, na przykład, co 24 godziny.

- Aby zablokować urządzenie, Kaspersky Endpoint Security for Android musi być ustawiony jako administrator urządzenia.

- Aby zablokować urządzenia z systemem Android 7.0 lub nowszym, Kaspersky Endpoint Security for Android musi być ustawiony jako funkcja dostępności.

- Na niektórych urządzeniach polecenie Anti-Theft może się nie uruchomić, jeśli tryb Oszczędzania baterii jest włączony na urządzeniu. Ten problem został potwierdzony na urządzeniu Alcatel 5080X.

- Aby zlokalizować urządzenia działające pod kontrolą systemu Android 10.0 lub nowszego użytkownik musi nadać uprawnienie "Cały czas".
- Aby wykonać zdjęcie złodziejowi przy pomocy urządzeń z systemem Android 11.0 lub nowszym użytkownik musi nadać uprawnienie "Podczas używania aplikacji", aby uzyskać dostęp do aparatu.

Znane problemy w działaniu Kontroli aplikacji

- Kaspersky Endpoint Security for Android musi być ustawiony jako usługa Ułatwień dostępu w celu zapewnienia poprawnego działania Kontroli aplikacji.
- Aby Kontrola aplikacji (kategorie aplikacji) działała, musisz włączyć korzystanie z Kaspersky Security Network. Kontrola aplikacji określa kategorię aplikacji na podstawie danych dostępnych w KSN. Aby korzystać z KSN, urządzenie mobilne musi być połączone z internetem. W Kontroli aplikacji możesz dodawać pojedyncze aplikacje do list zablokowanych i dozwolonych aplikacji. W takim przypadku KSN nie jest wymagany.
- Podczas konfigurowania Kontroli aplikacji zalecane jest odznaczenie pola **Blokuj aplikacje systemowe**. Blokowanie aplikacji systemowych może powodować problemy z działaniem urządzenia.

Znane problemy podczas konfigurowania poczty e-mail

- Zdalna konfiguracja skrzynki pocztowej jest dostępna tylko na następujących urządzeniach:
  - Urządzenia iOS MDM.
  - Urządzenia Samsung (Exchange ActiveSync).
  - Urządzenia z systemem Android z zainstalowanym klientem poczty TouchDown.

    W poprzednich wersjach Kaspersky Endpoint Security for Android możesz użyć Kaspersky Security Center do zdalnego skonfigurowania ustawień profilu TouchDown na urządzeniu użytkownika. Wycofano obsługę TouchDown w Kaspersky Endpoint Security for Android Service Pack 4. Więcej informacji można znaleźć na *stronie pomocy technicznej Symantec*.

    Po zaktualizowaniu wtyczki zarządzającej Kaspersky Endpoint Security for Android, ustawienia TouchDown w zasadzie są ukryte, ale zapisane. Jeśli nowe urządzenia zostaną podłączone, ustawienia TouchDown zostaną skonfigurowane po zastosowaniu zasady.

    Po zmodyfikowaniu i zapisaniu zasady, ustawienia TouchDown zostaną usunięte. Ustawienia TouchDown na urządzeniach użytkownika zostaną wyczyszczone po zastosowaniu zasady.

Znane problemy podczas konfigurowania mocy hasła odblokowującego urządzenie

- Na urządzeniach z Androidem 10.0 lub nowszym Kaspersky Endpoint Security przetwarza wymagania dotyczące mocy hasła na jedną z wartości systemowych: średnią lub wysoką.

  Jeśli wymagana długość hasła wynosi od 1 do 4 symboli, aplikacja prosi użytkownika o ustawienie hasła o średniej mocy. Musi być numeryczne (PIN) bez powtarzających się lub uporządkowanych (np. 1234) sekwencji lub alfanumeryczne. Kod PIN lub hasło musi mieć co najmniej 4 znaki.

Jeśli wymagana długość hasła to 5 lub więcej symboli, aplikacja prosi użytkownika o ustawienie silnego hasła. Musi być numeryczne (PIN) bez powtarzających się lub uporządkowanych sekwencji lub alfanumeryczne (hasło). Kod PIN musi mieć co najmniej 8 cyfr; hasło musi mieć co najmniej 6 znaków.

- Na urządzeniach z Androidem 10.0 lub nowszym odciskiem palca do odblokowywania ekranu można zarządzać tylko w przypadku profilu roboczego.

- Jeśli na urządzeniach działających pod kontrolą systemu Android 7.1.1 hasło odblokowujące nie spełnia firmowych wymagań bezpieczeństwa (Kontrola zgodności), aplikacja systemowa Ustawienia może działać niepoprawnie, gdy zostanie podjęta próba zmiany hasła odblokowującego z poziomu Kaspersky Endpoint Security for Android. Ten problem jest spowodowany przez znany błąd w Android 7.1.1. W tym przypadku, aby zmienić hasło odblokowujące, użyj tylko aplikacji systemowej Ustawienia.

- Na niektórych urządzeniach działających pod kontrolą systemu Android 6.0 lub nowszego może wystąpić błąd podczas wprowadzania hasła odblokowującego ekran, gdy dane na urządzeniu są zaszyfrowane. Ten problem dotyczy określonych funkcji usługi dostępności z oprogramowaniem fabrycznym MIUI.

Znane problemy podczas konfigurowania Wi-Fi

- Na urządzeniach działających pod kontrolą systemu Android w wersji 8.0 lub nowszego, nie można ponownie zdefiniować ustawień serwera proxy dla Wi-Fi przy użyciu zasady. Jednakże możesz ręcznie skonfigurować ustawienia serwera proxy dla sieci Wi-Fi na urządzeniu mobilnym.

Znane problemy podczas konfigurowania APN

- Zdalna konfiguracja APN jest dostępna tylko na urządzeniach iOS MDM lub urządzeniach Samsung.

- Skonfiguruj APN dla urządzeń iOS MDM w sekcji **Komunikacja przez sieci komórkowe**. Sekcja **APN** jest przestarzała. Przed skonfigurowaniem ustawień APN upewnij się, że pole **Zastosuj na urządzeniu** w sekcji **APN** jest odznaczone.

Znane problemy z Zaporą sieciową

- Korzystanie z Zapory sieciowej jest dostępne tylko na urządzeniach Samsung.

Znane problemy podczas konfigurowania VPN

- Zdalna konfiguracja VPN jest dostępna tylko na następujących urządzeniach:
  - Urządzenia iOS MDM.
  - Urządzenia Samsung.

Znane problemy podczas pracy z kontenerami

- W Kaspersky Security for Mobile Service Pack 3 Maintenance Release 2 nie ma już obsługi tworzenia kontenerów dla aplikacji mobilnych. Jednakże kontenery, które zostały utworzone we wcześniejszych wersjach aplikacji, mogą zostać dodane na urządzeniach Android.

- Aby zainstalować aplikacje z kontenera, na urządzeniu mobilnym użytkownika należy zezwolić na instalację aplikacji z nieznanych źródeł. Szczegóły dotyczące instalowania aplikacji bez Google Play można znaleźć w

pomocy Android.

- Konteneryzacja aplikacji nie jest obsługiwana na urządzeniach z systemem Android dla aplikacji, które zawierają więcej niż 65 536 metod (multidex configuration).

Znane problemy z ochroną dezinstalacji aplikacji

- Kaspersky Endpoint Security for Android musi być ustawiony jako administrator urządzenia.
- Aby chronić aplikację przed usunięciem na urządzeniach działających pod kontrolą systemu Android 7.0 lub nowszego, Kaspersky Endpoint Security for Android musi być ustawiony jako usługa funkcji Dostępności.
- Na niektórych urządzeniach Xiaomi i Huawei, ochrona przed usunięciem Kaspersky Endpoint Security for Android nie działa. Ten problem jest spowodowany przez specyficzne funkcje oprogramowania fabrycznego MIUI 7 i 8 na urządzeniach Xiaomi i oprogramowania fabrycznego EMUI na urządzeniach Huawei.

Znane problemy podczas konfigurowania ograniczeń urządzenia

- Na urządzeniach z Androidem 10.0 lub nowszym blokowanie korzystania z sieci Wi-Fi nie jest obsługiwane.
- Na urządzeniach z systemem Android 10.0 lub nowszym nie można całkowicie zabronić korzystania z aparatu.
- Na urządzeniach działających pod kontrolą systemu Android 11 lub nowszego, Kaspersky Endpoint Security for Android musi być ustawiony jako funkcja ułatwień dostępu. Kaspersky Endpoint Security for Android wyświetli pytanie o ustawienie aplikacji jako usługę funkcji Dostępności poprzez Kreator wstępnej konfiguracji. Użytkownik może pominąć ten krok lub wyłączyć tę usługę w ustawieniach urządzenia w późniejszym czasie. W takim przypadku nie będzie można ograniczyć korzystania z aparatu.

Znane problemy podczas wysyłania poleceń na urządzenia mobilne

- Na urządzeniach z systemem Android 12 lub nowszym, jeśli użytkownik przyznał uprawnienie "Użyj przybliżonej lokalizacji", aplikacja Kaspersky Endpoint Security for Android najpierw spróbuje uzyskać dokładną lokalizację urządzenia. Jeśli to się nie powiedzie, przybliżona lokalizacja urządzenia zostanie zwrócona tylko wtedy, gdy została odebrana nie więcej niż 30 minut wcześniej. W przeciwnym razie polecenie **Zlokalizuj urządzenie** nie powiedzie się.

Znane problemy z profilem roboczym Android

- Jeśli tworzysz profil roboczy Androida przy użyciu zasady, użytkownik musi przyznać uprawnienie "Zezwól na dostęp do zarządzania wszystkimi plikami" dla rozwiązania Kaspersky Endpoint Security for Android, które jest zainstalowane na urządzeniach z systemem Android 11 lub nowszym i jest powiązane z profilem roboczym.

Znane problemy z określonymi urządzeniami

- Na niektórych urządzeniach (na przykład Huawei, Meizu i Xiaomi) konieczne jest przyznanie aplikacji Kaspersky Endpoint Security for Android uprawnienia do autostartu lub ręczne dodanie jej do listy aplikacji uruchamianych w momencie uruchamiania systemu operacyjnego. Jeśli aplikacja nie została dodana do listy, Kaspersky Endpoint Security for Android przestaje wykonywać wszystkie swoje funkcje po ponownym uruchomieniu urządzenia mobilnego. Ponadto, jeśli urządzenie zostało zablokowane, nie można użyć polecenia odblokowania urządzenia. Możesz odblokować urządzenie tylko za pomocą jednorazowego kodu odblokowującego.

- Na niektórych urządzeniach (na przykład Meizu i Asus) z Androidem 6.0 lub nowszym, po zaszyfrowaniu danych i ponownym uruchomieniu urządzenia z systemem Android, musisz wprowadzić hasło numeryczne, aby odblokować urządzenie. Jeśli użytkownik używa hasła graficznego do odblokowania urządzenia, należy przekonwertować hasło graficzne na hasło numeryczne. Więcej informacji na temat konwertowania wzoru na hasło numeryczne można znaleźć na stronie działu pomocy technicznej producenta urządzenia mobilnego. Ten problem jest związany z działaniem usługi Ułatwień dostępu.

- Na niektórych urządzeniach Huawei z systemem Android 5.X, po ustawieniu Kaspersky Endpoint Security for Android jako funkcji dostępności może pojawić się niepoprawny komunikat o braku odpowiednich uprawnień. Aby ukryć ten komunikat, włącz aplikację jako aplikację chronioną w ustawieniach urządzenia.

- Na niektórych urządzeniach Huawei z Androidem 5.X lub 6.X, gdy tryb Oszczędzania baterii jest włączony dla Kaspersky Endpoint Security for Android, użytkownik może ręcznie zakończyć aplikację. Urządzenie użytkownika nie będzie już jednak chronione. Ten problem jest spowodowany działaniem niektórych funkcji oprogramowania Huawei. Aby przywrócić ochronę urządzenia, ręcznie uruchom Kaspersky Endpoint Security for Android. Zalecane jest wyłączenie trybu oszczędzania baterii dla Kaspersky Endpoint Security for Android w ustawieniach urządzenia.

- Na urządzeniach Huawei z oprogramowaniem fabrycznym EMUI z systemem Android 7.0 użytkownik może ukryć powiadomienie dotyczące stanu ochrony Kaspersky Endpoint Security for Android. Ten problem jest spowodowany działaniem niektórych funkcji oprogramowania Huawei.

- Na niektórych urządzeniach Xiaomi, podczas ustawiania długości hasła na więcej niż 5 znaków w zasadzie, użytkownik zostanie poproszony o zmianę hasła odblokowania ekranu zamiast kodu PIN. Nie można ustawić kodu PIN, który ma więcej niż 5 znaków. Ten problem jest spowodowany działaniem niektórych funkcji oprogramowania Xiaomi.

- Na urządzeniach Xiaomi z oprogramowaniem fabrycznym MIUI działającym pod kontrolą systemu Android 6.0, ikona programu Kaspersky Endpoint Security for Android może zostać ukryta na pasku stanu. Ten problem jest spowodowany działaniem niektórych funkcji oprogramowania Xiaomi. Zaleca się zezwolenie na wyświetlanie ikon powiadomień w ustawieniach powiadomień.

- Na niektórych urządzeniach Nexus z systemem Android 6.0.1 nie można nadać uprawnień niezbędnych do poprawnego działania z poziomu kreatora wstępnej konfiguracji programu Kaspersky Endpoint Security for Android. Ten problem jest spowodowany przez dobrze znaną wadę poprawki zabezpieczeń dla Androida firmy Google. Aby zapewnić poprawne działanie, wymagane uprawnienia muszą zostać przyznane ręcznie w ustawieniach urządzenia.

- Na pewnych urządzeniach Samsung działających pod kontrolą systemu Android 7.0 lub nowszego, jeśli użytkownik spróbuje skonfigurować nieobsługiwane metody odblokowania urządzenia (na przykład, wzór), urządzenie może zostać zablokowane, gdy spełnione będą następujące warunki: włączona jest ochrona przed dezinstalacją Kaspersky Endpoint Security for Android oraz ustawione są wymagania wobec siły hasła odblokowującego ekran. Aby odblokować urządzenie, należy wysłać specjalne polecenie na urządzenie.

- Na niektórych urządzeniach Samsung niemożliwe jest zablokowanie użycia odcisku palca do odblokowania urządzenia.

- Ochrona WWW nie może zostać włączona na niektórych urządzeniach Samsung, jeśli urządzenie jest połączone z siecią 3G/4G, posiada włączony tryb oszczędzania baterii i ogranicza zużycie danych w tle. Zaleca się wyłączenie funkcji ograniczającej procesy w tle w ustawieniach oszczędzania baterii.

- Na niektórych urządzeniach Samsung, jeśli hasło odblokowujące nie jest zgodne z firmowymi wymaganiami bezpieczeństwa, Kaspersky Endpoint Security for Android nie blokuje użycia odcisku palca do odblokowania ekranu.

- Po wykonaniu poleceń Anti-Theft (takich jak Lokalizacja, Blokada urządzenia, Odblokuj i Zrób zdjęcie (mugshot)), certyfikat ogólny i certyfikat VPN mogą zostać usunięte na niektórych urządzeniach Samsung. Aby móc

kontynuować, należy ponownie zainstalować certyfikaty. Ten problem pojawia się z powodu standardu bezpieczeństwa Mobile Device Fundamentals Protection Profile (MDFPP).

- Na niektórych urządzeniach Honor i Huawei nie można ograniczyć korzystania z Bluetooth. Jeśli Kaspersky Endpoint Security for Android spróbuje ograniczyć korzystanie z Bluetooth, system operacyjny wyświetli powiadomienie zawierające opcje odrzucenia lub zezwolenia na to ograniczenie. Użytkownik może odrzucić to ograniczenie i kontynuować korzystanie z Bluetooth.

- Na niektórych urządzeniach Samsung, po zainstalowaniu lub aktualizacji Kaspersky Endpoint Security z autonomicznego pakietu instalacyjnego, aktywacja profilu KNOX MDM jest niedostępna.

- Na urządzeniach Blackview użytkownik może wyczyścić pamięć aplikacji Kaspersky Endpoint Security for Android. W rezultacie ochrona i zarządzanie urządzeniem są wyłączone, wszystkie zdefiniowane ustawienia stają się nieskuteczne, a aplikacja Kaspersky Endpoint Security for Android zostaje usunięta z funkcji ułatwień dostępu. Dzieje się tak, ponieważ urządzenia tego dostawcy zapewniają dostosowaną aplikację Ostatnie ekrany z podwyższonymi uprawnieniami. Ta aplikacja może nadpisać ustawienia Kaspersky Endpoint Security for Android i nie można jej zastąpić, ponieważ jest częścią systemu operacyjnego Android.

- Na niektórych urządzeniach z systemem Android 11 aplikacja Kaspersky Endpoint Security for Android ulega awarii natychmiast po uruchomieniu. Ten problem jest spowodowany przez znany błąd w Android 11.

Instalacja

Ta sekcja pomocy jest przeznaczona dla specjalistów, którzy instalują Kaspersky Security for Mobile, a także dla specjalistów, którzy oferują pomoc techniczną organizacjom korzystającym z Kaspersky Security for Mobile.

Architektura rozwiązania

Kaspersky Security for Mobile zawiera następujące moduły:

- Aplikację mobilną Kaspersky Endpoint Security for Android

  Aplikacja Kaspersky Endpoint Security for Android zapewnia ochronę urządzeń mobilnych przed zagrożeniami internetowymi, wirusami i innymi programami, które stanowią zagrożenie. Obsługuje interakcję pomiędzy urządzeniem mobilnym a Serwerem administracyjnym Kaspersky Security Center przy użyciu Firebase Cloud Messaging.

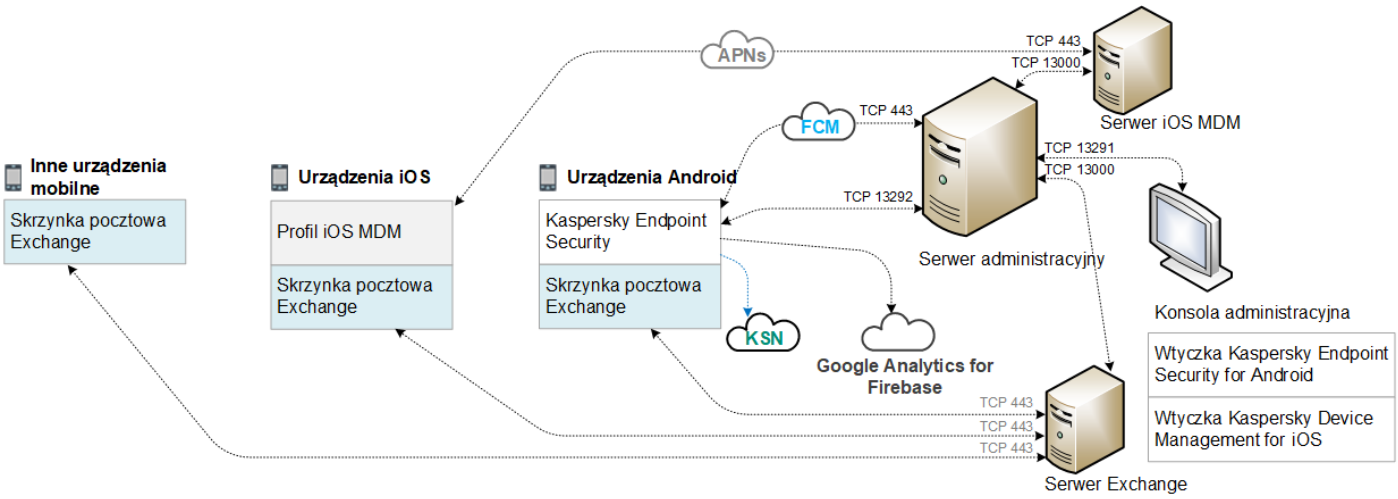
- Wtyczkę zarządzająca Kaspersky Endpoint Security for Android

  Wtyczka zarządzająca Kaspersky Endpoint Security for Android dostarcza interfejs zarządzania urządzeniami mobilnymi i aplikacjami mobilnymi zainstalowanymi na tych urządzeniach za pośrednictwem Konsoli administracyjnej Kaspersky Security Center.

- Wtyczka zarządzająca Kaspersky Device Management for iOS

  Wtyczka zarządzająca Kaspersky Device Management for iOS dostarcza interfejs zarządzania urządzeniami mobilnymi podłączonymi przy użyciu protokołu iOS MDM i Exchange ActiveSync za pośrednictwem Konsoli administracyjnej Kaspersky Security Center.

Architektura zintegrowanego rozwiązania Kaspersky Security for Mobile została przedstawiona na rysunku poniżej.



Architektura Kaspersky Security for Mobile

Więcej informacji na temat Konsoli administracyjnej, Serwera administracyjnego, serwera Exchange i serwera iOS MDM można znaleźć w *pomocy Kaspersky Security Center*.

Standardowe scenariusze instalacji zintegrowanego rozwiązania

Ta sekcja opisuje standardowe scenariusze instalacji zintegrowanego rozwiązania Kaspersky Security for Mobile.

Różne scenariusze wdrażania mogą zostać użyte do zainstalowania zintegrowanego rozwiązania na urządzeniach Android i urządzeniach iOS. Jeśli organizacja używa urządzeń mobilnych działających pod różnymi systemami operacyjnymi, aplikacje powinny zostać zainstalowane dla każdego systemu operacyjnego oddzielnie, postępując zgodnie z odpowiednim scenariuszem instalacji.

Scenariusz zdalnej instalacji Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android można zainstalować na urządzeniach mobilnych w sieci firmowej na kilka sposobów. Możesz użyć scenariusza instalacji najodpowiedniejszego dla Twojej organizacji lub połączyć kilka scenariuszy instalacji.

Szczegółowe informacje na temat wdrażania Kaspersky Endpoint Security for Android w Kaspersky Endpoint Security Cloud można znaleźć w *pomocy programu Kaspersky Endpoint Security Cloud*.

Instalowanie Kaspersky Endpoint Security for Android za pośrednictwem Kaspersky Security Center

Kaspersky Endpoint Security for Android można zainstalować z poziomu Kaspersky Security Center przy użyciu następujących metod:

- Dostarczając wiadomości z odnośnikiem Google Play (zalecane)
- Dostarczając wiadomości z odnośnikiem do autonomicznego pakietu aplikacji

Instalacja Kaspersky Endpoint Security for Android przy pomocy Google Play obejmuje wysłanie wiadomości zawierających odnośnik Google Play do użytkowników urządzeń z Konsoli administracyjnej.

Instalacja Kaspersky Endpoint Security for Android za pośrednictwem pakietu autonomicznego składa się na następujące kroki wykonywane przez administratora:

1. Utworzenie pakietu instalacyjnego aplikacji.
2. Skonfigurowanie ustawień pakietu instalacyjnego.
3. Utworzenie autonomicznego pakietu instalacyjnego.
4. Wysłanie wiadomości z odnośnikiem do pobrania autonomicznego pakietu instalacyjnego do użytkowników urządzeń Android. Masowe wysyłanie wiadomości jest dostępne.

Użytkownik instaluje Kaspersky Endpoint Security for Android na urządzeniu mobilnym po odebraniu wiadomości z odnośnikiem Google Play lub odnośnikiem do pobrania pakietu instalacyjnego z serwera sieciowego Kaspersky Security Center. Do rozpoczęcia korzystania z aplikacji nie są potrzebne żadne dodatkowe przygotowania.

Instalowanie Kaspersky Endpoint Security for Android z poziomu Google Play

Scenariusz zdalnej instalacji z poziomu Google Play jest zalecany w przypadkach, gdy niemożliwe jest przeprowadzenie zdalnej instalacji.

Kaspersky Endpoint Security for Android jest instalowany indywidualnie przez użytkowników z poziomu sklepu Google Play. Użytkownicy pobierają pakiet dystrybucyjny aplikacji mobilnej z Google Play i instalują aplikację na urządzeniach. Po zainstalowaniu aplikacji na urządzeniu, przed rozpoczęciem korzystania z niej konieczne są dodatkowe przygotowania: skonfigurowanie ustawień połączenia z Serwerem administracyjnym i zainstalowanie certyfikatu ogólnego.

Instalowanie Kaspersky Endpoint Security for Android z poziomu KNOX Mobile Enrollment

Wdrożenie Kaspersky Endpoint Security for Android obejmuje dodanie profilu KNOX MDM na urządzeniach mobilnych. Profil KNOX MDM zawiera odnośnik do aplikacji zainstalowanej na serwerze WWW Kaspersky Security Center lub innym serwerze. Po zainstalowaniu aplikacji na urządzeniu mobilnym, należy zainstalować także certyfikat ogólny.

Możesz zapoznać się z informacjami na temat instalacji za pośrednictwem KNOX Mobile Enrollment w sekcji Samsung KNOX.

Scenariusze zdalnego wdrażania profilu iOS MDM

Profil iOS MDM to profil, który zawiera ustawienia połączenia urządzenia mobilnego działającego pod kontrolą systemu iOS z Kaspersky Security Center. Po zainstalowaniu profilu iOS MDM i synchronizacji z Kaspersky Security Center, urządzenie staje się zarządzanym urządzeniem. Urządzenia mobilne są zarządzane poprzez usługę Apple Push Notification (APNs). Szczegółowe informacje na temat instalowania profilu iOS MDM i pracy z certyfikatem APNs można znaleźć w *pomocy Kaspersky Security Center*.

Korzystając z profilu iOS MDM, możesz wykonać następujące czynności:

- Zdalnie skonfigurować ustawienia urządzeń iOS MDM przy pomocy zasad grupowych.
- Wysyłać polecenia usunięcia danych i zablokowania urządzenia.

- Zdalnie instalować aplikacje firmy Kaspersky oraz aplikacje firm trzecich.

Profil iOS MDM można zainstalować na urządzeniach mobilnych w sieci firmowej na kilka sposobów. Możesz użyć scenariusza instalacji najodpowiedniejszego dla Twojej organizacji lub połączyć kilka scenariuszy instalacji.

Przed wdrożeniem profilu iOS MDM administrator musi wykonać następujące czynności:

1. Zainstalować serwer iOS MDM.
2. Uzyskać certyfikat usługi Apple Push Notification Service (certyfikat APNs).
3. Zainstalować certyfikat APNs na serwerze iOS MDM.

Szczegółowe informacje na temat instalowania serwera iOS MDM i pracy z certyfikatem APNs można znaleźć w *pomocy Kaspersky Security Center*.

Szczegółowe informacje na temat wdrażania profilu iOS MDM w Kaspersky Endpoint Security Cloud można znaleźć w *pomocy Kaspersky Endpoint Security Cloud*.

Zdalne instalowanie profilu iOS MDM za pośrednictwem Kaspersky Security Center

Zdalną instalację profilu iOS MDM za pośrednictwem Kaspersky Security Center można przeprowadzić, wysyłając wiadomości zawierające odnośnik do pobrania profilu iOS MDM. Masowe wysyłanie wiadomości jest dostępne.

Użytkownik instaluje profil iOS MDM na urządzeniu mobilnym po otrzymaniu wiadomości z odnośnikiem do serwera sieciowym Kaspersky Security Center Web Server. Nie są wymagane żadne dodatkowe przygotowania dla profilu iOS MDM.

Szczegółowe informacje na temat tworzenia profilu iOS MDM można znaleźć w *pomocy Kaspersky Security Center*.

Przygotowanie Konsoli administracyjnej do instalacji zintegrowanego rozwiązania

Ta sekcja oferuje instrukcje dotyczące przygotowania Konsoli administracyjnej do zainstalowania zintegrowanego rozwiązania.

Konfigurowanie ustawień Serwera administracyjnego dla podłączenia urządzeń mobilnych

Aby urządzenia mobilne mogły nawiązać połączenie z Serwerem administracyjnym, przed zainstalowaniem aplikacji mobilnej Kaspersky Endpoint Security skonfiguruj ustawienia połączenia urządzenia mobilnego we właściwościach Serwera administracyjnego.

W celu skonfigurowania ustawień Serwera administracyjnego dla podłączenia urządzeń mobilnych:

1. W menu kontekstowym Serwera administracyjnego wybierz **Właściwości**.

   Zostanie otwarte okno ustawień Serwera administracyjnego.

2. Wybierz **Ustawienia połączenia z serwerem** → **Porty dodatkowe**.

3. Zaznacz pole **Otwórz port dla urządzeń mobilnych**.

4. W polu **Port dla urządzeń mobilnych** określ port, poprzez który urządzenia mobilne nawiążą połączenie z Serwerem administracyjnym.

   Domyślnie używany jest port 13292. Jeśli pole **Otwórz port dla urządzeń mobilnych** jest odznaczone lub określono zły port połączenia, urządzenia mobilne nie będą mogły nawiązać połączenia z Serwerem administracyjnym.

5. W polu **Port do aktywacji klientów mobilnych** określ port, który będzie używany przez urządzenia mobilne do nawiązania połączenia z Serwerem administracyjnym w celu aktywacji aplikacji Kaspersky Endpoint Security for Android. Domyślnie używany jest port 13292.

6. Kliknij **OK**.

Wyświetlanie folderu Zarządzanie urządzeniami mobilnymi w Konsoli administracyjnej

W folderze **Zarządzanie urządzeniami mobilnymi** w Konsoli administracyjnej możesz wyświetlić listę urządzeń mobilnych zarządzanych przez Serwer administracyjny, skonfigurować ustawienia zarządzania urządzeniami mobilnymi, a także zainstalować certyfikaty na urządzeniach mobilnych użytkowników.

*W celu włączenia wyświetlania folderu **Zarządzanie urządzeniami mobilnymi** w Konsoli administracyjnej:*

1. Z menu kontekstowego Serwera administracyjnego wybierz **Widok → Konfiguracja interfejsu**.

2. W otwartym oknie zaznacz pole **Wyświetl Zarządzanie urządzeniami mobilnymi**.

3. Kliknij **OK**.

Folder **Zarządzanie urządzeniami mobilnymi** jest wyświetlany w drzewie Konsoli administracyjnej po ponownym uruchomieniu Konsoli administracyjnej.

Tworzenie grupy administracyjnej

Aby przeprowadzić scentralizowaną konfigurację aplikacji Kaspersky Endpoint Security for Android zainstalowanej na urządzeniach mobilnych użytkowników, zasady grupy muszą zostać zastosowane do urządzeń.

Aby zastosować zasadę do grupy urządzeń, przed zainstalowaniem aplikacji mobilnych na urządzeniach użytkowników zalecane jest utworzenie oddzielnej grupy dla tych urządzeń w folderze **Zarządzane urządzenia**.

Po utworzeniu grupy administracyjnej zalecane jest skonfigurowanie opcji automatycznego przydzielania do tej grupy urządzeń, na których chcesz zainstalować aplikację. Następnie skonfiguruj ustawienia, które są typowe dla wszystkich urządzeń, korzystając z zasady grupowej.

W celu utworzenia grupy administracyjnej:

1. Z drzewa konsoli wybierz folder **Zarządzane urządzenia**.

2. W obszarze roboczym folderu **Zarządzane urządzenia** lub jego podfolderu wybierz zakładkę **Urządzenia**.

3. Kliknij przycisk **Nowa grupa**.

Zostanie otwarte okno, w którym możesz utworzyć nową grupę.

4. W oknie **Nazwa grupy** wprowadź nazwę grupy i kliknij **OK**.

W drzewie konsoli pojawi się nowy folder grupy administracyjnej o określonej nazwie. Szczegółowe informacje dotyczące używania grup administracyjnych można znaleźć na stronie *pomocy Kaspersky Security Center*.

Tworzenie reguły automatycznego przenoszenia urządzeń do grup administracyjnych

Możesz zdalnie zarządzać ustawieniami aplikacji Kaspersky Endpoint Security for Android zainstalowanej na urządzeniach mobilnych użytkowników tylko wtedy, gdy urządzenia należą do wcześniej utworzonej grupy administracyjnej, dla której skonfigurowano zasadę grupową.

Jeśli reguła automatycznego przydzielania urządzeń mobilnych wykrytych w sieci do grupy administracyjnej nie jest skonfigurowana, podczas pierwszej synchronizacji urządzenia z Serwerem administracyjnym urządzenie jest automatycznie wysyłane do Konsoli administracyjnej, do folderu **Dodatkowe** → **Przeszukiwanie sieci** → **Domeny** → **KES10**. Zasada grupowa nie jest stosowana do tego urządzenia.

W celu utworzenia reguły automatycznego przydzielania urządzeń mobilnych do grupy administracyjnej:

1. Z drzewa konsoli wybierz folder **Urządzenia nieprzypisane**.
2. Z menu kontekstowego folderu **Urządzenia nieprzypisane** wybierz **Właściwości**.

   Zostanie otwarte okno **Właściwości: Urządzenia nieprzypisane**.
3. W sekcji **Przenieś urządzenia** kliknij **Dodaj**, aby uruchomić proces tworzenia reguł automatycznego przydzielania urządzeń do grup administracyjnych.

   Zostanie otwarte okno **Nowa reguła**.
4. Wpisz nazwę reguły.
5. Określ grupę administracyjną, do której urządzenia mobilne powinny zostać przydzielone po zainstalowaniu na nich aplikacji mobilnej Kaspersky Endpoint Security for Android. W tym celu kliknij **Przeglądaj** z prawej strony pola **Grupa, do której zostaną przeniesione urządzenia**, a następnie w otwartym oknie wybierz grupę.
6. W sekcji **Stosowanie reguły** wybierz **Uruchom raz dla każdego urządzenia**.
7. Zaznacz pole **Przenieść tylko urządzenia, które nie są dodane do grup administracyjnych**, aby podczas stosowania reguły, urządzenia mobilne, które zostały przydzielone do innych grup administracyjnych, nie były przydzielane do wybranej grupy.
8. Zaznacz pole **Włącz regułę**, aby reguła była stosowana do nowo wykrytych urządzeń.
9. Otwórz sekcję **Aplikacje** i wykonaj następujące czynności:

   a. Zaznacz pole **Wersja systemu operacyjnego**.

   b. Wybierz jeden lub kilka typów systemów operacyjnych urządzeń przydzielanych do określonej grupy: Android lub iOS.
10. Kliknij **OK**.

Nowo utworzona reguła jest wyświetlana na liście reguł przydzielania urządzeń w sekcji **Przenieś urządzenia** okna właściwości folderu **Urządzenia nieprzypisane**.

Zgodnie z regułą Kaspersky Security Center przypisuje do wybranej grupy wszystkie urządzenia, które spełniają określone wymagania i znajdują się w folderze **Urządzenia nieprzypisane**. Urządzenia mobilne, które wcześniej zostały przydzielone do folderu **Urządzenia nieprzypisane**, mogą zostać ręcznie przydzielone do żądanej grupy administracyjnej folderu **Zarządzane urządzenia**. Szczegółowe informacje dotyczące zarządzania grupami administracyjnymi i działań wykonywanych na nieprzypisanych urządzeniach można znaleźć na stronie *pomocy Kaspersky Security Center*.

Tworzenie certyfikatu ogólnego

Certyfikat ogólny należy utworzyć w Konsoli administracyjnej w celu zidentyfikowania użytkownika urządzenia mobilnego.

W celu utworzenia certyfikatu ogólnego:

1. W drzewie konsoli wybierz folder **Zarządzanie urządzeniami mobilnymi** → **Certyfikaty**.
2. W obszarze roboczym folderu **Certyfikaty** kliknij przycisk **Dodaj certyfikat**, aby uruchomić Kreator instalacji certyfikatu.
3. W oknie **Typ certyfikatu** wybierz opcję **Certyfikat ogólny**.
4. W oknie **Wybór użytkownika** określ użytkowników, dla których chcesz utworzyć certyfikat ogólny.
5. W oknie **Źródło certyfikatu** wybierz metodę, według której tworzony jest certyfikat ogólny.
   - Aby automatycznie utworzyć certyfikat ogólny przy użyciu narzędzi Serwera administracyjnego, wybierz **Określ certyfikat przy użyciu narzędzi serwera administracyjnego**.
   - Aby przypisać wcześniej utworzony certyfikat do użytkownika, wybierz opcję **Określ plik certyfikatu**. Kliknij przycisk **Określ**, aby otworzyć okno **Certyfikat**, w którym wybierz plik certyfikatu.

     Odznacz pole **Opublikuj certyfikat**, jeśli nie chcesz określić typu urządzenia mobilnego i metody powiadamiania użytkownika o utworzeniu certyfikatu.
6. W oknie **Metoda powiadamiania użytkownika** skonfiguruj ustawienia powiadamiania użytkownika urządzenia mobilnego o utworzeniu certyfikatu za pośrednictwem wiadomości tekstowej lub wiadomości e-mail.
7. W oknie **Generowanie certyfikatu** kliknij **Gotowe**, aby zakończyć pracę Kreatora instalacji certyfikatu.

Kreator instalacji certyfikatu utworzy certyfikat ogólny, który użytkownik może zainstalować na urządzeniu mobilnym. Aby uzyskać certyfikat, uruchom synchronizację urządzenia mobilnego z Serwerem administracyjnym. Więcej informacji na temat tworzenia certyfikatów i konfigurowania reguł ich przydzielania można znaleźć na stronie *pomocy Kaspersky Security Center*.

Instalowanie Kaspersky Endpoint Security for Android

Ta sekcja opisuje metody instalacji Kaspersky Endpoint Security for Android w sieci korporacyjnej.

Uprawnienia

Dla wszystkich funkcji aplikacji Kaspersky Endpoint Security for Android żąda wymaganych uprawnień. Kaspersky Endpoint Security for Android wyświetla pytanie o uprawnienia obowiązkowe podczas kończenia działania Kreatora instalacji, a także po zainstalowaniu, a przed korzystaniem z każdej funkcji aplikacji. Jeśli nie zostaną nadane uprawnienia obowiązkowe, nie będzie można zainstalować Kaspersky Endpoint Security for Android.

Na niektórych urządzeniach (na przykład, Huawei, Meizu i Xiaomi) należy ręcznie dodać Kaspersky Endpoint Security for Android do listy aplikacji uruchamianych w momencie uruchamiania systemu operacyjnego. Jeśli aplikacja nie została dodana do listy, Kaspersky Endpoint Security for Android przestaje wykonywać wszystkie swoje funkcje po ponownym uruchomieniu urządzenia mobilnego.

Na urządzeniach z systemem Android 11 lub nowszym musisz **wyłączyć uprawnienia do usuwania, jeśli aplikacja nie jest używana** w ustawieniach systemowych. W przeciwnym razie, gdy aplikacja nie będzie używana przez kilka miesięcy, system automatycznie zresetuje uprawnienia przyznane aplikacji przez użytkownika.

Usunięto obsługę Filtra Połączeń/SMS lub SIM Watch w Kaspersky Endpoint Security for Android Service Pack 4 Update 4 (wersja 10.8.0.103). W tym przypadku Kaspersky Endpoint Security for Android nie pyta użytkownika o uprawnienia zarządzania wiadomościami SMS. Aby włączyć Filtr Połączeń/SMS i wszystkie funkcje SIM Watch, musisz użyć wcześniejszej wersji Kaspersky Endpoint Security for Android.

Uprawnienia wymagane przez Kaspersky Endpoint Security for Android

Uprawnienie	Funkcja aplikacji
Telefon (wymagane tylko dla systemu Android 5.0 – 9.X)	Nawiązanie połączenia z Kaspersky Security Center (ID urządzenia)
Pamięć (wymagane)	Antywirus
Dostęp do zarządzania wszystkimi plikami	Antywirus (tylko dla systemu Android 11 lub nowszego)
Urządzenia Bluetooth w pobliżu (dla Androida w wersji 12 lub nowszej)	Ogranicz korzystanie z Bluetooth
Administrator urządzenia (obowiązkowe)	Anti-Theft – blokada urządzenia (tylko dla systemu Android 5.0 – 6.X)
	Anti-Theft – zrób zdjęcie złodziejowi przy użyciu przedniego aparatu
	Anti-Theft – włączenie alarmu
	Anti-Theft – pełny reset
	Ochrona hasłem
	Ochrona przed odinstalowaniem aplikacji
	Instalowanie certyfikatu bezpieczeństwa
	Kontrola aplikacji
	Zarządzanie KNOX (tylko dla urządzeń Samsung)
	Konfigurowanie Wi-Fi

	Konfigurowanie Exchange ActiveSync
	Ograniczenie korzystania z aparatu, Bluetooth i Wi-Fi
Aparat	Anti-Theft – zrób zdjęcie złodziejowi przy użyciu przedniego aparatu Na urządzeniach działających pod kontrolą systemu Android 11.0 lub nowszego użytkownik musi nadać uprawnienie "Podczas używania aplikacji", gdy zostanie o to poproszony.
Lokalizacja	Anti-Theft – lokalizacja urządzenia Na urządzeniach działających pod kontrolą systemu Android 10.0 lub nowszego użytkownik musi nadać uprawnienie "Cały czas", gdy zostanie o to poproszony.
Dostępność	Anti-Theft – blokada urządzenia (tylko dla systemu Android 7.0 lub nowszego)
	Ochrona WWW
	Kontrola aplikacji
	Ochrona przed odinstalowaniem aplikacji (tylko dla systemu Android 7.0 lub nowszego)
	Wyświetlanie ostrzeżeń Kaspersky Endpoint Security for Android (tylko dla systemu Android 10.0 lub nowszego)
	Ograniczenie korzystania z aparatu (tylko Android 11 lub nowszy)

Instalacja Kaspersky Endpoint Security for Android przy użyciu odnośnika Google Play

Kaspersky Endpoint Security for Android jest instalowany na urządzeniach mobilnych użytkowników, których konta zostały dodane do Kaspersky Security Center. Więcej informacji na temat kont użytkowników w Kaspersky Security Center można znaleźć pod adresem pomocy Kaspersky Security Center.

Kaspersky Security for Mobile umożliwia instalację aplikacji za pośrednictwem Kaspersky Security Center przy użyciu odnośnika Google Play (zalecana metoda).

Użytkownik otrzyma odnośnik do Google Play. Aplikacja może zostać zainstalowana zgodnie ze standardową procedurą instalacji na platformie Android. Dodatkowa konfiguracja Kaspersky Endpoint Security for Android po instalacji nie jest wymagana.

Niektóre urządzenia Huawei i Honor, które nie posiadają usług Google, a tym samym mają dostęp do aplikacji w Google Play. Jeśli niektórzy użytkownicy urządzeń Huawei i Honor nie mogą zainstalować aplikacji z Google Play, powinni otrzymać propozycję zainstalowania aplikacji z Huawei App Gallery.

Odnośnik zawiera następujące dane:

- Ustawienia synchronizacji Kaspersky Security Center.

- Certyfikat ogólny.

- Wskaźnik zaakceptowania warunków i zasad Umowy licencyjnej dla Kaspersky Endpoint Security for Android oraz dodatkowych oświadczeń. Jeśli administrator zaakceptuje warunki Umowy licencyjnej oraz dodatkowe oświadczenia w Konsoli administracyjnej, Kaspersky Endpoint Security for Android pominie krok akcpetacji w trakcie instalacji aplikacji.

W celu zainstalowania Kaspersky Endpoint Security for Android za pośrednictwem Kaspersky Security Center przy użyciu odnośnika Google Play:

1. W drzewie konsoli wybierz **Zarządzanie urządzeniami mobilnymi → Urządzenia mobilne**.

2. W obszarze roboczym folderu **Urządzenia mobilne** kliknij przycisk **Dodaj urządzenie mobilne**.

   Zostanie uruchomiony Kreator podłączania nowego urządzenia mobilnego. Postępuj zgodnie z instrukcjami Kreatora.

3. W oknie **System operacyjny** wybierz **Android**.

   Kaspersky Security Center sprawdza dostępność aktualizacji wtyczki zarządzającej. Jeśli Kaspersky Security Center wykryje aktualizacje, możesz zainstalować nową wersję wtyczki zarządzającej. Po zaktualizowaniu wtyczki zarządzającej możesz zaakceptować warunki Umowy licencyjnej oraz dodatkowe oświadczenia dla Kaspersky Endpoint Security for Android. Jeśli administrator zaakceptuje Umowę licencyjną i dodatkowe oświadczenia w Konsoli administracyjnej, Kaspersky Endpoint Security for Android pominie krok akceptacji w trakcie instalacji aplikacji. Ta funkcja jest dostępna w Kaspersky Security Center w wersji 12.

4. Na stronie **metody instalacji Kaspersky Endpoint Security for Android** wybierz, wybierz metodę instalacji aplikacji **Korzystając z łącza Google Play**.

5. W oknie **Wybierz użytkowników** wybierz jednego lub więcej użytkowników do zainstalowania Kaspersky Endpoint Security for Android na ich urządzeniach mobilnych.

   Jeśli na liście nie ma użytkownika, możesz dodać nowe konto użytkownika bez zamykania Kreatora podłączania nowego urządzenia mobilnego.

6. W oknie **Źródło certyfikatu** wybierz źródło certyfikatu w celu ochrony danych przesyłanych pomiędzy Kaspersky Endpoint Security for Android i Kaspersky Security Center:

   - **Utwórz certyfikat przy użyciu narzędzi Serwera administracyjnego.** W tym przypadku certyfikat zostanie utworzony automatycznie.

   - **Określ plik certyfikatu**. W tym przypadku Twój własny certyfikat musi zostać przygotowany z wyprzedzeniem, a następnie wybrany w oknie Kreatora. Ta opcja nie może zostać użyta, jeśli chcesz zainstalować Kaspersky Endpoint Security for Android na kilku urządzeniach mobilnych. Dla każdego użytkownika należy utworzyć oddzielny certyfikat.

7. W oknie **Metoda powiadamiania użytkownika** wybierz kanał do przekazywania odnośnika do instalacji aplikacji:

   - Aby wysłać odnośnik przez e-mail, wybierz **Wyślij odnośnik do Kaspersky Endpoint Security** i skonfiguruj ustawienia w sekcji **E-mail**. Upewnij się, że adres e-mail jest określony w ustawieniach kont użytkowników.

   - Aby wysłać odnośnik za pomocą wiadomości SMS, wybierz **Wyślij odnośnik do Kaspersky Endpoint Security** i skonfiguruj ustawienia w sekcji **Poprzez SMS**. Upewnij się, że numer telefonu jest określony w ustawieniach kont użytkowników.

   - Aby zainstalować Kaspersky Endpoint Security for Android za pomocą kodu QR, wybierz **Pokaż odnośnik do pakietu instalacyjnego** i zeskanuj kod QR przy użyciu aparatu urządzenia mobilnego.

- Jeśli żadna z wymienionych metod nie jest odpowiednia, wybierz **Pokaż odnośnik do pakietu instalacyjnego → Kopiuj**, aby skopiować do schowka odnośnik do instalacji Kaspersky Endpoint Security for Android. Użyj dowolnej metody, aby dostarczyć odnośnik do instalacji aplikacji. Możesz także skorzystać z innych metod instalacji Kaspersky Endpoint Security for Android.

8. Kliknij **Zakończ**, aby zamknąć Kreator podłączania nowego urządzenia mobilnego.

Po zainstalowaniu Kaspersky Endpoint Security for Android na urządzeniach mobilnych użytkowników, będziesz mógł skonfigurować ustawienia urządzeń i aplikacji, używając zasad grupowych. Możliwe będzie także wysłanie poleceń na urządzenia mobilne w celu ochrony danych w przypadku, gdy urządzenie zostanie zagubione bądź skradzione.

Inne metody instalacji Kaspersky Endpoint Security for Android

Możesz zainstalować Kaspersky Endpoint Security for Android, korzystając z łącza do własnego serwera internetowego lub poinstruować użytkowników, aby ręcznie zainstalowali aplikację.

Ręczna instalacja z Google Play lub Huawei AppGallery

Użytkownicy mogą ręcznie zainstalować Kaspersky Endpoint Security for Android z Google Play lub Huawei AppGallery. Aplikacja może zostać zainstalowana zgodnie ze standardową procedurą instalacji na platformie Android. Użytkownicy używają swoich własnych kont Google do instalacji aplikacji.

Szczegóły na temat procedury instalacji Kaspersky Endpoint Security for Android ze sklepu Google Play można znaleźć na stronie pomocy technicznej Google.

Szczegóły na temat procedury instalacji Kaspersky Endpoint Security for Android ze sklepu Huawei AppGallery można znaleźć na stronie pomocy technicznej HUAWEI.

Niektóre urządzenia Huawei i Honor, które nie posiadają usług Google, a tym samym mają dostęp do aplikacji w Google Play. Jeśli niektórzy użytkownicy urządzeń Huawei i Honor nie mogą zainstalować aplikacji z Google Play, powinni otrzymać propozycję zainstalowania aplikacji z Huawei App Gallery.

Po zainstalowaniu Kaspersky Endpoint Security for Android z poziomu Google Play lub Huawei AppGallery, należy przygotować aplikację do użycia. Proces przygotowania aplikacji do użycia składa się z następujących kroków:

1. Administrator wysyła ustawienia synchronizacji urządzenia mobilnego z Serwerem administracyjnym (adres serwera i numer portu) za pomocą dowolnej dostępnej metody (na przykład przez wysłanie wiadomości e-mail).

2. Użytkownik może skonfigurować ustawienia synchronizacji urządzenia mobilnego z Serwerem administracyjnym podczas działania Kreatora wstępnej konfiguracji lub w ustawieniach Kaspersky Endpoint Security for Android.

3. Administrator tworzy certyfikat ogólny dla użytkownika urządzenia mobilnego użytkownika.

4. Użytkownik otrzymuje automatyczne powiadomienie z prośbą o zainstalowanie certyfikatu ogólnego. Jeśli instalacja zostanie potwierdzona, certyfikat ogólny zostanie instalowany na urządzeniu mobilnym.

Dostęp do internetu powinien być włączony na urządzeniu mobilnym w celu synchronizacji z Serwerem administracyjnym.

Dodatkowe informacje na temat konfiguracji ustawień synchronizacji urządzenia mobilnego z Serwerem administracyjnym i otrzymania certyfikatu ogólnego można znaleźć w Pomocy Kaspersky Security Center.

Podczas następnej synchronizacji urządzenia mobilnego z Serwerem administracyjnym, urządzenie mobilne użytkownika z zainstalowanym programem Kaspersky Endpoint Security for Android zostanie przeniesione do folderu **Dodatkowe** → **Przeszukiwanie sieci** → **Domeny** w grupie administracyjnej, która została określona podczas instalacji aplikacji (domyślną grupą jest **KES10**). Możesz przenieść urządzenie mobilne do grupy administracyjnej, którą utworzyłeś w folderze Zarządzane urządzenia ręcznie lub przy użyciu reguł automatycznego przenoszenia.

Ta metoda instalacji jest przydatna, jeśli chcesz instalować określoną wersję Kaspersky Endpoint Security for Android.

W celu zainstalowania Kaspersky Endpoint Security for Android przy użyciu odnośnika do swojego własnego serwera sieciowego:

1. Utwórz pakiet instalacyjny i skonfiguruj jego ustawienia.

   Pakiet instalacyjny to zestaw plików utworzonych do zdalnej instalacji aplikacji firmy Kaspersky za pośrednictwem Kaspersky Security Center.

2. Utwórz autonomiczny pakiet instalacyjny.

   Autonomiczny pakiet instalacyjny to plik instalacyjny aplikacji mobilnej, który zawiera ustawienia połączenia aplikacji z Serwerem administracyjnym i wskaźnik zaakceptowania warunków i zasad Umowy licencyjnej dla Kaspersky Endpoint Security for Android. Jest on tworzony w oparciu o pakiet instalacyjny Kaspersky Endpoint Security for Android. Autonomiczny pakiet instalacyjny to specjalna wersja pakietu instalacyjnego.

Użytkownik otrzyma odnośnik do serwera sieciowego, na którym znajduje się autonomiczny pakiet instalacyjny dla Kaspersky Endpoint Security for Android. Aby zainstalować aplikację, użytkownik musi uruchomić plik APK. Dodatkowa konfiguracja Kaspersky Endpoint Security for Android po instalacji nie jest wymagana.

Aby zainstalować Kaspersky Endpoint Security for Android przy użyciu swojego własnego serwera sieciowego, instalacja aplikacji z nieznanych źródeł musi być dozwolona na urządzeniu mobilnym użytkownika.

Tworzenie i konfigurowanie pakietu instalacyjnego

Pakiet instalacyjny Kaspersky Endpoint Security for Android to samorozpakowujące się archiwum `sc_package.exe`. Archiwum zawiera pliki wymagane do zainstalowania aplikacji mobilnej na urządzeniach:

- `adb.exe`, `AdbWinApi.dll`, `AdbWinUsbApi.dll` – zestaw plików potrzebnych do zainstalowania Kaspersky Endpoint Security for Android.
- `installer.ini` – plik konfiguracyjny zawierający ustawienia połączenia z Serwerem administracyjnym.
- `KES10_xx_xx_xxx.apk` – plik instalacyjny dla Kaspersky Endpoint Security for Android.
- `kmlisten.exe` – narzędzie dostarczające pakiet instalacyjny aplikacji przy użyciu stacji roboczej.
- `kmlisten.ini` – plik konfiguracyjny zawierający ustawienia narzędzia dostarczającego pakiet instalacyjny.
- `kmlisten.kpd` – plik z opisem aplikacji.

W celu utworzenia pakietu instalacyjnego Kaspersky Endpoint Security for Android:

1. W drzewie konsoli wybierz folder **Dodatkowe** → **Zdalna instalacja** → **Pakiety instalacyjne**.

2. W obszarze roboczym folderu **Pakiety instalacyjne** kliknij przycisk **Utwórz pakiet instalacyjny**.

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

3. W oknie **Wybierz typ pakietu instalacyjnego** kliknij przycisk **Utwórz pakiet instalacyjny dla aplikacji Kaspersky**.

4. W oknie **Określanie nazwy pakietu instalacyjnego** wprowadź nazwę pakietu instalacyjnego, która będzie wyświetlana w obszarze roboczym folderu **Pakiety instalacyjne**.

5. W oknie **Wybierz pakiet instalacyjny aplikacji do zainstalowania** wybierz samorozpakowujące się archiwum `sc_package.exe` znajdujące się w pakiecie dystrybucyjnym.

   Jeśli już rozpakowałeś archiwum, wybierz plik z opisem aplikacji - `kmlisten.kpd`. W polu wejściowym pojawi się nazwa i numer wersji aplikacji.

6. W oknie **Zaakceptuj Umowę licencyjną** przeczytać ze zrozumieniem i zaakceptować warunki Umowy licencyjnej.

   Należy zaakceptować warunki Umowy licencyjnej dotyczące tworzenia pakietu instalacyjnego. Jeśli zaakceptujesz warunki Umowy licencyjnej w Konsoli administracyjnej, Kaspersky Endpoint Security for Android pominie krok akceptacji w trakcie instalacji aplikacji.

   Jeśli zdecydujesz się zatrzymać ochronę urządzeń mobilnych, możesz odinstalować aplikację Kaspersky Endpoint Security for Android i odrzucić Umowę licencyjną dla aplikacji. Więcej informacji na temat odrzucenia Umowy licencyjnej można znaleźć w *pomocy Kaspersky Security Center*.

Po zakończeniu działania kreatora, w obszarze roboczym folderu **Pakiety instalacyjne** pojawi się utworzony pakiet instalacyjny. Pakiety instalacyjne są przechowywane w folderze Pakiety, w folderze współdzielonym na Serwerze administracyjnym.

W celu skonfigurowania ustawień pakietu instalacyjnego:

1. W drzewie konsoli wybierz folder **Dodatkowe** → **Zdalna instalacja** → **Pakiety instalacyjne**.

2. W menu kontekstowym pakietu instalacyjnego Kaspersky Endpoint Security for Android wybierz **Właściwości**.

3. Na zakładce **Ustawienia** określ ustawienia połączenia z Serwerem administracyjnym dla urządzeń mobilnych oraz nazwę grupy administracyjnej, do której urządzenia mobilne zostaną dodane automatycznie po pierwszej synchronizacji z Serwerem administracyjnym. Postępuj zgodnie z poniższymi krokami:

   - W sekcji **Połączenie z Serwerem administracyjnym**, w polu **Adres serwera** wprowadź nazwę Serwera administracyjnego dla urządzeń mobilnych w formacie, jaki został użyty do zainstalowania **Obsługi urządzeń mobilnych** podczas instalacji Serwera administracyjnego.

     W zależności od formatu nazwy Serwera administracyjnego dla komponentu **Obsługa urządzeń mobilnych**, określ nazwę DNS lub adres IP Serwera administracyjnego. W polu **Numer portu SSL** określ numer portu Serwera administracyjnego, który jest otwarty dla połączeń z urządzeniami mobilnymi. Domyślnie używany jest port 13292.

   - W sekcji **Przenoszenie komputerów do grup**, w polu **Nazwa grupy** wprowadź nazwę grupy, do której po pierwszej synchronizacji z Serwerem administracyjnym zostaną dodane urządzenia mobilne (domyślnie **KES10**).

     Określona grupa zostanie automatycznie utworzona w folderze **Dodatkowe** → **Przeszukiwanie sieci** → **Domeny**.

   - W sekcji **Działania podczas instalacji** zaznacz pole **Żądaj adresu e-mail**, jeśli chcesz, żeby aplikacja żądała od użytkowników podania ich firmowych adresów e-mail, gdy aplikacja będzie uruchamiana po raz pierwszy.

Adres e-mail użytkownika jest wykorzystywany do tworzenia nazwy urządzenia mobilnego podczas dodawania go do grupy administracyjnej.

4. W celu zastosowania określonych ustawień kliknij **Zastosuj**.

Tworzenie autonomicznego pakietu instalacyjnego

W celu utworzenia autonomicznego pakietu instalacyjnego:

1. W drzewie konsoli wybierz folder **Dodatkowe → Zdalna instalacja → Pakiety instalacyjne**.
2. Wybierz pakiet instalacyjny Kaspersky Endpoint Security for Android.
3. Z menu kontekstowego pakietu instalacyjnego wybierz **Utwórz autonomiczny pakiet instalacyjny**.

   Zostanie uruchomiony kreator tworzenia autonomicznego pakietu instalacyjnego. Postępuj zgodnie z instrukcjami Kreatora.
4. Skonfiguruj sposoby, w jakie autonomiczne pakiety instalacyjne zostaną rozesłane:

   - Aby wysłać ścieżkę dostępu do utworzonego autonomicznego pakietu instalacyjnego do użytkowników za pośrednictwem poczty elektronicznej, w sekcji **Dalsze działania** kliknij odnośnik **Wyślij odnośnik do autonomicznego pakietu instalacyjnego w wiadomości e-mail**.

     Zostanie otwarte okno edytora wiadomości, a tekst w oknie będzie zawierał ścieżkę dostępu do folderu współdzielonego z autonomicznym pakietem instalacyjnym.

   - Aby umieścić odnośnik do utworzonego autonomicznego pakietu instalacyjnego na swojej stronie firmowej, kliknij odnośnik **Próbka kodu HTML do opublikowania odnośnika na stronie internetowej**.

     Zostanie otwarty plik tmp zawierający odnośniki HTML_RJL.
5. Aby opublikować autonomiczny pakiet instalacyjny na serwerze sieciowym Kaspersky Security Center Web Server i wyświetlić całą listę pakietów autonomicznych dla wybranego pakietu instalacyjnego, w oknie **Działanie Kreatora tworzenia autonomicznego pakietu instalacyjnego zostało pomyślnie zakończone** zaznacz pole **Otwórz listę autonomicznych pakietów instalacyjnych**.

Po zamknięciu kreatora zostanie otwarte okno **Lista pakietów autonomicznych dla pakietu instalacyjnego <nazwa pakietu instalacyjnego>**.

Zostanie otwarte okno **Lista pakietów autonomicznych dla pakietu instalacyjnego <nazwa pakietu instalacyjnego>** zawierające następujące informacje:

- Listę autonomicznych pakietów instalacyjnych.
- Ścieżkę sieciową do folderu współdzielonego w polu **Ścieżka dostępu**.
- Adres pakietu autonomicznego na serwerze sieciowym Kaspersky Security Center Web Server w polu **Adres internetowy**.

Jeśli wysyłasz powiadomienia e-mail, możesz określić adres w polu **Adres internetowy** lub ścieżkę w polu **Ścieżka dostępu** jako zasób, z którego użytkownicy mogą pobrać plik instalacyjny aplikacji. Jeśli wysyłasz powiadomienie tekstowe, musisz określić odnośnik do pobrania pojawiający się w polu **Adres internetowy**.

Zalecane jest skopiowanie adresu utworzonego pakietu autonomicznego do schowka, a następnie wklejenie odnośnika do żądanego pakietu instalacyjnego do powiadomienia tekstowego lub e-mail wysyłanego do użytkowników.

Konfigurowanie ustawień synchronizacji

Aby zarządzać urządzeniami mobilnymi i otrzymywać raporty lub statystyki z urządzeń mobilnych użytkowników, musisz skonfigurować ustawienia synchronizacji. Synchronizacja urządzeń mobilnych z Kaspersky Security Center może odbywać się w następujące sposoby:

- **Zgodnie z terminarzem**. Synchronizacja zgodnie z terminarzem odbywa się przy użyciu protokołu HTTP. Terminarz synchronizacji można skonfigurować w ustawieniach zasady grupy. Modyfikacje w ustawieniach zasady grupy, polecenia i zadania będą wykonywane, gdy urządzenie zostanie zsynchronizowane z Kaspersky Security Center zgodnie z terminarzem, czyli z opóźnieniem. Domyślnie urządzenia mobilne są synchronizowane z Kaspersky Security Center automatycznie co 6 godzin.

  W systemie Android 12 lub nowszych aplikacja może wykonać to zadanie później niż określono, jeśli urządzenie jest w trybie oszczędzania baterii.

- **Wymuszona**. Wymuszona synchronizacja odbywa się przy użyciu powiadomień typu push usługi FCM (Firebase Cloud Messaging). Wymuszona synchronizacja jest przeznaczona przede wszystkim do dostarczania w odpowiednim momencie poleceń na urządzenie mobilne. Jeśli chcesz używać wymuszonej synchronizacji, upewnij się, że ustawienia GSM są skonfigurowane w Kaspersky Security Center. W celu uzyskania więcej informacji, odwiedź stronę pomocy Kaspersky Security Center.

W celu skonfigurowania ustawień synchronizacji urządzenia mobilnego z Kaspersky Security Center:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Synchronizacja**.
5. Na liście rozwijalnej **Synchronizuj** wybierz częstotliwość synchronizacji.
6. Aby wyłączyć synchronizację urządzenia z Kaspersky Security Center podczas roamingu, zaznacz pole **Nie synchronizuj podczas roamingu**.

   Użytkownik urządzenia może ręcznie przeprowadzić synchronizację w ustawieniach aplikacji (→ **Ustawienia** → **Synchronizacja** → **Synchronizuj**).
7. Aby ukryć ustawienia synchronizacji (adres serwera, port i grupę administracyjną) przed użytkownikiem w ustawieniach aplikacji, odznacz pole **Pokaż ustawienia synchronizacji na urządzeniu**. Nie można zmodyfikować ukrytych ustawień.
8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center. Możesz ręcznie zsynchronizować urządzenie mobilne, korzystając ze specjalnego polecenia. Więcej informacji na temat pracy z poleceniami dla urządzeń mobilnych można znaleźć w *Pomocy Kaspersky Security Center*.

Aktywacja aplikacji Kaspersky Endpoint Security for Android

W Kaspersky Security Center licencja może obejmować różne grupy funkcji. Aby mieć pewność, że program Kaspersky Endpoint Security for Android jest w pełni funkcjonalny, licencja dla Kaspersky Security Center zakupiona przez organizację, musi oferować funkcję **Zarządzanie urządzeniami mobilnymi**. Funkcja **Zarządzanie urządzeniami mobilnymi** jest przeznaczona do łączenia urządzeń mobilnych z Kaspersky Security Center i zarządzania nimi.

Szczegółowe informacje na temat licencjonowania Kaspersky Security Center i opcji licencjonowania można znaleźć pod adresem *pomocy Kaspersky Security Center*.

Aktywacja aplikacji Kaspersky Endpoint Security for Android na urządzeniu mobilnym odbywa się poprzez dostarczenie aplikacji ważnych informacji o licencji. Informacje o licencji są dostarczane na urządzenie mobilne wraz z zasadą, gdy urządzenie zostaje zsynchronizowane z Kaspersky Security Center.

Jeśli aktywacja aplikacji Kaspersky Endpoint Security for Android nie zostanie zakończona w przeciągu 30 dni od zainstalowania aplikacji na urządzeniu mobilnym, aplikacja zostanie automatycznie przełączona w tryb ograniczonej funkcjonalności. W tym trybie większość komponentów aplikacji nie działa. Po przełączeniu w tryb ograniczonej funkcjonalności aplikacja przestanie wykonywać automatyczną synchronizację z Kaspersky Security Center. Dlatego też, jeśli z jakiegoś powodu aktywacja aplikacji nie zakończyła się w przeciągu 30 dni od zainstalowania aplikacji, użytkownik musi ręcznie zsynchronizować urządzenie z Kaspersky Security Center.

Jeśli Kaspersky Security Center nie jest zainstalowany w Twojej organizacji lub nie jest dostępny dla urządzeń mobilnych, użytkownicy mogą ręcznie aktywować aplikację Kaspersky Endpoint Security for Android na swoich urządzeniach.

W celu aktywowania Kaspersky Endpoint Security for Android:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Licencjonowanie**.
5. W sekcji **Licencjonowanie** otwórz listę rozwijalną **Klucz** i wybierz żądany klucz aktywacyjny z repozytorium kluczy Serwera administracyjnego Kaspersky Security Center.

   Szczegóły dotyczące aplikacji, dla której licencja została zakupiona, są wyświetlane w polu poniżej.
6. Zaznacz pole **Aktywuj przy pomocy klucza z magazynu Kaspersky Security Center**.

   Jeśli aplikacja została aktywowana bez użycia klucza przechowywanego w magazynie Kaspersky Security Center, Kaspersky Security for Mobile zastąpi ten klucz kluczem aktywacyjnym wybranym z listy **Klucz**.
7. Aby aktywować aplikację na urządzeniu mobilnym użytkownika, zablokuj możliwość wprowadzani zmian w ustawieniach.

8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

   Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Instalowanie profilu iOS MDM

W tej sekcji opisano sposoby wdrażania profili iOS MDM w sieci korporacyjnej.

Przed wdrożeniem profilu iOS MDM administrator musi wykonać następujące czynności:

1. Zainstalować serwer iOS MDM.
2. Uzyskać certyfikat usługi Apple Push Notification Service (certyfikat APNs).
3. Zainstalować certyfikat APNs na serwerze iOS MDM.

Szczegółowe informacje na temat instalowania serwera iOS MDM i pracy z certyfikatem APNs można znaleźć w *pomocy Kaspersky Security Center*.

Szczegółowe informacje na temat wdrażania profilu iOS MDM w Kaspersky Endpoint Security Cloud można znaleźć w *pomocy Kaspersky Endpoint Security Cloud*.

Informacje o trybach zarządzania urządzeniami iOS

System zarządzania urządzeniami iOS można wdrożyć na kilka różnych sposobów. Tryb zarządzania zależy od właściciela urządzenia mobilnego (prywatne lub firmowe) i firmowych wymagań bezpieczeństwa. Możesz wybrać tryb zarządzania najbardziej odpowiedni dla Twojej firmy oraz używać kilku trybów jednocześnie.

Urządzenia nienadzorowane

Nienadzorowane urządzenia iOS to prywatne urządzenia pracowników, które są podłączone do Kaspersky Security Center. W tym trybie użytkownik może korzystać z osobistego Apple ID, pracować z dowolnymi aplikacjami, a także przechowywać prywatne dane na urządzeniu. Możesz użyć zasady grupowej Kaspersky Device Management for iOS, aby skonfigurować dostęp do zasobów firmowych, ustawień zabezpieczeń i innych ustawień. Domyślnie, wszystkie urządzenia iOS są nienadzorowane.

Urządzenia nadzorowane

Nadzorowane urządzenia iOS to urządzenia firmowe, które są podłączone do Kaspersky Security Center. Wstępna konfiguracja urządzenia mobilnego odbywa się w Apple Configurator. *Apple Configurator* to aplikacja zaprojektowana do przygotowania i skonfigurowania urządzeń iOS. Aplikacja Apple Configurator jest instalowana na komputerze działającym pod kontrolą systemu OS X. Więcej informacji na temat pracy z Apple Configurator można znaleźć na stronie pomocy technicznej firmy Apple. Do dalszej konfiguracji możesz użyć zasady grupowej Kaspersky Device Management for iOS. Na urządzeniach nadzorowanych możesz uzyskać dostęp do rozszerzonej grupy ustawień. Na przykład, możesz skonfigurować Globalny serwer pośredniczący HTTP oraz dodatkowe ograniczenia (na przykład, zablokować korzystanie z iMessage i Game Center), a także możesz zablokować modyfikacje konta użytkownika.

Aby pracować z nadzorowanymi i nienadzorowanymi urządzeniami iOS, na serwerze iOS MDM musi być zainstalowany certyfikat APNs, a na urządzeniach mobilnych użytkowników musi być zainstalowany profil iOS MDM.

Instalowanie poprzez Kaspersky Security Center

Profil iOS MDM jest instalowany na urządzeniach mobilnych użytkowników, których konta zostały dodane do Kaspersky Security Center. Więcej informacji na temat kont użytkowników w Kaspersky Security Center można znaleźć pod adresem *pomocy Kaspersky Security Center*.

W celu zainstalowania profilu iOS MDM:

1. W drzewie konsoli wybierz **Zarządzanie urządzeniami mobilnymi** → **Urządzenia mobilne**.
2. W obszarze roboczym folderu **Urządzenia mobilne** kliknij przycisk **Dodaj urządzenie mobilne**.

   Zostanie uruchomiony Kreator podłączania nowego urządzenia mobilnego. Postępuj zgodnie z instrukcjami Kreatora.
3. W oknie **System operacyjny** wybierz **iOS**.
4. W oknie **Metoda ochrony urządzeń iOS MDM** wybierz **Użyj profilu iOS MDM serwera iOS MDM** i z listy wybierz profil iOS MDM.
5. W oknie **Wybierz użytkowników** wybierz jednego lub kilku użytkowników do zainstalowania profilu iOS MDM na ich urządzeniach mobilnych.

   Jeśli na liście nie ma użytkownika, możesz dodać nowe konto użytkownika bez zamykania Kreatora podłączania nowego urządzenia mobilnego.
6. W oknie **Źródło certyfikatu** zaznacz źródło certyfikatu w celu ochrony przesyłania danych między urządzeniem mobilnym a Kaspersky Security Center:

   - **Utwórz certyfikat przy użyciu narzędzi Serwera administracyjnego**. W tym przypadku certyfikat zostanie utworzony automatycznie.
   - **Określ plik certyfikatu**. W tym przypadku Twój własny certyfikat musi zostać przygotowany z wyprzedzeniem, a następnie wybrany w oknie Kreatora. Ta opcja nie może być używana, jeśli chcesz zainstalować profil iOS MDM na kilku urządzeniach mobilnych. Dla każdego użytkownika należy utworzyć oddzielny certyfikat.
7. W oknie **Metoda powiadamiania użytkownika** wybierz kanał do przekazywania odnośnika do instalacji aplikacji:

   - Aby wysłać odnośnik przez e-mail, wybierz **Wyślij odnośnik do profilu iOS MDM** i skonfiguruj ustawienia w sekcji **E-mail**. Upewnij się, że adres e-mail jest określony w ustawieniach kont użytkowników.
   - Aby wysłać odnośnik za pomocą wiadomości SMS, wybierz **Wyślij odnośnik do profilu iOS MDM** i skonfiguruj ustawienia w sekcji **SMS**. Upewnij się, że numer telefonu jest określony w ustawieniach kont użytkowników.
   - Aby zainstalować profil iOS MDM za pomocą kodu QR, wybierz opcję **Pokaż odnośnik do pakietu instalacyjnego** i zeskanuj kod QR za pomocą aparatu w urządzeniu mobilnym.
   - Jeśli żadna z wymienionych metod nie jest odpowiednia, wybierz opcję **Pokaż odnośnik do pakietu instalacyjnego** → **Kopiuj**, aby skopiować odnośnik do instalacji profilu iOS MDM do schowka. Użyj dowolnej metody, aby dostarczyć odnośnik do instalacji aplikacji.
8. Zakończ działanie Kreatora podłączania nowego urządzenia mobilnego.

Po zainstalowaniu profilu iOS MDM na urządzeniach mobilnych, można skonfigurować ustawienia aplikacji przy użyciu zasad grupy. Możliwe będzie także wysłanie poleceń na urządzenia mobilne w celu ochrony danych w przypadku, gdy urządzenie zostanie zagubione bądź skradzione.

Na urządzeniach mobilnych działających pod kontrolą systemu iOS 12.1 lub nowszego musisz ręcznie potwierdzić instalację profilu iOS MDM na urządzeniu mobilnym. Musisz także nadać uprawnienie do zdalnego zarządzania urządzeniem.

Instalowanie wtyczek zarządzających

W celu zarządzania urządzeniami mobilnymi, na stacji roboczej administratora należy zainstalować następujące wtyczki zarządzające:

- Wtyczka zarządzająca Kaspersky Endpoint Security for Android dostarcza interfejs zarządzania urządzeniami mobilnymi i aplikacjami mobilnymi zainstalowanymi na tych urządzeniach za pośrednictwem Konsoli administracyjnej Kaspersky Security Center.
- Wtyczka zarządzająca Kaspersky Device Management for iOS dostarcza interfejs zarządzania urządzeniami mobilnymi podłączonymi przy użyciu protokołu iOS MDM i Exchange ActiveSync za pośrednictwem Konsoli administracyjnej Kaspersky Security Center.

Możesz zainstalować wtyczki zarządzające, korzystając z następujących metod:

- Zainstaluj wtyczkę zarządzającą przy użyciu Kreatora wstępnej konfiguracji programu Kaspersky Security Center.

  Aplikacja automatycznie wyświetli pytanie o uruchomienie Kreatora wstępnej konfiguracji po zainstalowaniu Serwera administracyjnego, przy pierwszym nawiązaniu połączenia z nim. Możesz także ręcznie uruchomić Kreator wstępnej konfiguracji w dowolnym momencie.

  Kreator wstępnej konfiguracji umożliwia zaakceptowanie warunków i zasad Umowy licencyjnej dla aplikacji Kaspersky Endpoint Security for Android w Konsoli administracyjnej. Jeśli administrator zaakceptuje warunki Umowy licencyjnej w Konsoli administracyjnej, Kaspersky Endpoint Security for Android pominie zaakceptowanie kroku w trakcie instalacji aplikacji. Więcej informacji dotyczących Kreatora wstępnej konfiguracji dla Kaspersky Security Center można znaleźć w *Pomocy Kaspersky Security Center*.

- Zainstaluj wtyczkę zarządzającą, korzystając z listy dostępnych pakietów dystrybucyjnych Konsoli administracyjnej Kaspersky Security Center.

  Lista dostępnych pakietów dystrybucyjnych jest aktualizowana automatycznie po opublikowaniu nowych wersji aplikacji firmy Kaspersky.

- Pobierz pakiet dystrybucyjny z zewnętrznego źródła i zainstaluj nową wtyczkę zarządzającą, korzystając z pliku EXE.

  Na przykład, pakiet dystrybucyjny wtyczki zarządzającej może zostać pobrany ze strony internetowej Kaspersky.

Instalowanie wtyczek zarządzających z listy Konsoli administracyjnej

W celu zainstalowania wtyczek zarządzających:

1. W drzewie konsoli wybierz **Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

2. W obszarze roboczym wybierz **Działania dodatkowe → Wyświetl aktualne wersje aplikacji Kaspersky**.

   Spowoduje to otwarcie listy aktualnych wersji aplikacji firmy Kaspersky.

3. W sekcji **Urządzenia mobilne** wybierz wtyczkę **Kaspersky Endpoint Security for Android** lub **Kaspersky Device Management for iOS**.

4. Kliknij przycisk **Pobierz pakiety dystrybucyjne**.

   Pakiet dystrybucyjny wtyczki zostanie pobrany do pamięci komputera (plik EXE).

5. Uruchom plik EXE i postępuj zgodnie z instrukcjami Kreatora instalacji.

Instalowanie wtyczek zarządzających z pakietu dystrybucyjnego

W celu zainstalowania wtyczki zarządzającej Kaspersky Endpoint Security for Android:

Skopiuj plik instalacyjny wtyczki `klcfinst.exe` z pakietu dystrybucyjnego zintegrowanego rozwiązania i uruchom go na stacji roboczej administratora.

Instalacja jest wykonywana przez kreator i nie jest konieczne konfigurowanie ustawień.

W celu zainstalowania wtyczki zarządzającej Kaspersky Device Management for iOS:

Skopiuj plik instalacyjny wtyczki `klmdminst.exe` z pakietu dystrybucyjnego zintegrowanego rozwiązania i uruchom go na stacji roboczej administratora.

Instalacja jest wykonywana przez kreator i nie jest konieczne konfigurowanie ustawień.

Możesz upewnić się, że wtyczki zarządzające są zainstalowana, przeglądając listę zainstalowanych wtyczek zarządzających w oknie właściwości Serwera administracyjnego, w sekcji **Zaawansowane → Szczegóły dotyczące zainstalowanych wtyczek zarządzających dla aplikacji**.

Aktualizowanie poprzedniej wersji aplikacji

Aktualizacja aplikacji musi spełniać następujące wymagania:

- Wersja wtyczki zarządzającej Kaspersky Endpoint Security i wersja aplikacji mobilnej Kaspersky Endpoint Security for Android muszą się zgadzać.

  Numery wersji wtyczki zarządzającej i aplikacji mobilnej można sprawdzić w Informacjach o publikacji dla Kaspersky Security for Mobile.

- Upewnij się, że Kaspersky Security Center spełnia wymagania systemowe Kaspersky Security for Mobile.

- Wtyczki zarządzające Kaspersky Endpoint Security 10.0 Service Pack 2 (wersja 10.6.0.1801) i Kaspersky Device Management for iOS 10.0 Service Pack 2 (wersja 10.6.0.1767), a także późniejsze wersje mogą być automatycznie zaktualizowane do najnowszej wersji. Aktualizacje wcześniejszych wersji wtyczek zarządzających nie są wspierane.

  Aby zaktualizować wtyczki zarządzające wcześniejszych wersji, musisz usunąć zainstalowane wtyczki zarządzające i zasady grupowe, które zostały z nimi utworzone. Następnie zainstaluj nowe wersji wtyczek zarządzających. Więcej informacji na temat usuwania wtyczek zarządzających można znaleźć na *stronie internetowej pomocy technicznej Kaspersky*.

- Używaj tej samej wersji Kaspersky Endpoint Security for Android na wszystkich urządzeniach mobilnych organizacji.

Warunki i postanowienia pomocy technicznej dla wersji Kaspersky Security for Mobile dostępne są na *stronie internetowej pomocy technicznej Kaspersky*.

W celu wyświetlenia wersji i numeru kompilacji wtyczek zarządzających:

1. W drzewie konsoli, w menu kontekstowym Serwera administracyjnego wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego wybierz **Zaawansowane** → **Szczegóły dotyczące zainstalowanych wtyczek zarządzających dla aplikacji**.

   Obszar roboczy wyświetli informacje o zainstalowanych wtyczkach zarządzających w formacie `<Nazwa wtyczki> <Wersja> <Kompilacja>`.

Możesz wyświetlić wersję i numer kompilacji aplikacji Kaspersky Endpoint Security for Android za pomocą następujących metod:

- Jeśli Kaspersky Endpoint Security for Android został zainstalowany z autonomicznego pakietu instalacyjnego, możesz wyświetlić wersję i numer kompilacji aplikacji we właściwościach pakietu.
- Jeśli Kaspersky Endpoint Security for Android został zainstalowany przez Google Play, możesz wyświetlić numer kompilacji w ustawieniach aplikacji (→ **Informacje o aplikacji**).

Aktualizowanie poprzedniej wersji Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android można zaktualizować w następujące sposoby:

- Przy użyciu Google Play. Użytkownik urządzenia mobilnego pobiera najnowszą wersję aplikacji ze sklepu Google Play i instaluje ją na urządzeniu.
- Korzystając z Kaspersky Security Center. Możesz zdalnie zaktualizować wersję aplikacji na urządzeniu, korzystając z systemu do zdalnej administracji Kaspersky Security Center.

Możesz wybrać najodpowiedniejszą dla siebie metodę aktualizacji aplikacji. Możesz użyć tylko jednej metody aktualizacji.

Aktualizowanie aplikacji z poziomu Google Play

Aplikacja może zostać zaktualizowana z poziomu Google Play zgodnie ze standardową procedurą aktualizacji platformy Android. Aby aplikacja została zaktualizowana, należy spełnić następujące warunki:

- Użytkownik urządzenia musi posiadać konto Google.
- Urządzenie musi być podpięte do konta Google.
- Urządzenie musi być podłączone do internetu.

Po pobraniu aplikacji z Google Play, Kaspersky Endpoint Security for Android sprawdzi warunki i zasady Umowy licencyjnej. Jeśli warunki Umowy licencyjnej zostaną zaktualizowane, aplikacja wyśle żądanie do Kaspersky Security Center. Jeśli administrator zaakceptuje Umowę licencyjną w Konsoli administracyjnej, Kaspersky Endpoint Security for Android pominie zaakceptowanie kroku w trakcie instalacji aplikacji. Jeśli administrator korzysta z nieaktualnej wersji wtyczki zarządzającej Kaspersky Security Center poprosi o aktualizację wtyczki zarządzającej. Podczas aktualizacji wtyczki zarządzającej administrator może zaakceptować warunki Umowy licencyjnej w Konsoli administracyjnej dla Kaspersky Endpoint Security for Android.

Możesz dokonać aktualizacji aplikacji za pośrednictwem Google Play, jeśli program Kaspersky Endpoint Security for Android został zainstalowany z poziomu Google Play. Jeśli aplikacja została zainstalowana przy użyciu innej metody, nie możesz przeprowadzić aktualizacji aplikacji poprzez Google Play.

Aktualizowanie aplikacji poprzez Kaspersky Security Center

Program Kaspersky Endpoint Security for Android można zaktualizować przy użyciu Kaspersky Security Center po zastosowaniu zasady grupowej. W ustawieniach zasady grupowej możesz wybrać autonomiczny pakiet instalacyjny Kaspersky Endpoint Security for Android w wersji, która spełnia firmowe wymagania bezpieczeństwa.

Aktualizację można przeprowadzić za pośrednictwem Kaspersky Security Center, jeśli Kaspersky Endpoint Security for Android został zainstalowany za pośrednictwem Kaspersky Security Center. Jeśli aplikacja została zainstalowana z poziomu Google Play, nie możesz jej zaktualizować poprzez Kaspersky Security Center.

Aby zaktualizować Kaspersky Endpoint Security for Android przy użyciu autonomicznego pakietu instalacyjnego, instalacja aplikacji z nieznanych źródeł musi być dozwolona na urządzeniu mobilnym użytkownika. Szczegóły dotyczące instalowania aplikacji bez Google Play można znaleźć w *pomocy Android*.

W celu aktualizacji wersji aplikacji:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Dodatkowe**.
5. W sekcji **Aktualizacja Kaspersky Endpoint Security for Android** kliknij przycisk **Wybierz**.

   Zostanie otwarte okno **Aktualizacja Kaspersky Endpoint Security for Android**.
6. Na liście autonomicznych pakietów instalacyjnych Kaspersky Endpoint Security wybierz pakiet, który spełnia firmowe wymagania bezpieczeństwa.

   Kaspersky Endpoint Security można zaktualizować tylko do najnowszej wersji. Kaspersky Endpoint Security nie może zostać zaktualizowany do starszej wersji aplikacji.
7. Kliknij przycisk **Wybierz**.

   Opis wybranego autonomicznego pakietu instalacyjnego jest wyświetlany w sekcji **Aktualizacja Kaspersky Endpoint Security for Android**.

8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center. Użytkownik urządzenia mobilnego zostanie zapytany o zainstalowanie nowej wersji aplikacji. Po wyrażeniu zgody, nowa wersja aplikacji zostanie zainstalowana na urządzeniu mobilnym.

Instalowanie wcześniejszej wersji Kaspersky Endpoint Security for Android

Jeśli chcesz zapobiec automatycznej aktualizacji aplikacji i użyć określonej wersji Kaspersky Endpoint Security for Android, wyłącz automatyczną aktualizację aplikacji w ustawieniach Google Play. Więcej informacji można znaleźć na stronie pomocy technicznej Google.

Automatyczna aktualizacja Kaspersky Endpoint Security for Android jest dostępna tylko wtedy, gdy aplikacja została zainstalowana z Google Play lub poprzez Kaspersky Security Center przy użyciu odnośnika Google Play. Jeśli aplikacja została zainstalowana poprzez Kaspersky Security Center przy użyciu odnośnika do własnego serwera sieciowego (za pomocą autonomicznego pakietu instalacyjnego), automatyczna aktualizacja nie jest dostępna. W tym przypadku, możesz użyć zasady grupy do ręcznej aktualizacji Kaspersky Endpoint Security for Android.

W celu zainstalowania poprzedniej wersji Kaspersky Endpoint Security for Android:

1. Usuń Kaspersky Endpoint Security for Android z urządzeń mobilnych użytkowników.

2. Zainstaluj Kaspersky Endpoint Security for Android poprzez Kaspersky Security Center przy użyciu odnośnika do swojego własnego serwera sieciowego. W tym celu będziesz potrzebował pakietu instalacyjnego dla określonej wersji. Możesz pobrać pakiet dystrybucyjny dla wcześniejszych wersji Kaspersky Endpoint Security for Android na stronie internetowej pomocy technicznej Kaspersky.

Więcej informacji na temat wcześniejszych wersji Kaspersky Endpoint Security for Android można znaleźć *w pomocy dla odpowiedniej wersji Kaspersky Security for Mobile*.

Aktualizowanie poprzednich wersji wtyczek zarządzających

Możesz zaktualizować wtyczki zarządzające, korzystając z następujących metod:

- Zainstaluj nową wersję wtyczki zarządzającej z listy dostępnych pakietów dystrybucyjnych Konsoli administracyjnej Kaspersky Security Center.

  Lista dostępnych pakietów dystrybucyjnych jest aktualizowana automatycznie po opublikowaniu nowych wersji aplikacji firmy Kaspersky.

- Pobierz pakiet dystrybucyjny z zewnętrznego źródła i zainstaluj nową wersję wtyczki zarządzającej, korzystając z pliku EXE.

  Aby zaktualizować wtyczki zarządzające Kaspersky Endpoint Security for Android i Kaspersky Device Management for iOS, należy pobrać najnowszą wersję aplikacji ze strony internetowej Kaspersky Security for Mobile i uruchomić Kreator instalacji dla każdej z dwóch wtyczek. Poprzednia wersja wtyczek zostanie usunięta automatycznie podczas działania Kreatora instalacji.

Specjaliści z Kaspersky zalecają korzystanie z tej samej wersji aplikacji i wtyczek zarządzających. Jeśli użytkownik zaktualizuje aplikację z Google Play, program Kaspersky Security Center wyświetli komunikat z pytaniem o zaktualizowanie wtyczki zarządzającej.

Podczas aktualizacji wtyczek zarządzających, istniejące grupy administracyjne w folderze **Zarządzane urządzenia** i reguły automatycznego przenoszenia urządzeń z folderu **Urządzenia nieprzypisane** do tych grup zostają zapisane. Istniejące zasady grupowe dla urządzeń mobilnych także są zapisywane. Ustawienia nowej zasady, która implementuje nowe funkcje zintegrowanego rozwiązania Kaspersky Security for Mobile, zostaną dodane do istniejących zasad i będą posiadać wartości domyślne.

Jeśli w nowej wersji wtyczki zarządzającej dodano nowe ustawienia lub zmieniono domyślne wartości, zmiany zostaną zastosowane dopiero po otwarciu zasady grupowej. Do momentu, gdy administrator nie otworzy zasady grupowej, ustawienia poprzedniej wersji wtyczki zostaną zastosowane na urządzeniach mobilnych nawet wtedy, gdy wersja wtyczki została zaktualizowana.

Aktualizowanie z listy Konsoli administracyjnej

W celu zaktualizowania wtyczek zarządzających:

1. W drzewie konsoli wybierz **Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.
2. W obszarze roboczym wybierz **Działania dodatkowe → Wyświetl aktualne wersje aplikacji Kaspersky**.

   Spowoduje to otwarcie listy aktualnych wersji aplikacji firmy Kaspersky.
3. W sekcji **Urządzenia mobilne** wybierz wtyczkę **Kaspersky Endpoint Security for Android** lub **Kaspersky Device Management for iOS**.
4. Kliknij przycisk **Pobierz pakiety dystrybucyjne**.

   Pakiet dystrybucyjny wtyczki zostanie pobrany do pamięci komputera (plik EXE). Uruchom plik EXE. Postępuj zgodnie z instrukcjami Kreatora instalacji.

Aktualizowanie z pakietu dystrybucyjnego

W celu zaktualizowania wtyczki zarządzającej Kaspersky Endpoint Security for Android:

Skopiuj plik instalacyjny wtyczki `klcfinst.exe` z pakietu dystrybucyjnego zintegrowanego rozwiązania i uruchom go na stacji roboczej administratora.

Instalacja jest wykonywana przez kreator i nie jest konieczne konfigurowanie ustawień.

W celu zaktualizowania wtyczki zarządzającej Kaspersky Device Management for iOS:

Skopiuj plik instalacyjny wtyczki `klmdminst.exe` z pakietu dystrybucyjnego zintegrowanego rozwiązania i uruchom go na stacji roboczej administratora.

Instalacja wtyczki jest wykonywana przez kreator i nie jest konieczne konfigurowanie ustawień.

Możesz upewnić się, że wtyczki zarządzające są zaktualizowane, przeglądając listę zainstalowanych wtyczek zarządzających w oknie właściwości Serwera administracyjnego, w sekcji **Zaawansowane → Szczegóły dotyczące zainstalowanych wtyczek zarządzających dla aplikacji**.

Dezinstalowanie Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android można usunąć w następujące sposoby:

1. Usuwanie aplikacji przez użytkownika

   Użytkownik usuwa program Kaspersky Endpoint Security for Android ręcznie z poziomu interfejsu aplikacji. Aby użytkownicy mogli usunąć aplikację, usuwanie aplikacji powinno być dozwolone w zasadzie stosowanej na urządzeniu.

2. Usuwanie aplikacji przez administratora

   Administrator usuwa aplikację zdalnie z poziomu Konsoli administracyjnej Kaspersky Security Center. Aplikacja może zostać usunięta z osobnego urządzenia lub z kilku urządzeń jednocześnie.

Zdalne usuwanie aplikacji

Możesz zdalnie usunąć program Kaspersky Endpoint Security for Android z urządzeń mobilnych użytkowników w następujące sposoby:

- Poprzez zasadę grupy. Metoda ta jest wygodna, jeśli chcesz usunąć aplikację z kilku urządzeń jednocześnie.
- Poprzez konfigurowanie ustawień lokalnych aplikacji. Metoda ta jest wygodna, jeśli chcesz usunąć aplikację z osobnego urządzenia.

W celu usunięcia aplikację poprzez zastosowanie zasady grupy:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Dodatkowe**.
5. W sekcji **Usuwanie aplikacji Kaspersky Endpoint Security for Android** zaznacz pole **Odinstaluj Kaspersky Endpoint Security for Android z urządzenia**.
6. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W wyniku tego, Kaspersky Endpoint Security for Android jest usuwany z urządzeń mobilnych po synchronizacji z Serwerem administracyjnym. Użytkownicy urządzeń mobilnych otrzymują powiadomienie o usunięciu aplikacji.

W celu usunięcia aplikacji poprzez konfigurację ustawień lokalnych:

1. W drzewie konsoli wybierz **Zarządzanie urządzeniami mobilnymi → Urządzenia mobilne**.
2. Z listy urządzeń wybierz urządzenie, z którego chcesz usunąć aplikację.
3. Otwórz okno właściwości urządzenia poprzez dwukrotne kliknięcie.
4. Wybierz **Aplikacje → Kaspersky Endpoint Security for Android**.
5. Otwórz okno właściwości Kaspersky Endpoint Security poprzez dwukrotne kliknięcie.
6. Wybierz sekcję **Dodatkowe**.

7. W sekcji **Usuwanie Kaspersky Endpoint Security for Android** zaznacz pole **Odinstaluj Kaspersky Endpoint Security for Android z urządzenia**.

8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W wyniku tego, Kaspersky Endpoint Security for Android jest usuwany z urządzenia mobilnego po synchronizacji z Serwerem administracyjnym. Użytkownik urządzenia mobilnego otrzymuje powiadomienie o usunięciu aplikacji.

Zezwalanie użytkownikom na odinstalowanie aplikacji

Aby chronić aplikację przed usunięciem na urządzeniach działających pod kontrolą systemu Android 7.0 lub nowszego, Kaspersky Endpoint Security for Android musi być ustawiony jako usługa funkcji Dostępności. Jeśli Kreator wstępnej konfiguracji jest uruchomiony, Kaspersky Endpoint Security for Android wyświetli pytanie o nadanie aplikacji wszystkich wymaganych uprawnień. Użytkownik może pominąć te kroki lub wyłączyć te uprawnienia w ustawieniach urządzenia w późniejszym czasie. W takim przypadku aplikacja nie jest chroniona przed dezinstalacją.

Możesz zezwolić użytkownikom na usunięcie Kaspersky Endpoint Security for Android z ich urządzeń mobilnych w następujące sposoby:

- Poprzez zasadę grupy. Metoda ta jest wygodna, jeśli chcesz umożliwić użytkownikom usunięcie aplikacji z kilku urządzeń jednocześnie.
- Z poziomu lokalnych ustawień aplikacji. Metoda ta jest wygodna, jeśli chcesz umożliwić użytkownikowi osobnego urządzenia usunięcie aplikacji.

W celu umożliwienia usunięcia aplikacji w zasadzie grupy:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.

4. W oknie **Właściwości** wybierz sekcję **Dodatkowe**.

5. W sekcji **Usuwanie Kaspersky Endpoint Security for Android** ustaw pole **Zezwól na usuwanie Kaspersky Endpoint Security for Android**.

6. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, usuwanie aplikacji przez użytkowników jest dozwolone na urządzeniach mobilnych po synchronizacji z Serwerem administracyjnym. Przycisk usunięcia aplikacji staje się dostępny w ustawieniach Kaspersky Endpoint Security for Android.

W celu umożliwienia usunięcia aplikacji w ustawieniach lokalnych aplikacji:

1. W drzewie konsoli wybierz **Dodatkowe** → **Zarządzanie urządzeniami mobilnymi** → **Urządzenia mobilne**.

2. Z listy urządzeń wybierz urządzenie, z którego chcesz zezwolić na usunięcie aplikacji przez użytkownika.

3. Otwórz okno właściwości urządzenia poprzez dwukrotne kliknięcie.

4. Wybierz **Aplikacje** → **Kaspersky Endpoint Security for Mobile**.

5. Otwórz okno właściwości Kaspersky Endpoint Security poprzez dwukrotne kliknięcie.

6. Wybierz sekcję **Dodatkowe**.

7. W sekcji **Usuwanie Kaspersky Endpoint Security for Android** ustaw pole **Zezwól na usuwanie Kaspersky Endpoint Security for Android**.

8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, usuwanie aplikacji przez użytkownika jest dozwolone na urządzeniu mobilnych po synchronizacji z Serwerem administracyjnym. Przycisk usunięcia aplikacji staje się dostępny w ustawieniach Kaspersky Endpoint Security for Android.

Usuwanie aplikacji przez użytkownika

W celu samodzielnego usunięcia Kaspersky Endpoint Security for Android z urządzenia mobilnego użytkownik musi wykonać następujące czynności:

1. W oknie głównym Kaspersky Endpoint Security for Android dotknij → **Odinstaluj aplikację**.

   Na ekranie pojawi się monit proszący o potwierdzenie.

   Jeśli nie ma przycisku **Odinstaluj aplikację**, oznacza to, że administrator włączył ochronę przed usunięciem Kaspersky Endpoint Security for Android.

2. Potwierdź chęć usunięcia Kaspersky Endpoint Security for Android.

Aplikacja Kaspersky Endpoint Security for Android zostanie usunięta z urządzenia mobilnego użytkownika.

Konfiguracja i zarządzanie

Ta sekcja pomocy jest przeznaczona dla specjalistów, którzy administrują Kaspersky Security for Mobile, a także dla specjalistów, którzy oferują pomoc techniczną organizacjom korzystającym z Kaspersky Security for Mobile.

Rozpoczęcie pracy

Ta sekcja opisuje działania, które są zalecane do wykonania przed rozpoczęciem pracy z Kaspersky Security for Mobile.

Uruchamianie i zatrzymywanie działania aplikacji

Kaspersky Security Center automatycznie uruchamia i zatrzymuje wtyczki zarządzające Kaspersky Endpoint Security i Kaspersky Device Management for iOS.

Program Kaspersky Endpoint Security for Android jest uruchamiany podczas ładowania systemu operacyjnego i chroni urządzenie mobilne podczas całej sesji. Użytkownik może zatrzymać działanie aplikacji poprzez wyłączenie wszystkich komponentów Kaspersky Endpoint Security for Android. Możesz użyć zasad grupy do skonfigurowania uprawnień użytkownika do zarządzania komponentami aplikacji.

Na niektórych urządzeniach (na przykład, Huawei, Meizu i Xiaomi) należy ręcznie dodać Kaspersky Endpoint Security for Android do listy aplikacji uruchamianych w momencie uruchamiania systemu operacyjnego (**Bezpieczeństwo** → **Uprawnienia** → **Autouruchamianie**). Jeśli aplikacja nie została dodana do listy, Kaspersky Endpoint Security for Android przestaje wykonywać wszystkie swoje funkcje po ponownym uruchomieniu urządzenia mobilnego.

Należy także wyłączyć tryb Oszczędzania baterii dla Kaspersky Endpoint Security for Android. Jest to konieczne, aby aplikacja mogła działać w tle, na przykład uruchamiać zaplanowane skanowanie antywirusowe lub synchronizować urządzenie z Kaspersky Security Center. Ten problem jest związany z określonymi funkcjami oprogramowania wbudowanego tych urządzeń.

Tworzenie grupy administracyjnej

Aby przeprowadzić scentralizowaną konfigurację aplikacji Kaspersky Endpoint Security for Android zainstalowanej na urządzeniach mobilnych użytkowników, zasady grupy muszą zostać zastosowane do urządzeń.

Aby zastosować zasadę do grupy urządzeń, przed zainstalowaniem aplikacji mobilnych na urządzeniach użytkowników zalecane jest utworzenie oddzielnej grupy dla tych urządzeń w folderze **Zarządzane urządzenia**.

Po utworzeniu grupy administracyjnej zalecane jest skonfigurowanie opcji automatycznego przydzielania do tej grupy urządzeń, na których chcesz zainstalować aplikację. Następnie skonfiguruj ustawienia, które są typowe dla wszystkich urządzeń, korzystając z zasady grupowej.

W celu utworzenia grupy administracyjnej:

1. Z drzewa konsoli wybierz folder **Zarządzane urządzenia**.
2. W obszarze roboczym folderu **Zarządzane urządzenia** lub jego podfolderu wybierz zakładkę **Urządzenia**.
3. Kliknij przycisk **Nowa grupa**.

   Zostanie otwarte okno, w którym możesz utworzyć nową grupę.
4. W oknie **Nazwa grupy** wprowadź nazwę grupy i kliknij **OK**.

W drzewie konsoli pojawi się nowy folder grupy administracyjnej o określonej nazwie. Szczegółowe informacje dotyczące używania grup administracyjnych można znaleźć na stronie *pomocy Kaspersky Security Center*.

Profile grupowe do zarządzania urządzeniami mobilnymi

Zasada grupy to pakiet ustawień do zarządzania urządzeniami mobilnymi, które należą do grupy administracyjnej, oraz do zarządzania aplikacjami mobilnymi zainstalowanymi na urządzeniach. Możesz utworzyć zasadę grupową przy użyciu Kreatora tworzenia zasady.

Możesz użyć zasady do skonfigurowania ustawień pojedynczych urządzeń oraz grupy urządzeń. Dla grupy urządzeń ustawienia administracyjne można skonfigurować w oknie właściwości zasady grupowej. Dla pojedynczego urządzenia można je skonfigurować w oknie lokalnych ustawień aplikacji. Pojedyncze ustawienia zarządzania określone dla jednego urządzenia mogą różnić się od wartości ustawień skonfigurowanych w zasadzie dla grupy, do której należy to urządzenie.

Każdy parametr odzwierciedlony w zasadzie posiada atrybut "zablokowany", co pokazuje, czy możliwe jest modyfikowanie ustawienia w zasadach zagnieżdżonych poziomów hierarchii (dla grup zagnieżdżonych i podrzędnych Serwerów administracyjnych), w lokalnych ustawieniach aplikacji.

Wartości ustawień skonfigurowane w zasadzie i lokalnych ustawieniach aplikacji są zapisywane na Serwerze administracyjnym, rozsyłane na urządzenia mobilne podczas synchronizacji i zapisywane na urządzeniach jako bieżące ustawienia. Jeśli użytkownik określił inne wartości ustawień, które nie zostały "zablokowane", podczas kolejnej synchronizacji urządzenia z Serwerem administracyjnym nowe wartości ustawień są przesyłane do Serwera administracyjnego i zapisywane w lokalnych ustawieniach aplikacji zamiast wartości, które zostały wcześniej określone przez administratora.

Aby zapewnić aktualność ochrony urządzeń mobilnych, możesz monitorować urządzenia użytkowników pod kątem zgodności z zasadą zarządzania grupą.

Wskaźnik poziomu ochrony jest wyświetlany w górnej części okna zasadzie grupowej. Wskaźnik poziomu ochrony pomoże w skonfigurowaniu zasady w taki sposób, aby zapewnić wysoki poziom ochrony urządzenia. Stan wskaźnika poziomu ochrony zmienia się w zależności od ustawień zasady:

- **Wysoki poziom ochrony** – zapewniony jest odpowiedni poziom ochrony urządzenia. Wszystkie moduły ochrony działają zgodnie z ustawieniami zalecanymi przez Kaspersky.
- **Średni poziom ochrony** – poziom ochrony jest niższy niż zalecany. Niektóre krytyczne komponenty ochrony są wyłączone (na przykład, Ochrona WWW). Ważne problemy są oznaczone ikoną .
- **Niski poziom ochrony** – występują problemy, które mogą doprowadzić do infekcji urządzenia i utraty danych. Niektóre krytyczne komponenty ochrony są wyłączone (na przykład, ochrona urządzeń w czasie rzeczywistym). Krytyczne problemy są oznaczone ikoną .

Więcej informacji na temat zarządzania zasadami i grupami administracyjnymi w Konsoli administracyjnej Kaspersky Security Center można znaleźć na stronie *pomocy Kaspersky Security Center*.

Tworzenie profilu grupowego

Ta sekcja opisuje proces tworzenia zasad grupy dla urządzeń, na których zainstalowana jest aplikacja mobilna Kaspersky Endpoint Security for Android, oraz zasad dla urządzeń EAS i urządzeń iOS MDM.

Zasady utworzone dla grupy administracyjnej są wyświetlane w obszarze roboczym grupy w Konsoli administracyjnej Kaspersky Security Center, na zakładce **Zasady**. Przed nazwą zasady pojawi się ikona wskazująca stan zasady (aktywny / nieaktywny). Dla różnych aplikacji w grupie może zostać utworzonych wiele różnych zasad. Tylko jedna zasada dla każdej aplikacji może być aktywna. Po utworzeniu nowej aktywnej zasady, poprzednia aktywna zasada staje się nieaktywna.

Po utworzeniu zasady można zmodyfikować jej ustawienia.

W celu utworzenia zasady do zarządzania urządzeniami mobilnymi:

1. Z drzewa konsoli należy wybrać grupę administracyjną, dla której ma zostać utworzona zasada.
2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Kliknij odnośnik **Utwórz zasadę** w celu uruchomienia Kreatora tworzenia zasady.

Zostanie uruchomiony Kreator tworzenia nowej zasady.

Krok 1. Wybierz aplikację do utworzenia zasady grupy

W tym kroku wybierz aplikację, dla której chcesz utworzyć zasadę grupy na liście aplikacji:

- **Kaspersky Endpoint Security for Android** – dla urządzeń, na których używana jest aplikacja mobilna Kaspersky Endpoint Security for Android.

Zaleca się utworzenie osobnej zasady dla urządzeń Huawei i Honor, które nie mają usług Google Play. W ten sposób możesz wysyłać odnośniki do Huawei AppGallery do użytkowników wszystkich takich urządzeń.

- **Kaspersky Device Management for iOS** – dla urządzeń EAS i urządzeń iOS MDM.

Zasadę dla urządzeń mobilnych można utworzyć, jeśli wtyczka zarządzająca Kaspersky Endpoint Security for Android oraz wtyczka zarządzająca Kaspersky Device Management for iOS są zainstalowane na pulpicie administratora. Jeśli wtyczki nie są zainstalowane, nazwa odpowiedniej aplikacji nie pojawi się na liście aplikacji.

Przejdź do kolejnego kroku Kreatora tworzenia zasady.

Krok 2. Wprowadź nazwę zasady grupy

W tym kroku, w polu **Nazwa** wprowadź nazwę nowej zasady. Jeśli określisz nazwę istniejącej zasady, do jego nazwy automatycznie zostanie dodany przyrostek (1).

Przejdź do kolejnego kroku Kreatora tworzenia zasady.

Krok 3. Utwórz zasadę grupy dla aplikacji

W tym kroku Kreator zapyta o wybranie stanu zasady:

- **Zasada aktywna**. Kreator zapisze utworzoną zasadę na Serwerze administracyjnym. Przy kolejnej synchronizacji urządzenia mobilnego z Serwerem administracyjnym zasada zostanie użyta na urządzeniu jako zasada aktywna.

- **Zasada nieaktywna.** Kreator zapisze utworzoną zasadę na Serwerze administracyjnym jako zapasową zasadę. Ta zasada może być aktywowana w późniejszym czasie, po wystąpieniu określonego zdarzenia. Jeśli to konieczne, zasada nieaktywna może zostać przełączona w stan aktywny.

  Dla jednej aplikacji w grupie może zostać utworzonych wiele różnych zasad, ale tylko jedna z nich może być aktywna. Po utworzeniu nowej aktywnej zasady, poprzednia aktywna zasada automatycznie staje się nieaktywna.

Zakończ działanie Kreatora.

Konfigurowanie ustawień synchronizacji

Aby zarządzać urządzeniami mobilnymi i otrzymywać raporty lub statystyki z urządzeń mobilnych użytkowników, musisz skonfigurować ustawienia synchronizacji. Synchronizacja urządzeń mobilnych z Kaspersky Security Center może odbywać się w następujące sposoby:

- **Zgodnie z terminarzem**. Synchronizacja zgodnie z terminarzem odbywa się przy użyciu protokołu HTTP. Terminarz synchronizacji można skonfigurować w ustawieniach zasady grupy. Modyfikacje w ustawieniach zasady grupy, polecenia i zadania będą wykonywane, gdy urządzenie zostanie zsynchronizowane z Kaspersky Security Center zgodnie z terminarzem, czyli z opóźnieniem. Domyślnie urządzenia mobilne są synchronizowane z Kaspersky Security Center automatycznie co 6 godzin.

  W systemie Android 12 lub nowszych aplikacja może wykonać to zadanie później niż określono, jeśli urządzenie jest w trybie oszczędzania baterii.

- **Wymuszona**. Wymuszona synchronizacja odbywa się przy użyciu powiadomień typu push usługi FCM (Firebase Cloud Messaging). Wymuszona synchronizacja jest przeznaczona przede wszystkim do dostarczania w odpowiednim momencie poleceń na urządzenie mobilne. Jeśli chcesz używać wymuszonej synchronizacji, upewnij się, że ustawienia GSM są skonfigurowane w Kaspersky Security Center. W celu uzyskania więcej informacji, odwiedź stronę pomocy Kaspersky Security Center.

W celu skonfigurowania ustawień synchronizacji urządzenia mobilnego z Kaspersky Security Center:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Synchronizacja**.
5. Na liście rozwijalnej **Synchronizuj** wybierz częstotliwość synchronizacji.
6. Aby wyłączyć synchronizację urządzenia z Kaspersky Security Center podczas roamingu, zaznacz pole **Nie synchronizuj podczas roamingu**.

   Użytkownik urządzenia może ręcznie przeprowadzić synchronizację w ustawieniach aplikacji (→ **Ustawienia** → **Synchronizacja** → **Synchronizuj**).
7. Aby ukryć ustawienia synchronizacji (adres serwera, port i grupę administracyjną) przed użytkownikiem w ustawieniach aplikacji, odznacz pole **Pokaż ustawienia synchronizacji na urządzeniu**. Nie można zmodyfikować ukrytych ustawień.
8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center. Możesz ręcznie zsynchronizować urządzenie mobilne, korzystając ze specjalnego polecenia. Więcej informacji na temat pracy z poleceniami dla urządzeń mobilnych można znaleźć w *Pomocy Kaspersky Security Center*.

Zarządzanie rewizjami dla zasad grupowych

Kaspersky Security Center umożliwia śledzenie modyfikacji zasad grupowych. Za każdym razem, gdy zapisujesz zmiany wprowadzone w zasadzie grupowej zostaje utworzona *rewizja*. Każda rewizja posiada numer.

Możesz zarządzać rewizjami tylko dla zasad Kaspersky Endpoint Security for Android. Nie można zarządzać rewizjami w zasadzie Kaspersky Device Management for iOS.

Na rewizjach zasad grupowych można wykonywać następujące działania:

- Porównywać wybraną rewizję z bieżącą.
- Porównywać wybrane rewizje.
- Porównać zasadę z wybraną rewizją innej zasady.
- Wyświetlić wybraną rewizję.
- Wycofać zmiany wprowadzone w zasadzie do wybranej rewizji.
- Zapisać rewizje jako plik .txt.

Więcej informacji na temat zarządzania rewizjami zasad grupowych i innych obiektów (na przykład kont użytkowników), można znaleźć na stronie *pomocy Kaspersky Security Center*.

W celu wyświetlenia historii rewizji zasady grupowej:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Historia rewizji**.

   Wyświetlana zostanie lista rewizji zasad. Zawiera ona następujące informacje:

   - Numer rewizji zasady.
   - Data i godzina zmodyfikowania zasady.
   - Nazwa użytkownika, który zmodyfikował zasadę.
   - Działanie wykonane na zasadzie.
   - Opis rewizji dokonanej na ustawieniach zasady.

Usuwanie profilu grupowego

W celu usunięcia zasady grupy:

1. W drzewie konsoli wybierz grupę administracyjną, dla której chcesz usunąć zasadę.
2. W obszarze roboczym grupy administracyjnej, na zakładce **Zasady** wybierz zasadę, którą chcesz usunąć.
3. W menu kontekstowym zasady wybierz **Usuń**.

W rezultacie zasada grupy zostanie usunięta. Przed zastosowaniem nowej zasady grupy, urządzenia mobilne należące do grupy administracyjnej będą działać z ustawieniami określonymi w usuniętej zasadzie.

Ograniczanie uprawnień do konfigurowania zasad grupowych

Administratorzy Kaspersky Security Center mogą skonfigurować uprawnienia dostępu użytkowników Konsoli administracyjnej do różnych funkcji zintegrowanego rozwiązania Kaspersky Security for Mobile w zależności od obowiązków użytkowników.

W Konsoli administracyjnej możesz skonfigurować uprawnienia dostępu we właściwościach Serwera administracyjnego, na zakładkach **Bezpieczeństwo** i **Role użytkowników**. Zakładka **Role użytkowników** umożliwia dodanie standardowych ról użytkowników z predefiniowanym zestawem uprawnień. Sekcja **Bezpieczeństwo** umożliwia skonfigurowanie uprawnień dla jednego użytkownika lub grupy użytkowników bądź przypisanie ról do jednego użytkownika lub grupy użytkowników. Uprawnienia użytkownika dla każdej aplikacji są konfigurowane zgodnie z *zakresem funkcji*.

Możliwe jest także skonfigurowanie uprawnień użytkownika charakterystycznych dla obszarów działania. Informacje o podobieństwie obszarów działania z zakładkami zasady można znaleźć w Dodatku.

Dla każdego obszaru działania administrator może przydzielić następujące uprawnienia:

- **Zezwól na modyfikację**. Użytkownik Konsoli administracyjnej może zmieniać ustawienia zasady w oknie właściwości.
- **Blokuj modyfikację**. Użytkownik Konsoli administracyjnej nie może zmieniać ustawień zasady w oknie właściwości. Zakładki zasady należące do zakresu funkcji, dla którego to uprawnienie zostało przydzielone, nie są wyświetlane w interfejsie.

Więcej informacji na temat zarządzania uprawnieniami i rolami użytkowników w Konsoli administracyjnej Kaspersky Security Center można znaleźć w *pomocy Kaspersky Security Center*.

Ochrona

Ta sekcja zawiera informacje dotyczące zdalnego zarządzania ochroną urządzeń mobilnych w Konsoli administracyjnej Kaspersky Security Center.

Konfigurowanie ochrony antywirusowej na urządzeniach Android

Aby natychmiast wykrywać zagrożenia, wirusy i inne złośliwe aplikacje, należy skonfigurować ustawienia ochrony w czasie rzeczywistym i automatyczne uruchamianie skanowania antywirusowego.

Kaspersky Endpoint Security for Android wykrywa następujące typy obiektów:

- Wirusy, robaki, trojany i złośliwe narzędzia
- Adware
- Aplikacje, które mogą być wykorzystywane przez cyberprzestępców w celu wyrządzenia szkody na Twoim urządzeniu lub kradzieży danych osobowych

Antywirus posiada kilka ograniczeń:

- Jeśli Antywirus jest uruchomiony, zagrożenie wykryte w pamięci zewnętrznej urządzenia (takie jak karta SD) nie może zostać zneutralizowane automatycznie w profilu roboczym (Aplikacje z ikoną teczki, Konfigurowanie profilu roboczego Android). Kaspersky Endpoint Security for Android nie ma dostępu do pamięci zewnętrznej w profilu roboczym. Informacje o wykrytych obiektach są wyświetlane w sekcji **Stan** aplikacji. Aby zneutralizować obiekty wykryte w pamięci zewnętrznej, pliki obiektów muszą zostać usunięte ręcznie, a skanowanie urządzenia musi zostać uruchomione ponownie.

- Ze względu na ograniczenia techniczne, Kaspersky Endpoint Security for Android nie może skanować plików o rozmiarze 2 GB lub większym. Podczas skanowania aplikacja pomija takie pliki bez informowania o tym fakcie.

W celu skonfigurowania ustawienia ochrony w czasie rzeczywistym urządzenia mobilnego:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.

4. W oknie **Właściwości** wybierz sekcję **Ochrona**.

5. W sekcji **Ochrona** skonfiguruj ustawienia ochrony systemu plików urządzenia mobilnego:

   - Aby włączyć ochronę w czasie rzeczywistym urządzenia mobilnego przed zagrożeniami, zaznacz pole **Włącz ochronę**.

     Kaspersky Endpoint Security for Android skanuje tylko nowe aplikacje i pliki z folderu Pobrane.

   - Aby włączyć rozszerzoną ochronę urządzenia mobilnego przed zagrożeniami, zaznacz pole **Rozszerzony tryb ochrony**.

     Kaspersky Endpoint Security for Android skanuje wszystkie pliki otwierane, modyfikowane, przenoszone, kopiowane, instalowane lub zapisywane przez użytkownika na urządzeniu, a także nowo zainstalowane aplikacje mobilne.

     > Na urządzeniach z systemem Android 8.0 lub nowszym Kaspersky Endpoint Security for Android skanuje pliki, które użytkownik modyfikuje, przenosi, instaluje i zapisuje, a także kopie plików. Kaspersky Endpoint Security for Android nie skanuje plików po ich otwarciu lub plików źródłowych po ich skopiowaniu.

   - Aby włączyć dodatkowe skanowanie nowych aplikacji przed ich pierwszym uruchomieniem na urządzeniu użytkownika za pomocą usługi chmury Kaspersky Security Network, zaznacz pole **Ochrona w chmurze (KSN)**.

   - Aby zablokować oprogramowanie reklamowe i aplikacje, które mogą zostać wykorzystane przez przestępców w celu uszkodzenia urządzenia lub danych użytkownika, zaznacz pole wyboru **Wykrywaj oprogramowanie reklamowe, autodialery i aplikacje, które mogą być wykorzystywane przez przestępców do wyrządzenia szkody urządzeniu i danym użytkownika**.

6. Na liście **Akcja po wykryciu zagrożenia** wybierz jedną z następujących opcji:

   - **Usuń**

     Wykryte obiekty zostaną automatycznie usunięte. Użytkownik nie musi podejmować żadnych dodatkowych działań. Przed usunięciem obiektu, Kaspersky Endpoint Security for Android wyświetli tymczasowe powiadomienie o wykryciu obiektu.

   - **Pomiń**

Jeśli wykryte obiekty zostaną pominięte, Kaspersky Endpoint Security for Android ostrzeże użytkownika o problemach z ochroną urządzenia. Informacja na temat pominiętych obiektów jest wyświetlana w sekcji aplikacji **Stan**. Dla każdego pominiętego zagrożenia, aplikacja udostępnia działania użytkownikowi, które może wykonać w celu eliminacji zagrożenia. Lista pominiętych obiektów może ulec zmianie, na przykład, jeśli szkodliwy plik został usunięty lub przeniesiony. Aby uzyskać aktualną listę zagrożeń, uruchom pełne skanowanie urządzenia. Aby zapewnić solidną ochronę danych, wyeliminuj wszystkie wykryte obiekty.

- **Kwarantanna**

7. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

W celu skonfigurowania automatycznego uruchamiania skanowania antywirusowego na urządzeniu mobilnym:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Skanowanie**.
5. Aby zablokować oprogramowanie reklamowe i aplikacje, które mogą zostać wykorzystane przez przestępców w celu uszkodzenia urządzenia lub danych użytkownika, zaznacz pole wyboru **Wykrywaj oprogramowanie reklamowe, autodialery i aplikacje, które mogą być wykorzystywane przez przestępców do wyrządzenia szkody urządzeniu i danym użytkownika**.
6. Na liście **Akcja po wykryciu zagrożenia** wybierz jedną z następujących opcji:

   - **Usuń**

     Wykryte obiekty zostaną automatycznie usunięte. Użytkownik nie musi podejmować żadnych dodatkowych działań. Przed usunięciem obiektu, Kaspersky Endpoint Security for Android wyświetli tymczasowe powiadomienie o wykryciu obiektu.

   - **Pomiń**

     Jeśli wykryte obiekty zostaną pominięte, Kaspersky Endpoint Security for Android ostrzeże użytkownika o problemach z ochroną urządzenia. Informacja na temat pominiętych obiektów jest wyświetlana w sekcji aplikacji **Stan**. Dla każdego pominiętego zagrożenia, aplikacja udostępnia działania użytkownikowi, które może wykonać w celu eliminacji zagrożenia. Lista pominiętych obiektów może ulec zmianie, na przykład, jeśli szkodliwy plik został usunięty lub przeniesiony. Aby uzyskać aktualną listę zagrożeń, uruchom pełne skanowanie urządzenia. Aby zapewnić solidną ochronę danych, wyeliminuj wszystkie wykryte obiekty.

   - **Kwarantanna**

   - **Pytaj użytkownika**

     Aplikacja Kaspersky Endpoint Security for Android wyświetla powiadomienie z monitem o wybranie akcji, która ma zostać podjęta wobec wykrytego obiektu: **Pomiń** lub **Usuń**.

Jeśli aplikacja wykryje kilka zagrożeń, opcja **Pytaj użytkownika** umożliwi użytkownikowi urządzenia zastosowanie wybranej akcji do każdego pliku poprzez użycie opcji **Zastosuj do wszystkich**.

Program Kaspersky Endpoint Security for Android musi zostać ustawiony jako usługa dostępności w celu zapewnienia wyświetlania powiadomień na urządzeniach mobilnych działających pod kontrolą systemu Android 10.0 lub nowszego. Kaspersky Endpoint Security for Android wyświetli pytanie o ustawienie aplikacji jako usługę funkcji Dostępności poprzez Kreator wstępnej konfiguracji. Użytkownik może pominąć ten krok lub wyłączyć tę usługę w ustawieniach urządzenia w późniejszym czasie. W tym przypadku aplikacja Kaspersky Endpoint Security for Android wyświetla okno systemowe z monitem o wybranie akcji, która ma zostać podjęta na wykrytym obiekcie: Pomiń lub Usuń. Aby zastosować akcję na kilku obiektach, należy otworzyć Kaspersky Endpoint Security.

7. Sekcja **Zaplanowane skanowanie** zawiera ustawienia automatycznego uruchamiania pełnego skanowania systemu plików urządzenia. W tym celu kliknij przycisk **Terminarz** i określ częstotliwość pełnego skanowania w oknie **Terminarz**.

   W systemie Android 12 lub nowszych aplikacja może wykonać to zadanie później niż określono, jeśli urządzenie jest w trybie oszczędzania baterii.

8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center. Kaspersky Endpoint Security for Android skanuje wszystkie pliki, w tym zawartość archiwów.

Aby zapewnić aktualną ochronę urządzenia mobilnego, skonfiguruj ustawienia aktualizacji antywirusowych baz danych.

Domyślnie aktualizacje bazy danych aplikacji są wyłączone, gdy urządzenie jest w strefie roamingu. Zaplanowane aktualizacje antywirusowych baz danych nie są wykonywane.

W celu skonfigurowania ustawień aktualizacji antywirusowej bazy danych:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Aktualizacja baz danych**.
5. Jeśli chcesz, aby Kaspersky Endpoint Security for Android pobierał uaktualnienia baz danych zgodnie z terminarzem, gdy urządzenie jest w trybie roamingu, w sekcji **Aktualizacja baz danych podczas roamingu** zaznacz pole **Aktualizacja baz danych podczas roamingu**.

   Nawet jeśli pole jest odznaczone, użytkownik może ręcznie uruchomić aktualizację antywirusowych baz danych, gdy urządzenie jest w strefie roamingu.
6. W sekcji **Źródło uaktualnień baz danych** wybierz źródła uaktualnień, z którego Kaspersky Endpoint Security for Android pobiera i instaluje uaktualnienia antywirusowych baz danych aplikacji:
   - **Serwery Kaspersky**

Aplikacja używa serwerów aktualizacji Kaspersky jako źródła uaktualnień, z którego pobiera bazy danych Kaspersky Endpoint Security for Android na urządzenia mobilne użytkowników. Aby aktualizować bazy danych z serwerów Kaspersky, Kaspersky Endpoint Security for Android przesyła dane do Kaspersky (na przykład, ID uruchomienia zadania aktualizacji). Lista danych, które są przesyłane podczas aktualizacji bazy danych, jest dostępna w Umowie licencyjnej.

- **Serwer administracyjny**

  Aplikacja używa Serwera administracyjnego Kaspersky Security Center jako źródła uaktualnień, z którego pobiera bazy danych Kaspersky Endpoint Security for Android na urządzenia mobilne użytkowników.

- **Inne źródło**

  Aplikacja używa innych serwerów jako źródła uaktualnień, z którego pobiera bazy danych Kaspersky Endpoint Security for Android na urządzenia mobilne użytkowników. Aby uruchomić aktualizację, w polu poniżej należy wprowadzić adres serwera HTTP (np. http://domain.com/).

7. W sekcji **Zaplanowana aktualizacja baz danych** skonfiguruj ustawienia uruchamiania aktualizacji antywirusowych baz danych na urządzeniu użytkownika. W tym celu kliknij przycisk **Terminarz** i określ częstotliwość i czas uruchomienia aktualizacji w oknie **Terminarz**.

   W systemie Android 12 lub nowszych aplikacja może wykonać to zadanie później niż określono, jeśli urządzenie jest w trybie oszczędzania baterii.

8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Ochrona urządzeń Android w internecie

Aby chronić dane prywatne użytkownika urządzenia mobilnego w internecie, włącz Ochronę WWW. Ochrona WWW blokuje szkodliwe strony internetowe rozpowszechniające szkodliwy kod oraz phishingowe strony internetowe, których celem jest kradzież Twoich poufnych danych, a także uzyskanie dostępu do kont finansowych. Ochrona WWW skanuje strony internetowe przed ich otwarciem, korzystając z usługi chmury Kaspersky Security Network. Ochrona WWW umożliwia skonfigurowanie dostępu użytkownika do stron internetowych w oparciu o predefiniowane listy dozwolonych i blokowanych stron internetowych.

Kaspersky Endpoint Security for Android musi być ustawiony jako funkcja dostępności. Kaspersky Endpoint Security for Android wyświetli pytanie o ustawienie aplikacji jako usługę funkcji Dostępności poprzez Kreator wstępnej konfiguracji. Użytkownik może pominąć ten krok lub wyłączyć tę usługę w ustawieniach urządzenia w późniejszym czasie.

Ochrona WWW na urządzeniach z systemem Android działa tylko w przeglądarkach: Huawei Browser, Google Chrome (włączając funkcję Kart niestandardowych) i Samsung Internet Browser. Ochrona WWW dla przeglądarki Samsung Internet Browser nie blokuje stron na urządzeniu mobilnym, jeśli profil roboczy jest używany, a Ochrona WWW jest włączona tylko dla profilu roboczego.

W celu włączenia Ochrony WWW w przeglądarce Google Chrome, Huawei Browser lub Samsung Internet Browser:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.

4. W oknie **Właściwości** wybierz **Ochrona WWW**.

5. Aby korzystać z modułu Ochrona WWW, Ty lub użytkownik urządzenia powinien przeczytać i zaakceptować Oświadczenie dotyczące przetwarzania danych na potrzeby modułu Ochrona WWW (Oświadczenie dotyczące modułu Ochrona WWW):

   a. Kliknij odnośnik **Oświadczenie dotyczące modułu Ochrona WWW**.

   Spowoduje to otwarcie okna **Oświadczenie dotyczące przetwarzania danych na potrzeby modułu Ochrona WWW**. Aby zaakceptować Oświadczenie dotyczące modułu Ochrona WWW, należy przeczytać i zaakceptować Politykę prywatności.

   b. Kliknij odnośnik Polityka prywatności. Przeczytaj i zaakceptuj Politykę prywatności.

   Jeśli nie zaakceptujesz Polityki prywatności, użytkownik urządzenia mobilnego może zaakceptować Politykę prywatności w Kreatorze wstępnej konfiguracji lub w aplikacji (→ **Informacje o aplikacji** → **Warunki i postanowienia** → **Politykę prywatności**).

   c. Wybierz tryb zaakceptowania Oświadczenia dotyczącego modułu Ochrona WWW:

   - **Przeczytałem i akceptuję Oświadczenie dotyczące modułu Ochrona WWW**
   - **Wymagaj akceptacji przez użytkownika urządzenia Oświadczenia dotyczącego modułu Ochrona WWW**
   - **Nie akceptuję Oświadczenia dotyczącego modułu Ochrona WWW**

6. Jeśli wybierzesz **Nie akceptuję Oświadczenia dotyczącego modułu Ochrona WWW**, Ochrona WWW nie zablokuje stron na urządzeniu mobilnym. Użytkownik urządzenia mobilnego nie może włączyć modułu Ochrona WWW w Kaspersky Endpoint Security.

7. Zaznacz pole **Włącz Ochronę WWW**.

8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Ochrona danych na skradzionym lub zagubionym urządzeniu

Ta sekcja opisuje sposób konfiguracji ustawień ochrony przed nieautoryzowanym dostępem na urządzeniu w przypadku jego zagubienia lub kradzieży.

Wysyłanie poleceń na urządzenie mobilne

Aby chronić dane na zagubionym lub skradzionym urządzeniu mobilnym, możesz wysłać specjalne polecenia (patrz tabela poniżej).

Polecenia do ochrony danych na zagubionym lub skradzionym urządzeniu

Metody	Polecenie	Wynik wykonania polecenia

łączenia z Kaspersky Security Center		
Kaspersky Endpoint Security for Android	Zablokuj	Urządzenie mobilne jest zablokowane.
	Odblokuj	Po odblokowaniu urządzenia mobilnego działającego pod kontrolą systemu Android 5.0 – 6.X, hasło odblokowujące ekran (kod PIN) zostaje zresetowane do wartości "1234". Po odblokowaniu urządzenia działającego pod kontrolą systemu Android 7.0 lub nowszego, hasło odblokowujące ekran nie zostaje zmienione.
	Zlokalizuj urządzenie	Urządzenie zostanie zlokalizowane i wyświetlone na Google Maps. Dostawca usługi mobilnej pobiera opłatę za wysłanie wiadomości SMS oraz za dostęp do internetu. Na urządzeniach z systemem Android 12 lub nowszym, jeśli użytkownik przyznał uprawnienie "Użyj przybliżonej lokalizacji", aplikacja Kaspersky Endpoint Security for Android najpierw spróbuje uzyskać dokładną lokalizację urządzenia. Jeśli to się nie powiedzie, przybliżona lokalizacja urządzenia zostanie zwrócona tylko wtedy, gdy została odebrana nie więcej niż 30 minut wcześniej. W przeciwnym razie polecenie **Zlokalizuj urządzenie** nie powiedzie się.
	Zdjęcie (mugshot)	Urządzenie mobilne jest zablokowane. Zdjęcie złodzieja jest wykonywane przez przedni aparat urządzenia, gdy próbuje odblokować urządzenie. Dostawca usługi mobilnej pobiera opłatę za wysłanie wiadomości SMS oraz za dostęp do internetu. Podczas próby odblokowania urządzenia użytkownik automatycznie wyraża zgodę na zrobienie zdjęcia. W przypadku cofnięcia pozwolenia na korzystanie z kamery urządzenie mobilne wyświetla powiadomienie i prosi o udzielenie pozwolenia. Na urządzeniu mobilnym z systemem Android 12 lub nowszym, jeśli pozwolenie na korzystanie z aparatu zostało cofnięte w Szybkich ustawieniach, powiadomienie nie jest wyświetlane, ale wykonane zdjęcie jest czarne.
	Alarm	Urządzenie mobilne włączy alarm. Alarm będzie włączony przez 5 minut (lub przez 1 minutę, jeśli bateria urządzenia jest słaba).
	Wyczyść dane firmowe	Usuwane są dane w kontenerze, firmowe konto e-mail, ustawienia połączenia z firmową siecią Wi-Fi i VPN, nazwa punktu dostępu (APN), profil roboczy Android, kontener KNOX oraz klucz KNOX License Manager.
	Przywróć ustawienia fabryczne	Wszystkie dane zostają usunięte z urządzenia mobilnego i zostają przywrócone ustawienia fabryczne. Po wykonaniu tego polecenia, urządzenie nie będzie mogło odbierać i wykonywać poleceń.
Profil iOS MDM	Zablokuj	Urządzenie mobilne jest zablokowane.
	Odblokuj	Blokowanie urządzenia mobilnego przy użyciu kodu PIN jest wyłączone. Wcześniej określony kod PIN został zresetowany.
	Wyczyść	Wszystkie zainstalowane profile konfiguracyjne, profile informacyjne, profil iOS

	dane firmowe	MDM oraz aplikacje, dla których zaznaczono pole **Usuń wraz z profilem iOS MDM**, zostaną usunięte z urządzenia.
	Przywróć ustawienia fabryczne	Wszystkie dane zostają usunięte z urządzenia mobilnego i zostają przywrócone ustawienia fabryczne. Po wykonaniu tego polecenia, urządzenie nie będzie mogło odbierać i wykonywać poleceń.
Skrzynka pocztowa Exchange	Przywróć ustawienia fabryczne	Wszystkie dane zostają usunięte z urządzenia mobilnego i zostają przywrócone ustawienia fabryczne. Po wykonaniu tego polecenia, urządzenie nie będzie mogło odbierać i wykonywać poleceń.

Do wykonywania poleceń Kaspersky Endpoint Security for Android wymagane są specjalne uprawnienia i pozwolenia. Jeśli Kreator wstępnej konfiguracji jest uruchomiony, Kaspersky Endpoint Security for Android wyświetli pytanie o nadanie aplikacji wszystkich wymaganych uprawnień i pozwoleń. Użytkownik może pominąć te kroki lub wyłączyć te uprawnienia w ustawieniach urządzenia w późniejszym czasie. W takiej sytuacji niemożliwe będzie wykonywanie poleceń.

Na urządzeniach działających pod kontrolą systemu Android 10.0 lub nowszego użytkownik musi nadać uprawnienie "Cały czas", aby uzyskać dostęp do lokalizacji Na urządzeniach działających pod kontrolą systemu Android 11.0 lub nowszego użytkownik musi nadać uprawnienie "Podczas używania aplikacji", aby uzyskać dostęp do aparatu. W przeciwnym razie polecenia anti-theft nie będą działały. Użytkownik zostanie poinformowany o tym ograniczeniu i ponownie zostanie zapytany o nadanie uprawnień żądanego poziomu. Jeśli użytkownik wybierze opcję "Tylko teraz" dla uprawnienia dostępu do aparatu, aplikacja uzna, że dostęp został nadany. Jeśli ponownie zostanie wyświetlona prośba o nadanie uprawnienia dostępu do aparatu, zalecane jest bezpośrednie skontaktowanie się z użytkownikiem.

Aby dowiedzieć się więcej o wysyłaniu poleceń z listy urządzeń mobilnych w Konsoli administracyjnej, przejdź do *pomocy Kaspersky Security Center*.

Odblokowywanie urządzenia mobilnego

Urządzenie mobilne można odblokować przy pomocy następujących metod:

- Wyślij polecenie odblokowania urządzenia mobilnego.
- Wprowadź jednorazowy kod odblokowujący na urządzeniu mobilnym (tylko dla urządzeń Android).

Na niektórych urządzeniach (na przykład Huawei, Meizu i Xiaomi) konieczne jest ręczne dodanie Kaspersky Endpoint Security for Android do listy aplikacji uruchamianych podczas uruchamiania systemu operacyjnego. Jeśli aplikacja nie zostanie dodana do listy, będziesz mógł odblokować urządzenie tylko przy użyciu jednorazowego kodu odblokowującego. Nie możesz użyć poleceń do odblokowania urządzenia.

Aby dowiedzieć się więcej o wysyłaniu poleceń z listy urządzeń mobilnych w Konsoli administracyjnej, przejdź do *pomocy Kaspersky Security Center*.

Jednorazowy kod odblokowujący jest sekretnym kodem aplikacji do odblokowania urządzenia mobilnego. Jednorazowy kod jest generowany przez aplikację i jest unikatowy dla każdego urządzenia mobilnego. Możesz zmienić długość jednorazowego kodu (4, 8 lub 16 cyfr) w ustawieniach zasad grupy w sekcji **Anti-Theft**.

W celu odblokowania urządzenia mobilnego przy użyciu kodu jednorazowego:

1. W drzewie konsoli wybierz **Zarządzanie urządzeniami mobilnymi → Urządzenia mobilne**.
2. Wybierz urządzenie mobilne, dla którego chcesz uzyskać jednorazowy kod odblokowujący.

3. Otwórz okno właściwości urządzenia mobilnego poprzez dwukrotne kliknięcie.

4. Wybierz **Aplikacje** → **Kaspersky Endpoint Security for Android**.

5. Otwórz okno właściwości Kaspersky Endpoint Security poprzez dwukrotne kliknięcie.

6. Wybierz sekcję **Anti-Theft**.

7. Unikatowy kod dla wybranego urządzenia jest wyświetlany w polu **Kod jednorazowy** sekcji **Kod jednorazowo odblokowujący urządzenie**.

8. Użyj dowolnej z dostępnych metod (takiej jak e-mail), aby przekazać kod jednorazowy użytkownikowi zablokowanego urządzenia.

9. Użytkownik wprowadza jednorazowy kod na ekranie urządzenia, które jest zablokowane przez Kaspersky Endpoint Security for Android.

Urządzenie mobilne zostanie odblokowane. Po odblokowaniu urządzenia mobilnego działającego pod kontrolą systemu Android 5.0 – 6.X, hasło odblokowujące ekran (kod PIN) zostaje zresetowane do wartości "1234". Po odblokowaniu urządzenia działającego pod kontrolą systemu Android 7.0 lub nowszego, hasło odblokowujące ekran nie zostaje zmienione.

Szyfrowanie danych

Aby chronić dane przed nieautoryzowanym dostępem, należy włączyć szyfrowanie wszystkich danych na urządzeniu (na przykład, danych uwierzytelniających konta, nośników wymiennych i aplikacji, a także wiadomości e-mail, wiadomości SMS, kontaktów, zdjęć i innych plików). Aby uzyskać dostęp do zaszyfrowanych danych, należy określić specjalny klucz – hasło odblokowujące urządzenie. Jeśli dane są zaszyfrowane, dostęp do nich można uzyskać tylko wtedy, gdy urządzenie jest odblokowane.

Szyfrowanie danych jest domyślnie włączone na urządzeniach iOS zablokowanych przy użyciu hasła (**Ustawienia** → **Touch ID / Face ID i hasło** → **Włącz hasło)**.

W celu zaszyfrowania wszystkich danych na urządzeniu Android:

1. Włącz blokadę ekranu na urządzeniu Android (**Ustawienia** → **Bezpieczeństwo** → **Blokada ekranu**).

2. Ustaw hasło odblokowujące urządzenie, które jest zgodne z firmowymi wymaganiami bezpieczeństwa.

Nie jest zalecane używanie wzoru jako kodu odblokowującego urządzenie. Na niektórych urządzeniach Android działających pod kontrolą systemu Android 6.0 lub nowszego, po zaszyfrowaniu danych i ponownym uruchomieniu urządzenia Android, do odblokowania urządzenia należy wprowadzić hasło numeryczne zamiast wzoru. Ten problem jest związany z działaniem usługi Ułatwień dostępu. W tym przypadku, aby odblokować ekran urządzenia, przekonwertuj wzór na hasło numeryczne. Więcej informacji na temat konwertowania wzoru na hasło numeryczne można znaleźć na stronie działu pomocy technicznej producenta urządzenia mobilnego.

3. Włącz szyfrowanie wszystkich danych na urządzeniu (**Ustawienia** → **Bezpieczeństwo** → **Zaszyfruj telefon**).

Konfigurowanie siły hasła odblokowującego urządzenie

Aby chronić dostęp do urządzenia mobilnego użytkownika, należy ustawić hasło odblokowujące urządzenie.

Ta sekcja zawiera informacje na temat sposobu konfiguracji ochrony hasłem na urządzeniach Android oraz iOS.

Konfigurowanie silnego hasła odblokowującego dla urządzeń Android

Aby zabezpieczyć urządzenie Android, należy skonfigurować używanie hasła, o którego wprowadzenie użytkownik będzie proszony, gdy urządzenie przejdzie w tryb uśpienia.

Możesz nałożyć ograniczenia dotyczące aktywności użytkownika w przypadku, gdy hasło odblokowujące jest słabe (na przykład, zablokować urządzenie). Ograniczenia można nałożyć przy użyciu komponentu Kontrola zgodności. W tym celu, w ustawieniach reguły skanowania należy wybrać kryterium **Hasło odblokowujące nie spełnia wymagań bezpieczeństwa**.

Na pewnych urządzeniach Samsung działających pod kontrolą systemu Android 7.0 lub nowszego, jeśli użytkownik spróbuje skonfigurować nieobsługiwane metody odblokowania urządzenia (na przykład, wzór), urządzenie może zostać zablokowane, gdy spełnione będą następujące warunki: włączona jest ochrona przed dezinstalacją Kaspersky Endpoint Security for Android oraz ustawione są wymagania wobec siły hasła odblokowującego ekran. Aby odblokować urządzenie, należy wysłać specjalne polecenie na urządzenie.

W celu skonfigurowania korzystania z hasła odblokowującego:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Zarządzanie urządzeniami**.
5. Jeśli chcesz, żeby aplikacja sprawdzała, czy ustawiono hasło odblokowujące, w sekcji **Blokada ekranu** zaznacz pole **Wymagaj ustawienia hasła odblokowującego ekran**.

   Jeśli aplikacja wykryje, że na urządzeniu nie określono hasła systemowego, zapyta użytkownika o jego ustawienie. Hasło zostanie ustawione zgodnie z parametrami zdefiniowanymi przez administratora
6. Należy określić minimalną liczbę znaków.

   Minimalna liczba znaków w haśle użytkownika. Możliwe wartości: od 4 do 16 znaków.

   Domyślnie, hasło użytkownika powinno zawierać 4 znaki.

   Na urządzeniach z Androidem 10.0 lub nowszym Kaspersky Endpoint Security przetwarza wymagania dotyczące mocy hasła na jedną z wartości systemowych: średnią lub wysoką.

   Wartości dla urządzeń z systemem Android 10.0 lub nowszym są określane przez następujące reguły:

   - Jeśli wymagana długość hasła wynosi od 1 do 4 symboli, aplikacja prosi użytkownika o ustawienie hasła o średniej mocy. Musi być numeryczne (PIN) bez powtarzających się lub uporządkowanych (np. 1234) sekwencji lub alfabetyczne/alfanumeryczne. Kod PIN lub hasło musi mieć co najmniej 4 znaki.
   - Jeśli wymagana długość hasła to 5 lub więcej symboli, aplikacja prosi użytkownika o ustawienie silnego hasła. Musi być numeryczne (PIN) bez powtarzających się lub uporządkowanych sekwencji lub alfabetyczne/alfanumeryczne (hasło). Kod PIN musi mieć co najmniej 8 cyfr; hasło musi mieć co najmniej 6 znaków.

7. Jeśli chcesz, żeby użytkownik miał możliwość użycia odcisku palca do odblokowania ekranu, zaznacz pole **Zezwól na korzystanie z odcisków palców**. Jeśli hasło odblokowujące nie jest zgodne z firmowymi wymaganiami bezpieczeństwa, nie możesz użyć czytnika linii papilarnych do odblokowania ekranu.

   Na urządzeniach z Androidem 10.0 lub nowszym odciskiem palca do odblokowywania ekranu można zarządzać tylko w przypadku profilu roboczego.

   Kaspersky Endpoint Security for Android nie ogranicza korzystania ze skanera linii papilarnych do logowania się do aplikacji lub potwierdzania zakupów

   Na niektórych urządzeniach Samsung niemożliwe jest zablokowanie użycia odcisku palca do odblokowania urządzenia. Na niektórych urządzeniach Samsung, jeśli hasło odblokowujące nie jest zgodne z firmowymi wymaganiami bezpieczeństwa, Kaspersky Endpoint Security for Android nie blokuje użycia odcisku palca do odblokowania ekranu.

   Po dodaniu odcisku palca w ustawieniach urządzenia, użytkownik może odblokować ekran przy użyciu następujących metod:

   - Przyłóż palec do czytnika linii papilarnych (główna metoda).
   - Wprowadź hasło odblokowujące (metoda zapasowa).

8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie silnego hasła odblokowującego dla urządzeń iOS MDM

Aby chronić dane na urządzeniu iOS MDM, skonfiguruj ustawienia siły hasła odblokowującego.

Domyślnie użytkownik może użyć łatwego hasła. *Proste hasło* to hasło zawierające następujące po sobie lub powtarzające się znaki, na przykład: "abcd" lub "2222". Użytkownik nie może wprowadzić alfanumerycznego hasła, które zawiera znaki specjalne. Domyślnie, okres ważności hasła i liczba prób wprowadzenia hasła są nieograniczone.

W celu skonfigurowania ustawień siły hasła odblokowującego urządzenie iOS MDM:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie **Właściwości** wybierz sekcję **Hasło**.
5. W sekcji **Ustawienia hasła** zaznacz pole **Zastosuj ustawienia na urządzeniu**.
6. Skonfiguruj ustawienia siły hasła odblokowującego:
   - Aby umożliwić użytkownikowi używanie łatwego hasła, zaznacz opcję **Zezwól na proste hasło**.

- Aby wymagane było użycie w haśle liter i cyfr, zaznacz pole **Pytaj o wartość alfanumeryczną**.
- Na liście **Minimalna długość hasła** wybierz minimalną długość hasła w znakach.
- Na liście **Minimalna ilość znaków specjalnych** wybierz minimalną ilość znaków specjalnych w haśle (takich, jak "$", "&", "!").
- W polu **Maksymalny czas życia hasła** określ przedział czasu w dniach, w trakcie którego hasło będzie aktualne. Po minięciu tego okresu, Kaspersky Device Management for iOS informuje o konieczności zmiany hasła.
- Na liście **Włącz automatyczne blokowanie** wybierz czas, po jakim ma być włączone automatyczne blokowanie urządzenia iOS MDM.
- W polu **Historia haseł** określ liczbę użytych haseł (w tym bieżącego hasła), które Kaspersky Device Management for iOS porównuje z nowym hasłem, gdy użytkownik zmienia stare hasło. Jeśli hasła są takie same, nowe hasło jest odrzucane.
- Na liście **Maksymalny czas na odblokowanie bez hasła** wybierz czas, w trakcie którego użytkownik może odblokować urządzenie iOS MDM bez wprowadzenia hasła.
- Na liście **Maksymalna liczba prób dostępu** wybierz liczbę prób dostępu, które użytkownik może podjąć w celu wprowadzenia hasła odblokowującego urządzenie iOS MDM.

7. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, Kaspersky Device Management for iOS sprawdzi siłę hasła ustawionego na urządzeniu mobilnym użytkownika. Jeśli siła hasła odblokowującego urządzenie nie odpowiada zasadzie, użytkownik zostanie poproszony o zmianę hasła.

Konfigurowanie silnego hasła odblokowującego dla urządzeń EAS

Ustaw silne hasło odblokowujące do ochrony danych na urządzeniu EAS.

Domyślnie, jeśli urządzenie mobilne jest włączone, Kaspersky Device Management for iOS nie wyświetla pytania o wprowadzenie lub ustawienie hasła odblokowującego.

W celu skonfigurowania ustawień siły hasła odblokowującego urządzenie EAS:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia EAS.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie Właściwości wybierz sekcję **Hasło**.
5. W sekcji **Ustawienia hasła** zaznacz pole **Pytaj o hasło**.
6. Skonfiguruj ustawienia siły hasła odblokowującego:
   - Aby wymagane było użycie w haśle liter i cyfr, zaznacz pole **Pytaj o wartość alfanumeryczną**. W polu **Minimalna liczba zbiorów znaków** określ poziom siły hasła alfanumerycznego. Możliwe wartości: 1 do 4. Wartość "1" odpowiada najniższemu poziomowi siły.

- Aby zezwolić użytkownikowi na użycie funkcji odzyskiwania hasła, zaznacz pole **Włącz odzyskiwanie hasła**.
- Jeśli chcesz, żeby pliki były szyfrowane w pamięci urządzenia, zaznacz pole **Wymagaj szyfrowania na urządzeniu**.
- Jeśli chcesz, żeby pliki były szyfrowane na karcie pamięci, zaznacz pole **Wymagaj szyfrowania karty pamięci**.
- Aby umożliwić użytkownikowi używanie łatwego hasła zawierającego tylko liczby, zaznacz opcję **Zezwól na proste hasło**.
- Aby ograniczyć liczbę prób wprowadzenia hasła dostępu do urządzenia, zaznacz pole **Maksymalna liczba prób dostępu**. W polu po prawej stronie opcji do zaznaczenia określ liczbę prób wprowadzenia hasła, jaką użytkownik może podjąć w celu odblokowania urządzenia. Jeśli użytkownik niepoprawnie wprowadził hasło określoną liczbę razy z rzędu, Kaspersky Device Management for iOS usunie wszystkie dane z urządzenia.
- Aby określić minimalna długość hasła użytkownika, zaznacz pole **Minimalna długość hasła**. W polu po prawej stronie opcji do zaznaczenia określ minimalną liczbę znaków w haśle. Możliwe wartości: od 4 do 16 znaków.
- Aby wyświetlane było pytanie o wprowadzenie hasła, gdy urządzenie jest w stanie bezczynności od dłuższego czasu, zaznacz pole **Czas bezczynności do kolejnej próby wprowadzenia hasła (min)**. W polu po prawej stronie opcji do zaznaczenia określ czas bezczynności w minutach. Po upłynięciu tego czasu, aplikacja zażąda wprowadzenia hasła.
- Aby ograniczyć okres ważności hasła, zaznacz pole **Okres ważności hasła (dni)**. W polu po prawej stronie opcji do zaznaczenia określ okres ważności hasła. Po upłynięciu tego czasu, aplikacja zażąda zmiany hasła.
- W polu **Historia haseł** określ liczbę ostatnich haseł, które nie mogą zostać użyte ponownie.

7. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center. Po zastosowaniu zasady, Kaspersky Device Management for iOS sprawdzi, czy hasło jest ustawione na urządzeniu mobilnym użytkownika. Jeśli hasło odblokowujące nie zostało ustawione na urządzeniu, użytkownik zostanie poproszony o jego ustawienie. Hasło powinno być ustawione z uwzględnieniem ustawień zasady. Jeśli hasło odblokowujące urządzenie jest ustawione, ale nie odpowiada zasadzie, użytkownik zostanie poproszony o zmianę hasła.

Konfigurowanie wirtualnej sieci prywatnej (VPN)

Ta sekcja zawiera informacje na temat konfiguracji ustawień wirtualnej sieci prywatnej (VPN) w celu zapewnienia bezpiecznego połączenia z sieciami Wi-Fi.

Konfigurowanie VPN na urządzeniach Android (tylko Samsung)

Aby bezpiecznie łączyć urządzenie Android z sieciami Wi-Fi i chronić transfer danych, należy skonfigurować ustawienia dla VPN (Virtual Private Network - wirtualna sieć prywatna).

Konfiguracja VPN jest możliwa tylko dla urządzeń Samsung.

Podczas korzystania z wirtualnej sieci prywatnej należy mieć na uwadze następujące wymagania:

- Aplikacja, która korzysta z połączenia VPN, musi być dozwolona w ustawieniach Zapory sieciowej.
- Ustawienia wirtualnej sieci prywatnej, które są skonfigurowane w zasadzie, nie mogą być stosowane w aplikacjach systemowych. Połączenie VPN dla aplikacji systemowych musi być konfigurowane ręcznie.
- Niektóre aplikacje, które wykorzystują połączenie VPN, muszą posiadać dodatkowe ustawienia skonfigurowane przy pierwszym uruchomieniu. Aby skonfigurować ustawienia, połączenie VPN musi być dozwolone w ustawieniach aplikacji.

W celu skonfigurowania VPN na urządzeniu mobilnym użytkownika:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Zarządzaj Samsung KNOX → Zarządzaj urządzeniami Samsung**.
5. W sekcji **VPN** kliknij przycisk **Konfiguruj**.

   Zostanie otwarte okno **Sieć VPN**.
6. Z listy rozwijalnej **Typ połączenia** wybierz typ połączenia VPN.
7. W polu **Nazwa sieci** wprowadź nazwę kanału VPN.
8. W polu **Adres serwera** wpisz nazwę sieci lub adres IP serwera VPN.
9. Na liście **Domena/domeny wyszukiwania DNS** wpisz domenę wyszukiwania DNS, która ma zostać automatycznie dodana do nazwy serwera DNS.

   Możesz określić kilka domen wyszukiwania DNS, oddzielając je spacjami.
10. W polu **Serwer(y) DNS** wprowadź pełną nazwę domeny lub adres IP serwera DNS.

    Możesz określić kilka serwerów DNS, oddzielając je spacjami.
11. W polu **Routing** wprowadź zakres adresów IP, z którymi dane są wymieniane za pośrednictwem połączenia VPN.

    Jeśli zakres adresów IP nie jest określony w polu **Routing**, cały ruch internetowy będzie przechodził poprzez połączenie VPN.
12. Dodatkowo skonfiguruj następujące ustawienia dla sieci typów **IPSec Xauth PSK** i **L2TP IPSec PSK**:

    a. W polu **Klucz współdzielony IPSec** wprowadź hasło do predefiniowanego klucza IPSec.

    b. W polu **IPSec ID** wprowadź nazwę użytkownika urządzenia mobilnego.
13. Dla sieci **L2TP IPSec PSK** dodatkowo określ hasło do klucza L2TP w polu **Klucz L2TP**.
14. Dla sieci **PPTP** zaznacz pole **Użyj połączenia SSL**, aby aplikacja używała metody szyfrowania danych MPPE (Microsoft Point-to-Point Encryption) do zabezpieczenia transmisji danych, gdy urządzenie mobilne łączy się z serwerem VPN.
15. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie VPN na urządzeniach iOS MDM

Aby połączyć urządzenie iOS MDM z wirtualną siecią prywatną (VPN) i chronić dane podczas łączenia z VPN, skonfiguruj ustawienia połączenia z VPN.

W celu skonfigurowania połączenia z VPN na urządzeniu iOS MDM użytkownika:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie **Właściwości** wybierz sekcję **VPN**.
5. W sekcji **Sieci VPN** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Sieć VPN**.
6. W polu **Nazwa sieci** wprowadź nazwę kanału VPN.
7. Z listy rozwijalnej **Typ połączenia** wybierz typ połączenia VPN:

   - **L2TP** (Layer 2 Tunneling Protocol). Połączenie obsługuje autoryzację użytkownika urządzenia mobilnego iOS MDM przy uzyciu haseł MS-CHAP v2, uwierzytelniania dwuskładnikowe i automatycznego uwierzytelniania przy użyciu klucza publicznego.
   - **PPTP** (Point-to-Point Tunneling Protocol). Połączenie obsługuje autoryzację użytkownika urządzenia mobilnego iOS MDM przy użyciu haseł MS-CHAP v2 i uwierzytelniania dwuskładnikowego.
   - **IPSec (Cisco)**. Połączenie obsługuje autoryzację użytkownika w oparciu o hasło, uwierzytelnianie dwuskładnikowe i automatyczną autoryzację przy użyciu klucza publicznego i certyfikatów.
   - **Cisco AnyConnect**. Połączenie obsługuje zaporę sieciową Cisco Adaptive Security Appliance (ASA) w wersji 8.0(3).1 lub nowszej. Aby skonfigurować połączenie VPN, zainstaluj aplikację Cisco AnyConnect z poziomu App Store na urządzeniu mobilnym iOS MDM.
   - **Juniper SSL**. Połączenie obsługuje bramę VPN Juniper Networks SSL SA Series w wersji 6.4 lub nowszej z pakietem Juniper Networks IVE w wersji 7.0 lub nowszej. Aby skonfigurować połączenie VPN, zainstaluj aplikację JUNOS z poziomu App Store na urządzeniu mobilnym iOS MDM.
   - **F5 SSL**. Połączenie obsługuje rozwiązania SSL VPN: F5 BIG-IP Edge Gateway, Access Policy Manager oraz Fire. Aby skonfigurować połączenie VPN, zainstaluj aplikację F5 BIG-IP Edge Client z poziomu App Store na urządzeniu mobilnym iOS MDM.
   - **SonicWALL Mobile Connect**. Połączenie obsługuje urządzenia SonicWALL Aventail E-Class Secure Remote Access w wersji 10.5.4 lub nowszej, urządzenia SonicWALL SRA w wersji 5.5 lub nowszej, a także urządzenia SonicWALL Next-Generation Firewall, w tym TZ, NSA, E-Class NSA z systemem SonicOS w wersji 5.8.1.0 lub nowszej. Aby skonfigurować połączenie VPN, zainstaluj aplikację SonicWALL Mobile Connect z poziomu App Store na urządzeniu mobilnym iOS MDM.
   - **Aruba VIA**. Połączenie obsługuje kontrolery dostępu Aruba Networks. Aby je skonfigurować, zainstaluj aplikację Aruba Networks VIA z poziomu App Store na urządzeniu mobilnym iOS MDM.

- **Niestandardowy SSL**. Połączenie obsługuje autoryzację użytkownika urządzenia mobilnego iOS MDM przy użyciu haseł i certyfikatów oraz uwierzytelniania dwuskładnikowego.

8. W polu **Adres serwera** wpisz nazwę sieci lub adres IP serwera VPN.

9. W polu **Nazwa konta** wprowadź nazwę konta dla autoryzacji na serwerze VPN. Możesz użyć makr dostępnych na liście **Dostępne makra**.

10. Skonfiguruj ustawienia ochrony połączenia VPN zgodnie z wybranym typem wirtualnej sieci prywatnej.

11. Jeśli to konieczne, skonfiguruj ustawienia połączenia VPN poprzez serwer proxy:

    a. Wybierz zakładkę **Ustawienia serwera proxy**.

    b. Wybierz tryb konfiguracji serwera proxy i określ ustawienia połączenia.

    c. Kliknij **OK**.

    Ustawienia połączenia urządzenia z VPN poprzez serwer proxy zostaną skonfigurowane na urządzeniu iOS MDM.

12. Kliknij **OK**.

    Nowa sieć VPN będzie wyświetlana na liście.

13. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia połączenia z VPN zostaną skonfigurowane na urządzeniu iOS MDM użytkownika po zastosowaniu zasady.

Konfigurowanie Zapory sieciowej na urządzeniach Android (tylko Samsung)

Skonfiguruj ustawienia Zapory sieciowej, aby monitorować połączenia sieciowe na urządzeniu mobilnym użytkownika.

W celu skonfigurowania Zapory sieciowej na urządzeniu mobilnym:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.

4. W oknie **Właściwości** wybierz sekcję **Zarządzaj Samsung KNOX → Zarządzaj urządzeniami Samsung**.

5. W oknie **Zapora sieciowa** kliknij **Konfiguruj**.

   Zostanie otwarte okno **Zapora sieciowa**.

6. Wybierz tryb Zapory sieciowej:

   - Aby zezwolić na wszystkie połączenia przychodzące i wychodzące, przesuń suwak na **Zezwól na wszystko**.

   - Aby blokować całą aktywność sieciową za wyjątkiem aplikacji na liście wykluczeń, przesuń suwak na **Blokuj wszystkie, za wyjątkiem wykluczonych**.

7. Jeśli ustawiłeś tryb Zapory sieciowej na **Blokuj wszystkie, za wyjątkiem wykluczonych**, utwórz listę wykluczeń:

   a. Kliknij **Dodaj**.

   Zostanie otwarte okno **Wykluczenie dla Zapory sieciowej**.

   b. W polu **Nazwa aplikacji** wprowadź nazwę aplikacji mobilnej.

   c. W polu **Nazwa pakietu** wprowadź nazwę systemową pakietu aplikacji mobilnej (na przykład `com.mobileapp.example`).

   d. Kliknij **OK**.

8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Ochrona Kaspersky Endpoint Security for Android przed odinstalowaniem

Aby urządzenie mobilne było chronione i zgodne z firmowymi wymaganiami bezpieczeństwa, możesz włączyć ochronę przed odinstalowaniem Kaspersky Endpoint Security for Android. W tej sytuacji użytkownik nie będzie mógł usunąć aplikacji z poziomu interfejsu Kaspersky Endpoint Security for Android. Podczas dezinstalacji aplikacji przy pomocy narzędzi systemu operacyjnego Android zostanie wyświetlone pytanie o wyłączenie uprawnień administratora dla Kaspersky Endpoint Security for Android. Po wyłączeniu uprawnień, urządzenie mobilne zostanie zablokowane.

Na pewnych urządzeniach Samsung działających pod kontrolą systemu Android 7.0 lub nowszego, jeśli użytkownik spróbuje skonfigurować nieobsługiwane metody odblokowania urządzenia (na przykład, wzór), urządzenie może zostać zablokowane, gdy spełnione będą następujące warunki: włączona jest ochrona przed dezinstalacją Kaspersky Endpoint Security for Android oraz ustawione są wymagania wobec siły hasła odblokowującego ekran. Aby odblokować urządzenie, należy wysłać specjalne polecenie na urządzenie.

W celu włączenia ochrony przed odinstalowaniem Kaspersky Endpoint Security for Android:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.

4. W oknie **Właściwości** wybierz sekcję **Dodatkowe**.

5. W sekcji **Usuwanie Kaspersky Endpoint Security for Android** odznacz pole **Zezwól na usuwanie Kaspersky Endpoint Security for Android**.

   Aby chronić aplikację przed usunięciem na urządzeniach działających pod kontrolą systemu Android 7.0 lub nowszego, Kaspersky Endpoint Security for Android musi być ustawiony jako usługa funkcji Dostępności. Jeśli Kreator wstępnej konfiguracji jest uruchomiony, Kaspersky Endpoint Security for Android wyświetli pytanie o nadanie aplikacji wszystkich wymaganych uprawnień. Użytkownik może pominąć te kroki lub wyłączyć te uprawnienia w ustawieniach urządzenia w późniejszym czasie. W takim przypadku aplikacja nie jest chroniona przed dezinstalacją.

6. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center. Jeśli zostanie podjęta próba usunięcia aplikacji, urządzenie mobilne zostanie zablokowane.

Wykrywanie hackowania urządzenia (root)

Kaspersky Security for Mobile umożliwia wykrywanie hackowania urządzenia (root). Pliki systemowe są niezabezpieczone na zhackowanym urządzeniu i dlatego mogą być modyfikowane. Ponadto aplikacje firm trzecich z nieznanych źródeł mogą być instalowane na zhakowanych urządzeniach. Po wykryciu próby włamania, zalecamy natychmiastowe przywrócenie normalnego działania urządzenia.

Aby wykryć, kiedy użytkownik uzyskuje uprawnienia root, Kaspersky Endpoint Security for Android korzysta z następujących usług:

- *Wbudowana usługa Kaspersky Endpoint Security for Android* to usługa Kaspersky, która sprawdza, czy użytkownik urządzenia mobilnego uzyskał uprawnienia root (Kaspersky Mobile Security SDK).

- *SafetyNet Attestation* to usługa Google, która sprawdza integralność systemu operacyjnego, analizuje sprzęt i oprogramowanie urządzenia oraz identyfikuje inne problemy z bezpieczeństwem. Więcej informacji na temat usługi zaświadczania SafetyNet Attestation można znaleźć na stronie Centrum pomocy produktu Android.

Jeśli urządzenie zostało zhakowane, otrzymasz powiadomienie. Możesz wyświetlić powiadomienia o włamaniu w obszarze roboczym Serwera administracyjnego, na zakładce **Monitorowanie**. Możesz także wyłączyć powiadomienia dotyczące włamań w ustawieniach powiadomień o zdarzeniach.

Na urządzeniach działających pod kontrolą systemu Android możesz nałożyć ograniczenia dotyczące aktywności użytkownika w przypadku, gdy urządzeni zostanie zhakowane (na przykład, zablokować urządzenie) Możesz nałożyć ograniczenia przy użyciu modułu Kontrola zgodności (patrz rysunek poniżej). W tym celu, w ustawieniach zasad skanowania wybierz kryterium **Został przeprowadzony jailbreak systemu**.

Konfigurowanie globalnego serwera proxy HTTP na urządzeniach iOS MDM

Aby chronić ruch internetowy na urządzeniu użytkownika, skonfiguruj ustawienia połączenia urządzenia iOS MDM z internetem poprzez serwer proxy.

Automatyczne połączenie z internetem poprzez serwer proxy jest dostępne tylko dla kontrolowanych urządzeń.

W celu skonfigurowania ustawień globalnego serwera proxy HTTP na urządzeniu iOS MDM użytkownika:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.

4. W oknie **Właściwości** wybierz sekcję **Globalny serwer pośredniczący HTTP**.

5. W sekcji **Ustawienia globalnego serwera proxy HTTP** zaznacz pole **Zastosuj ustawienia na urządzeniu**.

6. Wybierz typ konfiguracji globalnego serwera proxy HTTP.

Domyślnie, wybrany jest ręczny typ konfiguracji globalnego serwera proxy HTTP, a użytkownik nie może nawiązywać połączenia z sieciami wymagającymi wstępnego uwierzytelniania bez połączenia z serwerem proxy. *Sieci wymagające uwierzytelniania* to sieci bezprzewodowe, które wymagają wstępnej autoryzacji na urządzeniu mobilnym bez łączenia z serwerem proxy.

- W celu ręcznego określenia ustawień połączenia z serwerem proxy:

  a. Z listy rozwijalnej **Typ ustawień proxy** wybierz **Ręcznie**.

  b. W polu **Adres serwera proxy i port** wprowadź nazwę hosta lub adres IP serwera proxy oraz numer portu serwera proxy.

  c. W polu **Nazwa użytkownika** określ nazwę konta użytkownika do autoryzacji na serwerze proxy. Możesz użyć makr dostępnych na liście **Dostępne makra**.

  d. W polu **Hasło** określ hasło do konta użytkownika do autoryzacji na serwerze proxy.

  e. Aby zezwolić użytkownikowi na korzystanie z sieci wymagających uwierzytelniania, zaznacz pole **Zezwól na dostęp do sieci publicznych wymagających logowania bez łączenia z proxy**.

- W celu skonfigurowania ustawień połączenia z serwerem proxy przy użyciu predefiniowanego pliku PAC (Proxy Auto Configuration):

  a. Z listy rozwijalnej **Typ ustawień proxy** wybierz **Automatycznie**.

  b. W polu **URL pliku PAC** wprowadź adres internetowy pliku PAC (na przykład: http://www.example.com/filename.pac).

  c. Aby zezwolić użytkownikowi na połączenie urządzenia mobilnego z siecią bezprzewodową bez użycia serwera proxy, gdy nie można uzyskać dostępu do pliku PAC, zaznacz pole **Zezwól na bezpośrednie połączenie, jeśli nie można uzyskać dostępu do pliku PAC**.

  d. Aby zezwolić użytkownikowi na korzystanie z sieci wymagających uwierzytelniania, zaznacz pole **Zezwól na dostęp do sieci publicznych wymagających logowania bez łączenia z proxy**.

7. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, użytkownik urządzenia mobilnego nawiąże połączenie z internetem poprzez serwer proxy.

Dodawanie nowych certyfikatów zabezpieczeń na urządzeniach iOS MDM

Aby uprościć uwierzytelnianie użytkownika i zapewnić bezpieczeństwo danych, dodaj certyfikaty na urządzeniu iOS MDM użytkownika. Dane podpisane przy użyciu certyfikatu są chronione przed modyfikacją podczas wymiany sieci. Szyfrowanie danych przy użyciu certyfikatu zapewnia dodatkowy poziom ochrony danych. Certyfikat może zostać użyty także do zweryfikowania tożsamości użytkownika.

Kaspersky Device Management for iOS obsługuje następujące standardy certyfikatów:

- **PKCS#1** – szyfrowanie przy użyciu klucza publicznego w oparciu o algorytmy RSA.
- **PKCS#12** – przechowywanie i przesyłanie certyfikatu i klucza prywatnego.

W celu dodania certyfikatu zabezpieczenia na urządzeniu iOS MDM użytkownika:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie **Właściwości** wybierz sekcję **Certyfikaty**.
5. W sekcji **Certyfikaty** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Certyfikat**.
6. W polu **Nazwa pliku** określ ścieżkę do certyfikatu:

   Pliki certyfikatów PKCS#1 posiadają rozszerzenia cer, crt lub der. Pliki certyfikatów PKCS#12 posiadają rozszerzenia p12 lub pfx.
7. Kliknij **Otwarta**.

   Jeśli certyfikat jest chroniony hasłem, określ hasło. Nowy certyfikat pojawi się na liście.
8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, zostanie wyświetlone pytanie o zainstalowanie certyfikatów z utworzonej listy.

Dodawanie profilu SCEP na urządzeniach iOS MDM

Profil SCEP należy dodać w celu umożliwienia użytkownikowi urządzenia iOS MDM automatyczne pobieranie certyfikatów z Centrum certyfikacji poprzez internet. Profil SCEP umożliwia obsługę protokołu Simple Certificate Enrollment Protocol.

Domyślnie dodawany jest profil SCEP z następującymi ustawieniami:

- Alternatywna nazwa podmiotu nie jest używana do rejestracji certyfikatów.
- Podejmowane są trzy próby przeszukiwania serwera SCEP w odstępach 10-sekundowych. Jeśli wszystkie próby podpisania certyfikatu nie powiodły się, powinieneś wygenerować nowe żądanie podpisania certyfikatu.
- Otrzymany certyfikat nie może zostać użyty do podpisania ani do szyfrowania danych.

Możesz zmodyfikować określone ustawienia podczas dodawania profilu SCEP.

W celu dodania profilu SCEP:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.

4. W oknie **Właściwości** wybierz sekcję **SCEP**.

5. W sekcji **Profile SCEP** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Profil SCEP**.

6. W polu **Adres internetowy serwera** wprowadź adres internetowy serwera SCEP, na którym znajduje się Centrum certyfikacji.

   Adres internetowy zawiera adres IP lub pełną nazwę domeny (FQDN). Na przykład: http://10.10.10.10/certserver/companyscep.

7. W polu **Nazwa** wprowadź nazwę Centrum certyfikacji znajdującego się na serwerze SCEP.

8. W polu **Podmiot** wprowadź wiersz z atrybutami użytkownika urządzenia iOS MDM, które znajdują się w certyfikacie X.500.

   Atrybuty mogą zawierać szczegóły dotyczące kraju (C), organizacji (O) i standardowej nazwy użytkownika (CN). Na przykład: /C=RU/O=MyCompany/CN=User/. Możesz użyć innych atrybutów określonych w RFC 5280.

9. Z listy rozwijalnej **Typ alternatywnej nazwy podmiotu** wybierz typ alternatywnej nazwy podmiotu serwera SCEP:

   - **Nie** – identyfikacja przy użyciu alternatywnej nazwy nie jest wykorzystywana.
   - **Nazwa RFC 822** – identyfikacja przy użyciu adresu e-mail. Adres e-mail należy określić zgodnie z RFC 822.
   - **Nazwa DNS** – identyfikacja przy użyciu nazwy domeny.
   - **URI** – identyfikacja przy użyciu adresu IP lub adresu w formacie FQDN.

   Alternatywną nazwę podmiotu można użyć do identyfikacji użytkownika urządzenia mobilnego iOS MDM.

10. W polu **Alternatywna nazwa podmiotu** wprowadź alternatywną nazwę podmiotu certyfikatu X.500. Wartość alternatywnej nazwy podmiotu zależy od jego typu: adres e-mail użytkownika, domena lub adres internetowy.

11. W polu **Nazwa podmiotu NT** wpisz nazwę DNS użytkownika urządzenia mobilnego iOS MDM w sieci Windows NT.

    Nazwa podmiotu NT jest zawarta w żądaniu certyfikatu wysyłanym do serwera SCEP.

12. W polu **Liczba prób przeszukiwania na serwerze SCEP** określ maksymalną liczbę prób przeszukiwania na serwerze SCEP w celu uzyskania podpisanego certyfikatu.

13. W polu **Częstotliwość prób (w sekundach)** określ przedział czasu w sekundach pomiędzy próbami przeszukiwania serwera SCEP w celu uzyskania podpisanego certyfikatu.

14. W polu **Żądanie rejestracji** wprowadź wcześniej opublikowany klucz rejestracji.

    Przed podpisaniem certyfikatu serwer SCEP żąda od użytkownika urządzenia mobilnego klucza. Jeśli to pole pozostanie puste, SCEP nie będzie żądał klucza.

15. Z listy rozwijalnej **Rozmiar klucza** wybierz rozmiar klucza rejestracji w bitach: 1024 lub 2048.

16. Jeśli chcesz zezwolić użytkownikowi na używanie certyfikatu pobranego z serwera SCEP jako certyfikatu podpisywania, zaznacz pole **Użyj do podpisywania**.

17. Jeśli chcesz zezwolić użytkownikowi na używanie certyfikatu pobranego z serwera SCEP do szyfrowania danych, zaznacz pole **Użyj do szyfrowania**.

Nie można używać certyfikatu serwera SCEP jako certyfikatu podpisywania danych i certyfikatu szyfrowania danych jednocześnie.

18. W polu **Odcisk palca certyfikatu** wprowadź unikatowy odcisk palca certyfikatu do sprawdzenia autentyczności odpowiedzi z Centrum certyfikacji. Można go użyć z algorytmem haszującym SHA-1 lub MD5. Odcisk palca certyfikatu można skopiować ręcznie lub wybrać certyfikat, korzystając z przycisku **Utwórz z certyfikatu**. Jeśli odcisk palca jest tworzony przy użyciu przycisku **Utwórz z certyfikatu**, zostanie automatycznie dodany do pola.

    Odcisk palca certyfikatu musi zostać określony, jeśli wymiana danych pomiędzy urządzeniem mobilnym a Centrum certyfikacji odbywa się po protokole HTTP.

19. Kliknij **OK**.

    Nowy profil SCEP pojawi się na liście.

20. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, urządzenie mobilne użytkownika jest konfigurowane do automatycznego pobierania certyfikatu z Centrum certyfikacji poprzez internet.

Kontrola

Ta sekcja zawiera informacje dotyczące zdalnego monitorowania urządzeń mobilnych w Konsoli administracyjnej Kaspersky Security Center.

Konfigurowanie ograniczeń

Ta sekcja opisuje sposób konfiguracji dostępu użytkowników do funkcji urządzeń mobilnych.

Specjalne uwagi dotyczące urządzeń z systemem Android w wersji 10 lub nowszej

Android 10 wprowadził liczne zmiany i ograniczenia dotyczące interfejsu API 29 lub nowszego. Niektóre z tych zmian wpływają na dostępność lub funkcjonalność niektórych funkcji aplikacji. Te uwagi dotyczą tylko urządzeń z systemem Android 10 lub nowszym.

Możliwość włączania, wyłączania i konfigurowania Wi-Fi

- Sieci Wi-Fi można dodawać, usuwać i konfigurować w Konsoli administracyjnej Kaspersky Security Center. Gdy sieć Wi-Fi jest dodana do zasady, Kaspersky Endpoint Security otrzymuje tę konfigurację sieci podczas pierwszego połączenia z Kaspersky Security Center.

- Gdy urządzenie wykryje sieć skonfigurowaną przez Kaspersky Security Center, Kaspersky Endpoint Security poprosi użytkownika o połączenie się z tą siecią. Jeśli użytkownik zdecyduje się połączyć z siecią, wszystkie ustawienia skonfigurowane przez Kaspersky Security Center zostaną zastosowane automatycznie. Następnie urządzenie automatycznie łączy się z tą siecią, gdy jest w zasięgu, bez wyświetlania dalszych powiadomień użytkownikowi.

- Jeśli urządzenie użytkownika jest już połączone z inną siecią Wi-Fi, czasami użytkownik może nie zostać poproszony o zatwierdzenie dodania sieci. W takich przypadkach użytkownik musi wyłączyć i ponownie włączyć Wi-Fi, aby otrzymać sugestię.

- Gdy Kaspersky Endpoint Security zasugeruje użytkownikowi połączenie się z siecią Wi-Fi, a użytkownik odmówi, uprawnienia aplikacji do zmiany stanu Wi-Fi zostaną cofnięte. Kaspersky Endpoint Security nie może wówczas proponować połączenia z sieciami Wi-Fi, dopóki użytkownik nie udzieli ponownie uprawnienia, przechodząc do sekcji **Ustawienia** → **Aplikacje i powiadomienia** → **Specjalny dostęp do aplikacji** → **Zarządzanie połączeniem Wi-Fi** → **Kaspersky Endpoint Security**.

- Obsługiwane są tylko otwarte sieci i sieci z szyfrowaniem WPA2-PSK. Szyfrowania WEP i WPA nie są obsługiwane.

- Jeśli hasło do sieci sugerowanej wcześniej przez aplikację zostanie zmienione, użytkownik musi ręcznie usunąć tę sieć z listy znanych sieci. Urządzenie będzie wtedy mogło otrzymać propozycję sieci od Kaspersky Endpoint Security i połączyć się z nią.

- Gdy system operacyjny urządzenia zostanie zaktualizowany z systemu Android w wersji 9 lub wcześniejszej do systemu Android w wersji 10 lub nowszej i/lub Kaspersky Endpoint Security zainstalowany na urządzeniu z systemem Android w wersji 10 lub nowszej zostanie zaktualizowany, sieci, które zostały wcześniej dodane za pośrednictwem Kaspersky Security Center, nie mogą być modyfikowane lub usuwane za pośrednictwem zasad Kaspersky Security Center. Użytkownik może jednak ręcznie modyfikować lub usuwać takie sieci ręcznie w ustawieniach urządzenia.

- Na urządzeniach z systemem Android 10 użytkownik jest proszony o podanie hasła przy próbie ręcznego połączenia się z chronioną sugerowaną siecią. Połączenie automatyczne nie wymaga wprowadzania hasła. Jeśli urządzenie użytkownika jest podłączone do innej sieci Wi-Fi, użytkownik musi najpierw rozłączyć się z tą siecią, aby automatycznie połączyć się z jedną z sugerowanych sieci.

- Na urządzeniach z systemem Android 11 użytkownik może ręcznie połączyć się z chronioną siecią sugerowaną przez aplikację bez konieczności wprowadzania hasła.

- Po usunięciu Kaspersky Endpoint Security z urządzenia, sieci proponowane wcześniej przez aplikację są ignorowane.

- Zabronienie korzystania z sieci Wi-Fi nie jest obsługiwane.

Dostęp do aparatu

- Na urządzeniach z systemem Android 10 nie można całkowicie zabronić korzystania z aparatu. Nadal dostępne jest zabronienie używania aparatu w profilu roboczym.

- Jeśli aplikacja innej firmy spróbuje uzyskać dostęp do aparatu urządzenia, zostanie ona zablokowana, a użytkownik zostanie powiadomiony o problemie. Nie można jednak blokować aplikacji korzystających z aparatu podczas działania w tle.

- Po odłączeniu kamery zewnętrznej od urządzenia w niektórych przypadkach może zostać wyświetlone powiadomienie o niedostępności kamery.

Zarządzanie metodami odblokowywania ekranu

- Kaspersky Endpoint Security przetwarza teraz wymagania dotyczące mocy hasła na jedną z wartości systemowych: średnią lub wysoką.

- Jeśli wymagana długość hasła wynosi od 1 do 4 symboli, aplikacja prosi użytkownika o ustawienie hasła o średniej mocy. Musi być numeryczne (PIN) bez powtarzających się lub uporządkowanych (np. 1234) sekwencji lub alfanumeryczne. Kod PIN lub hasło musi mieć co najmniej 4 znaki.

- Jeśli wymagana długość hasła to 5 lub więcej symboli, aplikacja prosi użytkownika o ustawienie silnego hasła. Musi być numeryczne (PIN) bez powtarzających się lub uporządkowanych sekwencji lub alfanumeryczne (hasło). Kod PIN musi mieć co najmniej 8 cyfr; hasło musi mieć co najmniej 6 znaków.

- Używanie odcisku palca do odblokowywania ekranu jest możliwe tylko w przypadku profilu roboczego.

Konfigurowanie ograniczeń dla urządzeń Android

Aby zabezpieczyć urządzenie Android, skonfiguruj ustawienia korzystania z Wi-Fi, aparatu i Bluetooth na urządzeniu.

Domyślnie, użytkownik może korzystać z Wi-Fi, aparatu i Bluetooth na urządzeniu bez ograniczeń.

W celu skonfigurowania ograniczeń korzystania z Wi-Fi, aparatu i Bluetooth na urządzeniu:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.

4. W oknie **Właściwości** wybierz sekcję **Zarządzanie urządzeniami**.

5. W sekcji **Ograniczenia** skonfiguruj korzystanie z Wi-Fi, aparatu i Bluetooth:

   - Aby na urządzeniu mobilnym użytkownika wyłączyć moduł Wi-Fi, zaznacz pole **Zabroń korzystania z Wi-Fi**.

     Na urządzeniach z Androidem 10.0 lub nowszym blokowanie korzystania z sieci Wi-Fi nie jest obsługiwane.

   - Aby na urządzeniu mobilnym użytkownika wyłączyć aparat, zaznacz pole **Zabroń korzystania z aparatu**.

     Na urządzeniach z systemem Android 10.0 lub nowszym nie można całkowicie zabronić korzystania z aparatu.

     Na urządzeniach działających pod kontrolą systemu Android 11 lub nowszego, Kaspersky Endpoint Security for Android musi być ustawiony jako funkcja ułatwień dostępu. Kaspersky Endpoint Security for Android wyświetli pytanie o ustawienie aplikacji jako usługę funkcji Dostępności poprzez Kreator wstępnej konfiguracji. Użytkownik może pominąć ten krok lub wyłączyć tę usługę w ustawieniach urządzenia w późniejszym czasie. W takim przypadku nie będzie można ograniczyć korzystania z aparatu.

   - Aby na urządzeniu mobilnym użytkownika wyłączyć Bluetooth, zaznacz pole **Zabroń korzystania z Bluetooth**.

Na urządzeniach z systemem Andoid w wersji 12 lub nowszej korzystanie z Bluetooth można wyłączyć tylko, jeśli użytkownik urządzenia przydzielił uprawnienie **Urządzenia Bluetooth w pobliżu**. Użytkownik może przyznać to uprawnienie w trakcie działania Kreatora wstępnej konfiguracji lub później.

6. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie ograniczeń funkcji urządzeń iOS MDM

Aby zapewnić zgodność z firmowymi wymaganiami bezpieczeństwa, skonfiguruj ograniczenia działania urządzenia iOS MDM.

W celu skonfigurowania ograniczeń funkcji urządzenia iOS MDM:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie **Właściwości** wybierz sekcję **Ograniczenia funkcji**.
5. W sekcji **Ustawienia ograniczeń funkcji** zaznacz pole **Zastosuj ustawienia na urządzeniu**.
6. Skonfiguruj ograniczenia funkcji urządzenia iOS MDM.
7. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.
8. Wybierz sekcję **Ograniczenia dla aplikacji**.
9. W sekcji **Ustawienia ograniczeń aplikacji** zaznacz pole **Zastosuj ustawienia na urządzeniu**.
10. Skonfiguruj ograniczenia dla aplikacji na urządzeniu iOS MDM.
11. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.
12. Wybierz sekcję **Ograniczenia dla multimediów**.
13. W sekcji **Ustawienia ograniczeń treści multimedialnych** zaznacz pole **Zastosuj ustawienia na urządzeniu**.
14. Skonfiguruj ograniczenia dla treści multimedialnych na urządzeniu iOS MDM.
15. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, ograniczenia dla funkcji, aplikacji i multimediów zostaną skonfigurowane na urządzeniu mobilnym użytkownika.

Konfigurowanie ograniczeń funkcji urządzeń EAS

Skonfiguruj ograniczenia funkcji urządzenia w celu zapewnienia bezpieczeństwa urządzenia EAS.

Domyślnie, użytkownik może korzystać z funkcji urządzenia EAS bez ograniczeń.

W celu skonfigurowania ograniczeń dotyczących funkcji urządzenia EAS:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia EAS.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie Właściwości wybierz sekcję **Ograniczenia funkcji**.
5. W sekcji **Ustawienia ograniczeń funkcji** zezwól na lub zablokuj korzystanie z funkcji urządzenia EAS:
   - Aby zezwolić na podłączanie kart pamięci i innych nośników wymiennych do urządzenia, zaznacz pole **Zezwól na dyski wymienne**.
   - Aby zezwolić na korzystanie z aparatu, zaznacz pole **Zezwól na korzystanie z kamery**.
   - Aby zezwolić na połączenia z sieciami Wi-Fi, zaznacz pole **Zezwól na korzystanie z Wi-Fi**.
   - Aby zezwolić na korzystanie z portów podczerwieni, zaznacz pole **Zezwól na połączenia wykorzystujące podczerwień**.
   - Aby zezwolić na wykorzystywanie urządzenia jako punktu dostępowego Wi-Fi do tworzenia sieci bezprzewodowej, zaznacz pole **Zezwól na użycie urządzenia jako punktu dostępowego Wi-Fi**.
   - Aby zezwolić na łączenie urządzenia ze zdalnym pulpitem, zaznacz pole **Zezwól na połączenie pulpitu zdalnego**.
   - Aby zezwolić na użycie klienta Desktop ActiveSync na urządzeniu, zaznacz pole **Zezwól na synchronizację pulpitu**.
   - Na liście rozwijalnej **Użycie Bluetooth** zezwól na lub zablokuj użycie Bluetooth na urządzeniu EAS:
     - **Zezwól**. Użycie Bluetooth na urządzeniu mobilnym jest dozwolone.
     - **Podczas korzystania z telefonu głośnomówiącego**. Użycie Bluetooth jest dozwolone, gdy bezprzewodowy zestaw słuchawkowy jest podłączony do urządzenia mobilnego.
     - **Odmów**. Użycie Bluetooth na urządzeniu mobilnym jest zablokowane.
6. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie dostępu użytkownika do stron internetowych

Ta sekcja opisuje sposób konfiguracji dostępu do stron internetowych na urządzeniach Android i iOS.

Konfigurowanie dostępu do stron internetowych na urządzeniach Android

Możesz użyć Ochrony WWW do skonfigurowania dostępu użytkowników urządzeń Android do stron internetowych. Ochrona WWW obsługuje również filtrowanie stron internetowych według kategorii zdefiniowanych w usłudze chmury Kaspersky Security Network. Filtrowanie umożliwia ograniczenie dostępu użytkownika do pewnych stron internetowych lub kategorii stron internetowych (na przykład do stron z kategorii "Hazard, loterie, zakłady bukmacherskie" lub "Komunikacja przez internet"). Ochrona WWW chroni także dane osobowe użytkowników w internecie.

Kaspersky Endpoint Security for Android musi być ustawiony jako funkcja dostępności. Kaspersky Endpoint Security for Android wyświetli pytanie o ustawienie aplikacji jako usługę funkcji Dostępności poprzez Kreator wstępnej konfiguracji. Użytkownik może pominąć ten krok lub wyłączyć tę usługę w ustawieniach urządzenia w późniejszym czasie. W takiej sytuacji Ochrona WWW nie będzie działać.

Ochrona WWW na urządzeniach z systemem Android działa tylko w przeglądarkach: Huawei Browser, Google Chrome (włączając funkcję Kart niestandardowych) i Samsung Internet Browser. Ochrona WWW dla przeglądarki Samsung Internet Browser nie blokuje stron na urządzeniu mobilnym, jeśli profil roboczy jest używany, a Ochrona WWW jest włączona tylko dla profilu roboczego.

Ochrona WWW jest włączona domyślnie: dostęp użytkownika do stron internetowych z kategorii **Phishing** i **Szkodliwe oprogramowanie** jest zablokowany.

W celu skonfigurowania ustawień dostępu użytkownika urządzenia do stron internetowych:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz **Ochrona WWW**.
5. Zaznacz pole **Włącz Ochronę WWW**.
6. Aby korzystać z modułu Ochrona WWW, Ty lub użytkownik urządzenia powinien przeczytać i zaakceptować Oświadczenie dotyczące przetwarzania danych na potrzeby modułu Ochrona WWW (Oświadczenie dotyczące modułu Ochrona WWW):
   a. Kliknij odnośnik **Oświadczenie dotyczące modułu Ochrona WWW**.

      Spowoduje to otwarcie okna **Oświadczenie dotyczące przetwarzania danych na potrzeby modułu Ochrona WWW**. Aby zaakceptować Oświadczenie dotyczące modułu Ochrona WWW, należy przeczytać i zaakceptować Politykę prywatności.

   b. Kliknij odnośnik Polityka prywatności. Przeczytaj i zaakceptuj Politykę prywatności.

      Jeśli nie zaakceptujesz Polityki prywatności, użytkownik urządzenia mobilnego może zaakceptować Politykę prywatności w Kreatorze wstępnej konfiguracji lub w aplikacji (→ **Informacje o aplikacji** → **Warunki i postanowienia** → **Politykę prywatności**).

   c. Wybierz tryb zaakceptowania Oświadczenia dotyczącego modułu Ochrona WWW:

- **Przeczytałem i akceptuję Oświadczenie dotyczące modułu Ochrona WWW**
- **Wymagaj akceptacji przez użytkownika urządzenia Oświadczenia dotyczącego modułu Ochrona WWW**
- **Nie akceptuję Oświadczenia dotyczącego modułu Ochrona WWW**

Jeśli wybierzesz **Nie akceptuję Oświadczenia dotyczącego modułu Ochrona WWW**, Ochrona WWW nie zablokuje stron na urządzeniu mobilnym. Użytkownik urządzenia mobilnego nie może włączyć modułu Ochrona WWW w Kaspersky Endpoint Security.

7. Jeśli chcesz, żeby aplikacja ograniczała dostęp użytkownika do stron internetowych w zależności od ich zawartości, wykonaj następujące czynności:
   a. W sekcji **Ochrona WWW**, z listy rozwijalnej wybierz **Strony internetowe z wybranych kategorii są zabronione**.
   b. Utwórz listę zablokowanych kategorii, zaznaczając pola obok kategorii stron internetowych, do których aplikacja będzie blokowała dostęp.
8. Jeśli chcesz, żeby aplikacja zezwalała użytkownikowi na dostęp do stron internetowych określonych przez administratora, wykonaj następujące czynności:
   a. W sekcji **Ochrona WWW**, z listy rozwijalnej wybierz **Dozwolone są jedynie strony internetowe znajdujące się na liście**.
   b. Utwórz listę stron internetowych, dodając adresy stron internetowych, do których aplikacja nie będzie blokowała dostępu. Kaspersky Endpoint Security for Android obsługuje tylko wyrażenia regularne. Podczas wprowadzania adresu dozwolonej strony internetowej należy skorzystać z następującego szablonu:
      - `http:\/\/www\.example\.com.*` — wszystkie strony potomne strony internetowej są dozwolone (na przykład: `http://www.example.com/about`).
      - `https:\/\/.*example\.com` — wszystkie poddomeny strony internetowej są dozwolone (na przykład: `https://pictures.example.com`).

      Możesz także użyć wyrażenia `https?`, aby wybrać protokoły HTTP i HTTPS. Więcej informacji na temat wyrażeń regularnych można znaleźć na stronie asysty technicznej Oracle.
9. Jeśli chcesz, żeby aplikacja blokowała użytkownikowi dostęp do wszystkich stron internetowych, w sekcji **Ochrona WWW**, z listy rozwijalnej wybierz **Wszystkie strony internetowe są zablokowane**.
10. Aby znieść ograniczenia dotyczące dostępu do stron internetowych oparte na zawartości, odznacz pole **Włącz Ochronę WWW**.
11. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie dostępu do stron internetowych na urządzeniach iOS MDM

Skonfiguruj ustawienia Ochrony WWW, aby kontrolować dostęp do stron internetowych dla użytkowników urządzeń iOS MDM. Ochrona WWW kontroluje dostęp użytkownika do stron internetowych w oparciu o listy dozwolonych i zablokowanych stron internetowych. Ochrona WWW umożliwia także dodanie zakładek stron internetowych na panelu zakładek w Safari.

Domyślnie, dostęp do stron internetowych nie jest ograniczony.

Ustawienia Ochrony WWW można skonfigurować tylko dla urządzeń nadzorowanych.

W celu skonfigurowania dostępu do stron internetowych na urządzeniu iOS MDM użytkownika:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie **Właściwości** wybierz sekcję **Ochrona WWW**.
5. W sekcji **Ustawienia Ochrony WWW** zaznacz pole **Zastosuj ustawienia na urządzeniu**.
6. W celu zablokowania dostępu do blokowanych stron internetowych i zezwolenia na dostęp do dozwolonych stron internetowych:
   a. Z listy rozwijalnej **Tryb filtrowania sieci** wybierz tryb **Ogranicz treści dla dorosłych**.
   b. W sekcji **Dozwolone strony internetowe** utwórz listę dozwolonych stron internetowych.
      Adres strony internetowej powinien rozpoczynać się od `"http://"` lub `"https://"`. Kaspersky Device Management for iOS zezwala na dostęp do wszystkich stron internetowych w domenie. Na przykład, jeśli dodałeś adres http://www.example.com do listy dozwolonych stron internetowych, dostęp będzie dozwolony do http://pictures.example.com i http://example.com/movies. Jeśli lista dozwolonych stron internetowych jest pusta, aplikacja zezwoli na dostęp do wszystkich stron internetowych innych niż te znajdujące się na liście blokowanych stron internetowych.
   c. W sekcji **Zabronione strony internetowe** utwórz listę zablokowanych stron internetowych.
      Adres strony internetowej powinien rozpoczynać się od `"http://"` lub `"https://"`. Kaspersky Device Management for iOS blokuje dostęp do wszystkich stron internetowych w domenie.
7. W celu zablokowania dostępu do wszystkich stron internetowych innych niż dozwolone strony internetowe na liście zakładek:
   a. Z listy rozwijalnej **Tryb filtrowania sieci** wybierz tryb **Zezwól tylko na strony internetowe dodane do zakładek**.
   b. W sekcji **Zakładki** utwórz listę zakładek dozwolonych stron internetowych.
      Adres strony internetowej powinien rozpoczynać się od `"http://"` lub `"https://"`. Kaspersky Device Management for iOS zezwala na dostęp do wszystkich stron internetowych w domenie. Jeśli lista zakładek jest pusta, aplikacja zezwala na dostęp do wszystkich stron internetowych. Kaspersky Device Management for iOS doda strony internetowe z listy zakładek na karcie zakładek w Safari na urządzeniu mobilnym użytkownika.
8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, Ochrona WWW zostanie skonfigurowana na urządzeniu mobilnym użytkownika zgodnie z wybranym trybem i utworzonymi listami.

Kontrola zgodności urządzeń Android z firmowymi wymaganiami bezpieczeństwa

Możesz kontrolować urządzenia Android pod kątem zgodności z firmowymi wymaganiami bezpieczeństwa. Firmowe wymagania bezpieczeństwa regulują sposób pracy użytkownika z urządzeniem. Na przykład, ochrona w czasie rzeczywistym musi być włączona na urządzeniu, antywirusowe bazy danych muszą być aktualne, a hasło do urządzenia musi być wystarczająco silne. Kontrola zgodności opiera się na liście reguł. Reguła zgodności obejmuje następujące komponenty:

- Kryterium sprawdzania urządzenia (na przykład, brak zablokowanych aplikacji na urządzeniu).
- Czas, jaki użytkownik ma na wyeliminowanie braku zgodności (na przykład 24 godziny).
- Działanie, jakie zostanie podjęte na urządzeniu, jeśli użytkownik nie wyeliminuje niezgodności w określonym przedziale czasu (na przykład, zablokowanie urządzenia).

  W systemie Android 12 lub nowszych aplikacja może wykonać to zadanie później niż określono, jeśli urządzenie jest w trybie oszczędzania baterii.

Jeśli użytkownik nie wyeliminuje braku zgodności w ciągu określonego czasu, dostępne będą następujące działania:

- **Blokuj wszystkie aplikacje poza systemowymi**. Zablokowane jest uruchamianie wszystkich aplikacji na urządzeniu mobilnym użytkownika, za wyjątkiem aplikacji systemowych.
- **Zablokuj urządzenie**. Urządzenie mobilne jest zablokowane. Aby uzyskać dostęp do danych, należy odblokować urządzenie. Jeśli przyczyna zablokowania urządzenia nie zostanie usunięta po odblokowaniu urządzenia, urządzenie zostanie zablokowane ponownie po określonym czasie.
- **Wyczyść dane firmowe**. Usuwane są dane w kontenerze, firmowe konto e-mail, ustawienia połączenia z firmową siecią Wi-Fi i VPN, nazwa punktu dostępu (APN), profil roboczy Android, kontener KNOX oraz klucz KNOX License Manager.
- **Pełny reset**. Wszystkie dane zostają usunięte z urządzenia mobilnego i zostają przywrócone ustawienia fabryczne. Po zakończeniu tego działania, urządzenie nie będzie już zarządzanym urządzeniem. Aby połączyć urządzenie z Kaspersky Security Center, należy ponownie zainstalować Kaspersky Endpoint Security for Android.

W celu utworzenia reguły skanowania do sprawdzania urządzeń pod kątem zgodności z zasadą grupy:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Kontrola zgodności**.
5. Aby otrzymywać powiadomienia o urządzeniach, które nie są zgodne z zasadą, w sekcji **Powiadomienia dotyczące niezgodności** zaznacz pole **Powiadom administratora**.

Jeśli urządzenie nie jest zgodne z zasadą, podczas synchronizacji urządzenia z Serwerem administracyjnym program Kaspersky Endpoint Security for Android zapisuje w dzienniku zdarzeń wpis dla **Wykryto naruszenie: <nazwa sprawdzonego kryterium>**. Dziennik zdarzeń można przejrzeć na zakładce **Zdarzenia**, we właściwościach Serwera administracyjnego lub w lokalnych właściwościach aplikacji.

6. Aby informować użytkownika urządzenia o braku zgodności jego urządzenia z zasadą, w sekcji **Powiadomienia dotyczące niezgodności** zaznacz pole **Powiadom użytkownika**.

   Jeśli urządzenie nie jest zgodne z zasadą, podczas synchronizacji urządzenia z Serwerem administracyjnym program Kaspersky Endpoint Security for Android powiadamia użytkownika o tym fakcie w sekcji **Stan**.

7. W sekcji **Reguły zgodności** utwórz listę reguł sprawdzania urządzenia pod kątem zgodności z zasadą. Postępuj zgodnie z poniższymi krokami:

   a. Kliknij **Dodaj**.

      Zostanie uruchomiony Kreator reguły zgodności.

   b. Postępuj zgodnie z instrukcjami Kreatora reguły zgodności.

      Po zakończeniu działania Kreatora, nowa reguła zostanie wyświetlona w sekcji **Reguły zgodności**, na liście reguł zgodności.

8. Aby tymczasowo wyłączyć utworzoną regułę zgodności, użyj przełącznika znajdującego się obok wybranej reguły.

9. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center. Jeśli urządzenie użytkownika nie odpowiada regułom, ograniczenia, które określiłeś na liście reguł zgodności, zostaną zastosowane na urządzeniu.

Kontrola uruchamiania aplikacji

Ta sekcja zawiera instrukcje dotyczące konfiguracji dostępu użytkownika do aplikacji na urządzeniu mobilnym.

Kontrola uruchamiania aplikacji na urządzeniach Android

Aby chronić urządzenie mobilne użytkownika, należy skonfigurować ustawienia uruchamiania aplikacji na urządzeniu.

Możesz nałożyć ograniczenia na aktywność użytkownika na urządzeniu, na którym są zainstalowane zablokowane aplikacje lub nie są zainstalowane wymagane aplikacje (na przykład, zablokować urządzenie). Ograniczenia można nałożyć przy użyciu komponentu Kontrola zgodności. W tym celu, w ustawieniach reguły skanowania należy wybrać kryterium **Zainstalowane są zabronione aplikacje**, **Aplikacje z zabronionych kategorii są zainstalowane** lub **Nie wszystkie wymagane aplikacje są zainstalowane**.

Kaspersky Endpoint Security for Android musi być ustawiony jako usługa Ułatwień dostępu w celu zapewnienia poprawnego działania Kontroli aplikacji. Kaspersky Endpoint Security for Android wyświetli pytanie o ustawienie aplikacji jako usługę funkcji Dostępności poprzez Kreator wstępnej konfiguracji. Użytkownik może pominąć ten krok lub wyłączyć tę usługę w ustawieniach urządzenia w późniejszym czasie. W takiej sytuacji Kontrola aplikacji nie będzie działać.

W celu skonfigurowania ustawień uruchamiania aplikacji na urządzeniu mobilnym:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Kontrola aplikacji**.
5. W sekcji **Tryb działania** wybierz tryb uruchamiania aplikacji na urządzeniu mobilnym użytkownika:
   - Aby zezwolić użytkownikowi na uruchamianie wszystkich aplikacji, za wyjątkiem tych określonych na liście kategorii oraz aplikacji wskazanych jako zablokowane aplikacje, wybierz tryb **Zablokowane aplikacje**.
   - Aby zezwolić użytkownikowi na uruchamianie tylko tych aplikacji określonych na liście kategorii oraz aplikacji wskazanych jako dozwolone, wybierz tryb **Dozwolone aplikacje**.
6. Jeśli chcesz, żeby Kaspersky Endpoint Security for Android wysyłał dane dotyczące zabronionych aplikacji do dziennika zdarzeń bez ich blokowania, zaznacz pole **Nie blokuj zabronionych aplikacji, tylko zapisuj w dzienniku zdarzeń**.

   Podczas kolejnej synchronizacji urządzenia mobilnego użytkownika z Serwerem administracyjnym, Kaspersky Endpoint Security for Android zapisze w dzienniku zdarzeń wpis dla **Zabroniona aplikacja została zainstalowana**. Dziennik zdarzeń można przejrzeć na zakładce **Zdarzenia**, we właściwościach Serwera administracyjnego lub w lokalnych właściwościach aplikacji.
7. Jeśli chcesz, żeby Kaspersky Endpoint Security for Android blokował uruchamianie aplikacji systemowych na urządzeniu mobilnym użytkownika (np. Kalendarz, Aparat i Ustawienia) w trybie **Dozwolone aplikacje**, zaznacz pole **Blokuj aplikacje systemowe**.

   Eksperci z Kaspersky zalecają włączenie blokowania uruchamiania aplikacji systemowych.
8. Aby skonfigurować uruchamianie aplikacji, utwórz listę kategorii i aplikacji.

   Więcej informacji na temat kategorii aplikacji można znaleźć w Dodatkach.

   Lista aplikacji należących do każdej kategorii znajduje się na stronie internetowej Kaspersky.
9. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie ograniczeń urządzenia EAS dla aplikacji

Aby zapewnić bezpieczeństwo urządzenia EAS, skonfiguruj ograniczenia aktywności aplikacji (przeglądarka, niepodpisane aplikacje).

Domyślnie, użytkownik może korzystać z aplikacji na urządzeniu EAS bez ograniczeń.

W celu skonfigurowania ograniczeń dotyczących aktywności aplikacji na urządzeniu EAS:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia EAS.
2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.

4. W oknie Właściwości zasady wybierz sekcję **Ograniczenia dla aplikacji**.

5. W sekcji **Ustawienia ograniczeń aplikacji** skonfiguruj ograniczenia aktywności aplikacji:

   - Aby zezwolić użytkownikowi na korzystanie z przeglądarki, zaznacz pole **Zezwól na użycie przeglądarki**.
   - Aby zezwolić użytkownikowi na utworzenie prywatnych kont pocztowych (POP3 lub IMAP4), zaznacz pole **Zezwól na pocztę prywatną**.
   - Aby zezwolić użytkownikowi na uruchamianie aplikacji, które nie są podpisane przy użyciu certyfikatu uwierzytelniania, zaznacz pole **Zezwól na niepodpisane aplikacje**.
   - Aby zezwolić użytkownikowi na instalowanie aplikacji, które nie są podpisane przy użyciu certyfikatu uwierzytelniania, zaznacz pole **Zezwól na niepodpisane pakiety instalacyjne**.

6. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Inwentaryzacja oprogramowania na urządzeniach Android

Możesz przeprowadzić inwentaryzację aplikacji na urządzeniach Android podłączonych do Kaspersky Security Center. Kaspersky Endpoint Security for Android pobiera informacje o wszystkich aplikacjach zainstalowanych na urządzeniach mobilnych. Informacje uzyskane podczas inwentaryzacji są wyświetlane we właściwościach urządzenia, w sekcji **Zdarzenia**. Możesz sprawdzić szczegółowe informacje o każdej zainstalowanej aplikacji, w tym jej wersję oraz producenta.

W celu włączenia inwentaryzacji oprogramowania:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.

4. W oknie **Właściwości** wybierz sekcję **Kontrola aplikacji**.

5. W sekcji **Inwentaryzacja oprogramowania** zaznacz pole **Wyślij dane dotyczące zainstalowanych aplikacji**.

6. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center. Kaspersky Endpoint Security for Android wysyła dane do dziennika zdarzeń za każdym razem, gdy aplikacja zostaje zainstalowana lub usunięta z urządzenia.

Konfigurowanie wyświetlania urządzeń Android w Kaspersky Security Center

W celu zapewnienia wygodnej pracy z listą urządzeń mobilnych, należy skonfigurować ustawienia wyświetlania urządzeń w Kaspersky Security Center. Domyślnie lista urządzeń mobilnych jest wyświetlana w drzewie konsoli **Dodatkowe → Zarządzenie urządzeniami mobilnymi → Urządzenia mobilne**. Informacje o urządzeniu są aktualizowane automatycznie. Listę urządzeń mobilnych możesz zaktualizować ręcznie, klikając przycisk **Aktualizuj** w prawym górnym rogu.

Po podłączeniu urządzenia do Kaspersky Security Center, urządzenia są automatycznie dodawane do listy urządzeń mobilnych. Lista urządzeń mobilnych może zawierać szczegółowe informacje o tym urządzeniu: model, system operacyjny, adres IP i inne.

Możesz skonfigurować format nazwy urządzenia i wybrać stan urządzenia. Stan urządzenia informuje o sposobie działania komponentów Kaspersky Endpoint Security for Android na urządzeniu mobilnym użytkownika.

Komponenty Kaspersky Endpoint Security for Android mogą nie działać z następujących powodów:

- Użytkownik wyłączył komponent w ustawieniach urządzenia.
- Użytkownik nie udzielił aplikacji niezbędnych uprawnień do działania komponentu (na przykład brak uprawnień do określania lokalizacji urządzenia dla odpowiedniego polecenia Anti-Theft).

Aby wyświetlić stan urządzenia, we właściwościach grupy administracyjnej należy włączyć warunek **Określone przez aplikację** (**Właściwości → Stan urządzenia → Ustaw stan urządzenia na Krytyczny, jeśli** i **Ustaw stan urządzenia na Ostrzeżenie, jeśli**). We właściwościach grupy administracyjnej możesz wybrać inne kryteria tworzenia stanu urządzenia mobilnego.

W celu skonfigurowania wyświetlania urządzeń Android w Kaspersky Security Center:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Informacje o urządzeniu**.
5. W sekcji **Nazwa urządzenia w Kaspersky Security Center** wybierz format dla nazwy urządzenia w Konsoli administracyjnej:
   - Model urządzenia [e-mail, ID urządzenia].
   - Model urządzenia [e-mail (jeśli jest) lub ID urządzenia].

   ID urządzenia to unikatowy numer ID, który jest generowany przez Kaspersky Endpoint Security for Android z danych otrzymanych z urządzenia. W przypadku urządzeń mobilnych działających pod kontrolą systemu Android 10 lub nowszego, Kaspersky Endpoint Security for Android używa SSAID (Android ID) lub sumy kontrolnej innych danych otrzymanych z urządzenia. Dla wcześniejszych wersji systemu Android aplikacja używa IMEI.
6. Ustaw atrybut Blokada na zablokowaną pozycję ( ).
7. W sekcji **Stan urządzenia w Kaspersky Security Center** ustaw odpowiedni stan urządzenia, jeśli komponent Kaspersky Endpoint Security for Android nie działa: (**Krytyczne**), (**Ostrzeżenie**) lub (**OK**).

   Na liście urządzeń mobilnych stan urządzenia będzie się zmieniał zgodnie z wybranym stanem.
8. Ustaw atrybut Blokada na zablokowaną pozycję.

9. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Zarządzanie

Ta sekcja zawiera informacje dotyczące zdalnego zarządzania ustawieniami urządzeń mobilnych w Konsoli administracyjnej Kaspersky Security Center.

Konfigurowanie połączenia z siecią Wi-Fi

Ta sekcja zawiera instrukcje dotyczące konfiguracji automatycznego połączenia z firmową siecią Wi-Fi na urządzeniach Android i iOS MDM.

Łączenie urządzeń Android z siecią Wi-Fi

W celu połączenia urządzenia mobilnego z siecią Wi-Fi:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Wi-Fi**.
5. W sekcji **Sieci Wi-Fi** kliknij **Dodaj**.

   Zostanie otwarte okno **Sieć Wi-Fi**.
6. W polu **Identyfikator zestawu usług (SSID)** wpisz nazwę sieci Wi-Fi, która zawiera punkt dostępu (SSID).
7. W sekcji **Ochrona sieci** wybierz typ zabezpieczenia sieci Wi-Fi (otwarta lub bezpieczna sieć, chroniona przy pomocy protokołu WEP lub WPA/WPA2 PSK).
8. Jeśli w poprzednim kroku wybrałeś bezpieczną sieć, w polu **Hasło** ustaw hasło dostępu do sieci.
9. W polu **Adres serwera proxy i port** wprowadź adres IP lub nazwę DNS serwera proxy oraz numer portu (jeśli to konieczne).

   Na urządzeniach działających pod kontrolą systemu Android w wersji 8.0 lub nowszego, nie można ponownie zdefiniować ustawień serwera proxy dla Wi-Fi przy użyciu zasady. Jednakże możesz ręcznie skonfigurować ustawienia serwera proxy dla sieci Wi-Fi na urządzeniu mobilnym.

Jeśli do łączenia się z siecią Wi-Fi używasz serwera proxy, możesz użyć zasady do skonfigurowania ustawień łączenia z siecią. Na urządzeniach działających pod kontrolą systemu Android 8.0 lub nowszego należy ręcznie skonfigurować ustawienia serwera proxy. Na urządzeniach działających pod kontrolą systemu Android 8.0 lub nowszego nie możesz korzystać z zasady do zmiany ustawień połączenia z siecią Wi-Fi, za wyjątkiem hasła dostępu do sieci.

Jeśli nie korzystasz z serwera proxy do łączenia się z siecią Wi-Fi, nie ma ograniczeń korzystania z zasad do zarządzania połączeniem z siecią Wi-Fi.

10. W polu **Nie używaj serwera proxy dla adresów** wygeneruj listę adresów internetowych, do których dostęp można uzyskać bez użycia serwera proxy.

    Na przykład, możesz wprowadzić adres `example.com`. W tym przypadku serwer proxy nie będzie użyty w przypadku adresów `pictures.example.com`, `example.com/movies` itp. Protokół (na przykład `http://`) można pominąć.

    Na urządzeniach działających pod kontrolą systemu Android 8.0 lub nowszego, wykluczenie serwera proxy dla adresów internetowych nie działa.

11. Kliknij **OK**.

    Dodana sieć Wi-Fi będzie wyświetlana na liście **Sieci Wi-Fi**.

    Na liście sieci można modyfikować lub usuwać sieci Wi-Fi, korzystając z przycisków **Edytuj** i **Usuń**, znajdujących się w górnej części listy.

12. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center. Po zastosowaniu zasady na urządzeniu mobilnym, użytkownik może nawiązać połączenie z dodaną siecią Wi-Fi, bez określania ustawień sieci.

Na urządzeniach z systemem Android w wersji 10.0 lub nowszej, jeśli użytkownik odmówi połączenia z proponowaną siecią Wi-Fi, uprawnienia aplikacji do zmiany stanu Wi-Fi zostaną cofnięte. Użytkownik musi nadać to uprawnienie ręcznie.

Łączenie urządzeń iOS MDM z siecią Wi-Fi

Aby urządzenie iOS MDM automatycznie łączyło się z dostępną siecią Wi-Fi i aby chronić dane podczas tego połączenia, należy skonfigurować ustawienia połączenia.

W celu skonfigurowania ustawień połączenia urządzenia iOS MDM z siecią Wi-Fi:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie **Właściwości** wybierz sekcję **Wi-Fi**.

5. W sekcji **Sieci Wi-Fi** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Sieć Wi-Fi**.

6. W polu **Identyfikator zestawu usług (SSID)** wpisz nazwę sieci Wi-Fi, która zawiera punkt dostępu (SSID).

7. Jeśli chcesz, żeby urządzenie iOS MDM automatycznie łączyło się z siecią Wi-Fi, zaznacz pole **Automatyczne połączenie**.

8. Aby uniemożliwić połączenie urządzeń iOS MDM z siecią Wi-Fi wymagającą wstępnego uwierzytelniania, zaznacz pole **Wyłącz wykrywanie sieci wymagających uwierzytelniania**.

   Aby używać sieci wymagającej uwierzytelniania, musisz subskrybować sieć, zaakceptować umowę lub uiścić opłatę. Sieci wymagające uwierzytelnienia mogą znajdować się, na przykład, w hotelach i kawiarniach.

9. Jeśli chcesz, żeby sieć Wi-Fi była ukrywana na liście dostępnych sieci na urządzeniu iOS MDM, zaznacz pole **Sieć ukryta**.

   W tej sytuacji, aby połączyć się z siecią, użytkownik musi ręcznie wpisać Identyfikator zestawu usług (SSID), określony w ustawieniach routera Wi-Fi na urządzeniu mobilnym.

10. Z listy rozwijalnej **Ochrona sieci** wybierz typ ochrony połączenia z siecią Wi-Fi:

    - **Wyłączono**. Autoryzacja użytkownika nie jest wymagana.
    - **WEP**. Sieć jest zabezpieczona przy pomocy protokołu Wireless Encryption Protocol (WEP).
    - **WPA/WPA2 (Personal)**. Sieć jest zabezpieczona przy pomocy protokołu WPA / WPA2 (Wi-Fi Protected Access).
    - **WPA2 (Personal)**. Sieć jest zabezpieczona przy pomocy protokołu WPA2 (Wi-Fi Protected Access 2.0). Ochrona WPA2 jest dostępna tylko na urządzeniach działających pod kontrolą systemu iOS w wersji 8 lub nowszej. WPA2 nie jest dostępne na urządzeniach Apple TV.
    - **Dowolne (Personal)**. Sieć jest zabezpieczona przy pomocy protokołu szyfrowania WEP, WPA lub WPA2 w zależności od typu routera Wi-Fi. Do autoryzacji używany jest klucz szyfrowania unikatowy dla każdego użytkownika.
    - **WEP (Dynamic)**. Sieć jest zabezpieczona przy pomocy protokołu WEP z użyciem klucza dynamicznego.
    - **WPA/WPA2 (Enterprise)**. Sieć jest zabezpieczona przy pomocy protokołu szyfrowania WPA/WPA2 z użyciem protokołu 802.1X.
    - **WPA2 (Enterprise)**. Sieć jest zabezpieczona przy pomocy protokołu szyfrowania WPA2 z użyciem jednego klucza współdzielonego przez wszystkich użytkowników (802.1X). Ochrona WPA2 jest dostępna tylko na urządzeniach działających pod kontrolą systemu iOS w wersji 8 lub nowszej. WPA2 nie jest dostępne na urządzeniach Apple TV.
    - **Dowolne (Enterprise)**. Sieć jest zabezpieczona przy pomocy protokołu WEP lub WPA / WPA2 w zależności od typu routera Wi-Fi. Do autoryzacji używany jest jeden klucz szyfrowania dostępny dla wszystkich użytkowników.

    Jeśli wybrałeś **WEP (Dynamic)**, **WPA/WPA2 (Enterprise)**, **WPA2 (Enterprise)** lub **Dowolne (Enterprise)** na liście **Ochrona sieci**, w sekcji **Protokoły** możesz wybrać typy protokołów EAP (Extensible Authentication Protocol) do identyfikacji użytkownika w sieci Wi-Fi.

    W sekcji **Certyfikaty zaufane** możesz także utworzyć listę zaufanych certyfikatów do uwierzytelniania użytkownika urządzenia iOS MDM na zaufanych serwerach.

11. Skonfiguruj ustawienia konta do autoryzacji użytkownika po połączeniu urządzenia iOS MDM z siecią Wi-Fi:

a. W sekcji **Uwierzytelnienie** kliknij przycisk **Konfiguruj**.

Zostanie otwarte okno **Uwierzytelnianie**.

b. W polu **Nazwa użytkownika** wprowadź nazwę konta do autoryzacji użytkownika po połączeniu z siecią Wi-Fi.

c. Aby użytkownik musiał ręcznie wpisywać hasło po każdym nawiązaniu połączenia z siecią Wi-Fi, zaznacz pole **Pytaj o hasło przy każdym połączeniu**.

d. W polu **Hasło** wpisz hasło do konta do autoryzacji w sieci Wi-Fi.

e. Z listy rozwijalnej **Certyfikat uwierzytelniania** wybierz certyfikat do autoryzacji użytkownika w sieci Wi-Fi. Jeśli na liście nie ma żadnego certyfikatu, **możesz go dodać w sekcji** Certyfikaty.

f. W polu **ID użytkownika** wprowadź ID użytkownika, wyświetlany podczas transmisji danych po autoryzacji zamiast nazwy użytkownika.

Identyfikator użytkownika został stworzony w celu zapewnienia większego bezpieczeństwa procesu autoryzacji - nazwa użytkownika nie jest wyświetlana otwarcie, ale przesyłana poprzez zaszyfrowany tunel TLS.

g. Kliknij **OK**.

Ustawienia konta do autoryzacji użytkownika po nawiązaniu połączenia z siecią Wi-Fi zostaną skonfigurowane na urządzeniu iOS MDM.

12. Jeśli to konieczne, skonfiguruj ustawienia połączenia z siecią Wi-Fi poprzez serwer proxy:

a. W sekcji **Serwer proxy** kliknij przycisk **Konfiguruj**.

b. W otwartym oknie **Serwer proxy** wybierz tryb konfiguracji serwera proxy i określ ustawienia połączenia.

c. Kliknij **OK**.

Ustawienia połączenia urządzenia z siecią Wi-Fi poprzez serwer proxy zostaną skonfigurowane na urządzeniu iOS MDM.

13. Kliknij **OK**.

Nowa sieć Wi-Fi będzie wyświetlana na liście.

14. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia połączenia z siecią Wi-Fi zostaną skonfigurowane na urządzeniu iOS MDM użytkownika po zastosowaniu zasady. Urządzenie mobilne użytkownika zostanie automatycznie połączone z dostępnymi sieciami Wi-Fi. Bezpieczeństwo danych podczas połączenia z siecią Wi-Fi jest zapewniane przez technologię uwierzytelniania.

Konfigurowanie poczty

Ta sekcja zawiera informacje dotyczące konfiguracji skrzynek pocztowych na urządzeniach mobilnych.

Konfigurowanie skrzynki pocztowej na urządzeniach iOS MDM

Aby umożliwić użytkownikowi urządzenia iOS MDM pracę z wiadomościami e-mail, dodaj konto pocztowe użytkownika do listy kont na urządzeniu iOS MDM.

Domyślnie, konto pocztowe jest dodawane z następującymi ustawieniami:

- Protokół pocztowy – IMAP.
- Użytkownik może przenosić wiadomości e-mail między kontami użytkownika oraz synchronizować adresy kont.
- Użytkownik może używać dowolnego klienta poczty e-mail (inny niż Mail) do korzystania z poczty.
- Połączenie SSL nie jest używane podczas przesyłania wiadomości.

Możesz zmodyfikować określone ustawienia podczas dodawania konta.

W celu dodania konta e-mail użytkownika urządzenia iOS MDM:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie **Właściwości** wybierz **E-mail**.
5. W sekcji **Konto e-mail** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Konto e-mail**.
6. W polu **Opis** wpisz opis konta e-mail użytkownika.
7. Wybierz protokół pocztowy:
   - **POP**
   - **IMAP**
8. Jeśli to konieczne, w polu **Przedrostek ścieżki IMAP** określ przedrostek ścieżki IMAP.

   Przedrostek ścieżki IMAP musi zostać wprowadzony z użyciem wielkich liter (na przykład: GMAIL dla Google Mail). To pole jest dostępne, jeśli wybrano protokół konta IMAP.
9. W polu **Nazwa użytkownika wyświetlana w wiadomościach** wprowadź nazwę użytkownika, jaka ma być wyświetlana w polu **Od:** dla wszystkich wiadomości wychodzących.
10. W polu **Adres e-mail** określ adres e-mail użytkownika urządzenia iOS MDM.
11. Skonfiguruj ustawienia dodatkowe konta e-mail:
    - Aby umożliwić użytkownikowi przenoszenie wiadomości e-mail pomiędzy kontami użytkownika, zaznacz pole **Zezwól na przenoszenie wiadomości pomiędzy kontami**.
    - Aby zezwolić na synchronizację używanych adresów e-mail pomiędzy kontami użytkowników, zaznacz pole **Zezwól na synchronizację ostatnich adresów**.
    - Aby zezwolić użytkownikowi na użycie usługi Mail Drop do wysyłania załączników o dużych rozmiarach, zaznacz pole **Zezwól na Mail Drop**.

- Aby zezwolić użytkownikowi na używanie tylko standardowego klienta poczty elektronicznej iOS, zaznacz pole **Zezwól wyłącznie na korzystanie z aplikacji Mail**.

12. Skonfiguruj ustawienia korzystania z protokołu S/MIME w aplikacji Mail. *S/MIME* to protokół przesyłania zaszyfrowanych wiadomości posiadających podpis cyfrowy.

    - Aby używać protokołu S/MIME do podpisywania poczty wychodzącej, zaznacz pole **Podpisuj wiadomości** i wybierz certyfikat dla podpisu. Podpis cyfrowy potwierdza autentyczność nadawcy i wskazuje, że zawartość wiadomości nie została zmodyfikowana podczas przesyłania do odbiorcy. Podpis wiadomości jest dostępny na urządzeniach działających pod kontrolą systemu iOS w wersji 10.3 lub nowszej.

    - Aby używać protokołu S/MIME do szyfrowania poczty wychodzącej, zaznacz pole **Domyślnie szyfruj wiadomości** i wybierz certyfikat dla szyfrowania (klucz publiczny). Szyfrowanie wiadomości jest dostępne tylko na urządzeniach działających pod kontrolą systemu iOS w wersji 10.3 lub nowszej.

    - Aby umożliwić użytkownikowi szyfrowanie pojedynczych wiadomości, zaznacz pole **Pokaż przycisk przełącznika do szyfrowania wiadomości**. Aby wysłać szyfrowane wiadomości, użytkownik musi kliknąć ikonę w aplikacji Mail, w polu **Do**.

13. W sekcjach **Serwer poczty przychodzącej** i **Serwer poczty wychodzącej** kliknij przycisk **Ustawienia** w celu skonfigurowania ustawień połączenia z serwerem:

    - **Adres serwera i port**: Nazwy hostów lub adresy IP serwerów poczty przychodzącej i serwerów poczty wychodzącej oraz numery portów.

    - **Nazwa konta**: Nazwa konta użytkownika do autoryzacji serwera poczty wychodzącej i przychodzącej.

    - **Typ uwierzytelniania**: Typ uwierzytelniania konta e-mail użytkownika na serwerach poczty wychodzącej i przychodzącej.

    - **Hasło**: Hasło do konta do przeprowadzenia autoryzacji na serwerze poczty wychodzącej i przychodzącej, chronionym przy pomocy wybranej metody uwierzytelniania.

    - **Używaj jednego hasła do serwerów poczty przychodzącej i wychodzącej**: Użycie jednego hasła do autoryzacji użytkownika na serwerach poczty przychodzącej i wychodzącej.

    - **Użyj połączenia SSL**: Użycie protokołu przesyłania danych SSL (Secure Sockets Layer), który wykorzystuje szyfrowanie i uwierzytelnianie w oparciu o certyfikat do zabezpieczenia transmisji danych.

14. Kliknij **OK**.

    Nowe konto e-mail pojawi się na liście.

15. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, konta e-mail z utworzonej listy zostaną dodane na urządzeniu mobilnym użytkownika.

Konfigurowanie skrzynki pocztowej Exchange na urządzeniach iOS MDM

Aby umożliwić użytkownikowi urządzenia iOS MDM korzystanie z poczty firmowej, kalendarza, kontaktów, notatek i zadań, dodaj konto Exchange ActiveSync użytkownika na serwerze Microsoft Exchange.

Domyślnie, na serwerze Microsoft Exchange zostanie dodane konto z następującymi ustawieniami:

- Poczta jest synchronizowana raz w tygodniu.

- Użytkownik może przenosić wiadomości między kontami użytkownika oraz synchronizować adresy kont.
- Użytkownik może używać dowolnego klienta poczty e-mail (inny niż Mail) do korzystania z poczty.
- Połączenie SSL nie jest używane podczas przesyłania wiadomości.

Możesz zmodyfikować określone ustawienia podczas dodawania konta Exchange ActiveSync.

W celu dodania konta Exchange ActiveSync użytkownika urządzenia iOS MDM:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie **Właściwości** wybierz sekcję **Exchange ActiveSync**.
5. W sekcji **Konta Exchange ActiveSync** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Konto Exchange ActiveSync** na zakładce **Ogólne**.
6. W polu **Nazwa konta** wprowadź nazwę konta dla autoryzacji na serwerze Microsoft Exchange. Możesz użyć makr dostępnych na liście **Dostępne makra**.
7. W polu **Adres serwera** wpisz nazwę sieci lub adres IP serwera Microsoft Exchange.
8. Aby używać protokołu przesyłania danych SSL (Secure Sockets Layer) do ochrony transmisji danych, zaznacz pole **Użyj połączenia SSL**.
9. W polu **Domena** wprowadź nazwę domeny użytkownika urządzenia iOS MDM. Możesz użyć makr dostępnych na liście **Dostępne makra**.
10. W polu **Nazwa konta użytkownika** wprowadź nazwę użytkownika urządzenia iOS MDM.

    Jeśli pozostawisz to pole puste, Kaspersky Device Management for iOS zapyta użytkownika o wprowadzenie nazwy użytkownika podczas stosowania zasady na urządzeniu iOS MDM. Możesz użyć makr dostępnych na liście **Dostępne makra**.
11. W polu **Adres e-mail** określ adres e-mail użytkownika urządzenia iOS MDM. Możesz użyć makr dostępnych na liście **Dostępne makra**.
12. W polu **Hasło** wpisz hasło do konta Exchange ActiveSync do autoryzacji na serwerze Microsoft Exchange.
13. Wybierz zakładkę **Dodatkowe** i skonfiguruj ustawienia dodatkowe konta Exchange ActiveSync:
    - **Liczba dni do synchronizacji poczty <czas>**.
    - **Typ uwierzytelniania**.
    - **Zezwól na przenoszenie wiadomości pomiędzy kontami**.
    - **Zezwól na synchronizację ostatnich adresów**.
    - **Zezwól wyłącznie na korzystanie z aplikacji Mail**.

14. Skonfiguruj ustawienia korzystania z protokołu S/MIME w aplikacji Mail. *S/MIME* to protokół przesyłania zaszyfrowanych wiadomości posiadających podpis cyfrowy.

    - Aby używać protokołu S/MIME do podpisywania poczty wychodzącej, zaznacz pole **Podpisuj wiadomości** i wybierz certyfikat dla podpisu. Podpis cyfrowy potwierdza autentyczność nadawcy i wskazuje, że zawartość wiadomości nie została zmodyfikowana podczas przesyłania do odbiorcy. Podpis wiadomości jest dostępny na urządzeniach działających pod kontrolą systemu iOS w wersji 10.3 lub nowszej.

    - Aby używać protokołu S/MIME do szyfrowania poczty wychodzącej, zaznacz pole **Domyślnie szyfruj wiadomości** i wybierz certyfikat dla szyfrowania (klucz publiczny). Szyfrowanie wiadomości jest dostępne tylko na urządzeniach działających pod kontrolą systemu iOS w wersji 10.3 lub nowszej.

    - Aby umożliwić użytkownikowi szyfrowanie pojedynczych wiadomości, zaznacz pole **Pokaż przycisk przełącznika do szyfrowania wiadomości**. Aby wysłać szyfrowane wiadomości, użytkownik musi kliknąć ikonę w aplikacji Mail, w polu **Do**.

15. Kliknij **OK**.

    Nowe konto Exchange ActiveSync pojawi się na liście.

16. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, konta Exchange ActiveSync z utworzonej listy zostaną dodane na urządzeniu mobilnym użytkownika.

Konfigurowanie skrzynki pocztowej Exchange na urządzeniach Android (tylko Samsung)

Aby pracować z firmowymi e-mailami, kontaktami i kalendarzem na urządzeniu mobilnym, powinieneś skonfigurować ustawienia skrzynki pocztowej Exchange.

Konfiguracja skrzynki Exchange jest możliwa tylko dla urządzeń Samsung.

W celu skonfigurowania skrzynki pocztowej Exchange na urządzeniu mobilnym:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.

4. W oknie **Właściwości** wybierz sekcję **Zarządzaj Samsung KNOX → Zarządzaj urządzeniami Samsung**.

5. W oknie **Exchange ActiveSync** kliknij przycisk **Konfiguruj**.

   Zostanie otwarte okno **Ustawienia serwera pocztowego Exchange**.

6. W polu **Adres serwera** wprowadź adres IP lub nazwę DNS serwera, na którym znajduje się serwer pocztowy.

7. W polu **Domena** wprowadź nazwę domeny użytkownika mobilnego w sieci firmowej.

8. Na liście rozwijalnej **Okres synchronizacji** wybierz żądany przedział synchronizacji dla urządzenia mobilnego z serwerem Microsoft Exchange.

9. Aby korzystać z protokołu przesyłania danych SSL (Secure Sockets Layer), zaznacz pole **Użyj połączenia SSL**.

10. Aby korzystać z cyfrowych certyfikatów w celu ochrony transferu danych pomiędzy urządzeniem mobilnym i serwerem Microsft Exchange, zaznacz pole **Weryfikuj certyfikat serwera**.

11. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

    Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Zarządzanie aplikacjami mobilnymi firm trzecich

Kontenery mogą zostać użyte do monitorowania aktywności aplikacji mobilnych uruchamianych na urządzeniu użytkownika. *Kontener* to specjalna powłoka dla aplikacji mobilnych, która umożliwia kontrolowanie aktywności aplikacji w kontenerze, chroniąc w ten sposób dane osobiste i firmowe użytkownika, znajdujące się na urządzeniu.

W Kaspersky Security for Mobile Service Pack 3 Maintenance Release 2 nie ma już obsługi tworzenia kontenerów dla aplikacji mobilnych. Jednakże kontenery, które zostały utworzone we wcześniejszych wersjach aplikacji, mogą zostać dodane na urządzeniach Android.

Możesz zainstalować aplikację w kontenerze na urządzeniu użytkownika w jeden z następujących sposobów:

- Wysyłając do użytkownika wiadomość e-mail z odnośnikiem do pakietu instalacyjnego aplikacji w kontenerze.
- Określając w sekcji **Kontrola aplikacji** okna właściwości zasady aplikację w kontenerze jako wymaganą lub dozwoloną aplikację. Po zsynchronizowaniu urządzenia mobilnego z Kaspersky Security Center, pakiet dystrybucyjny aplikacji w kontenerze jest automatycznie kopiowany na urządzenie użytkownika.

Aby zainstalować aplikacje z kontenera, na urządzeniu mobilnym użytkownika należy zezwolić na instalację aplikacji z nieznanych źródeł. Aby chronić urządzenie i dane po zainstalowaniu aplikacji z kontenera, zalecane jest zablokowanie instalacji aplikacji z nieznanych źródeł. Szczegóły dotyczące instalowania aplikacji bez Google Play można znaleźć w *pomocy Android*.

Konfigurowanie powiadomień dla Kaspersky Endpoint Security for Android

Jeśli nie chcesz, aby powiadomienia Kaspersky Endpoint Security for Android rozpraszały użytkownika urządzenia mobilnego, możesz wyłączyć pewne powiadomienia.

Kaspersky Endpoint Security używa następujących narzędzi do wyświetlania stanu ochrony urządzenia:

- **Powiadomienie o stanie ochrony**. To powiadomienie jest przypięte do paska powiadomień. Powiadomienie o stanie ochrony nie może zostać usunięte. Powiadomienie wyświetla stan ochrony urządzenia (na przykład:) oraz liczbę problemów (jeśli jakiekolwiek występują). Możesz dotknąć stan ochrony urządzenia i wyświetlić listę problemów w aplikacji.
- **Powiadomienia aplikacji**. Te powiadomienia informują użytkownika urządzenia o aplikacji (na przykład: wykryciu zagrożenia).
- **Komunikaty wyskakujące**. Wiadomości wyskakujące wymagają działania ze strony użytkownika urządzenia (na przykład, działanie, jakie należy wykonać po wykryciu zagrożenia).

Domyślnie włączone są wszystkie powiadomienia Kaspersky Endpoint Security for Android.

Użytkownik urządzenia z systemem Android może wyłączyć wszystkie powiadomienia z Kaspersky Endpoint Security for Android w ustawieniach na pasku powiadomień. Jeśli powiadomienia są wyłączone, użytkownik nie monitoruje działania aplikacji i może zignorować ważne informacje (na przykład informacje o błędach podczas synchronizacji urządzenia z Kaspersky Security Center). W takim przypadku, aby sprawdzić stan działania aplikacji, użytkownik musi otworzyć Kaspersky Endpoint Security for Android.

W celu skonfigurowania wyświetlania powiadomień dotyczących działania Kaspersky Endpoint Security for Android:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Dodatkowe**.
5. W sekcji **Powiadomienia aplikacji** kliknij przycisk **Konfiguruj**.

   Zostanie otwarte okno **Ustawienia powiadomień urządzenia**.
6. Zaznacz problemy Kaspersky Endpoint Security for Android, które mają zostać ukryte na urządzeniu mobilnym użytkownika, i kliknij przycisk **OK**.

   Program Kaspersky Endpoint Security for Android nie będzie wyświetlał problemów w powiadomieniu o stanie ochrony oraz w sekcji **Stan** w aplikacji. Program Kaspersky Endpoint Security for Android będzie dalej wyświetlał powiadomienie o stanie ochrony i powiadomienia aplikacji.

   Niektóre problemy z Kaspersky Endpoint Security for Android są obowiązkowe i nie można ich wyłączyć (na przykład problemy związane z wygaśnięciem licencji).
7. Aby ukryć wszystkie powiadomienia i komunikaty wyskakujące, wybierz **Wyłącz powiadomienia i wyskakujące okienka, gdy aplikacja działa w tle**.

   Program Kaspersky Endpoint Security for Android będzie wyświetlał tylko powiadomienia dotyczące stanu ochrony. Powiadomienie wyświetla stan ochrony urządzenia (na przykład:) oraz liczbę problemów. Aplikacja wyświetla powiadomienia także wtedy, gdy użytkownik pracuje z aplikacją (na przykład, gdy użytkownik ręcznie aktualizuje antywirusowe bazy danych).

   Eksperci z Kaspersky zalecają włączenie powiadomień i powiadomień wyskakujących. Jeśli wyłączysz powiadomienia i wiadomości wyskakujące, gdy aplikacja działa w tle, aplikacja nie ostrzeże użytkowników o zagrożeniach w czasie rzeczywistym. Użytkownicy urządzeń mobilnych mogą poznać stan ochrony urządzenia tylko wtedy, gdy otworzą aplikację.
8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center. Powiadomienia Kaspersky Endpoint Security for Android, które wyłączysz, nie będą wyświetlane na urządzeniu mobilnym użytkownika.

Łączenie urządzeń iOS MDM z AirPlay

Skonfiguruj połączenie z urządzeniami AirPlay, aby włączyć strumieniowanie muzyki, zdjęć i filmów z urządzenia iOS MDM na urządzenia AirPlay. Aby możliwe było korzystanie z technologii AirPlay, urządzenie mobilne i urządzenia AirPlay muszą być połączone z tą samą siecią bezprzewodową. Urządzenia AirPlay obejmują urządzenia Apple TV (drugiej i trzeciej generacji), urządzenia AirPort Express, głośniki lub zestaw radiowy z obsługą AirPlay.

Automatyczne połączenie z urządzeniami AirPlay jest dostępne tylko dla kontrolowanych urządzeń.

W celu skonfigurowania ustawień połączenia urządzenia iOS MDM z urządzeniami AirPlay:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie **Właściwości** wybierz sekcję **AirPlay**.
5. W sekcji **Urządzenia AirPlay** zaznacz pole **Zastosuj ustawienia na urządzeniu**.
6. W sekcji **Hasła** kliknij przycisk **Dodaj**.

   W tabeli haseł zostanie dodany pusty rząd.
7. W kolumnie **Nazwa urządzenia** wprowadź nazwę urządzenia AirPlay w sieci bezprzewodowej.
8. W kolumnie **Hasło** wprowadź hasło do urządzenia AirPlay.
9. Aby ograniczyć dostęp urządzeń iOS MDM do urządzeń AirPlay, w sekcji **Dozwolone urządzenia** utwórz listę dozwolonych urządzeń. W tym celu dodaj adresy MAC urządzeń AirPlay do listy dozwolonych urządzeń.

   Dostęp do urządzeń AirPlay, które nie znajdują się na liście dozwolonych urządzeń, jest zablokowany. Jeśli lista dozwolonych urządzeń pozostanie pusta, Kaspersky Device Management for iOS zezwoli na dostęp do wszystkich urządzeń AirPlay.
10. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, urządzenie mobilne użytkownika automatycznie nawiąże połączenie z urządzeniami AirPlay w celu strumieniowania treści multimedialnych.

Łączenie urządzeń iOS MDM z AirPrint

Aby umożliwić drukowanie dokumentów z urządzenia iOS MDM bezprzewodowo przy użyciu technologii AirPrint, skonfiguruj automatyczne łączenie z drukarkami AirPrint. Urządzenie mobilne i drukarka muszą być połączone z tą samą siecią bezprzewodową. Dostęp współdzielony dla wszystkich użytkowników należy skonfigurować na drukarce AirPrint.

W celu skonfigurowania ustawień połączenia urządzenia iOS MDM z drukarką AirPrint:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.

4. W oknie **Właściwości** wybierz sekcję **AirPrint**.

5. W sekcji **Drukarki AirPrint** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Drukarka**.

6. W polu **Adres IP** wprowadź adres IP drukarki AirPrint.

7. W polu **Ścieżka zasobu** wprowadź ścieżkę do drukarki AirPrint.

   Ścieżka do drukarki odpowiada kluczowi rp (ścieżka zasobu) protokołu Bonjour. Na przykład:

   - printers/Canon_MG5300_series
   - ipp/print
   - Epson_IPP_Printer

8. Kliknij **OK**.

   Nowo dodana drukarka AirPrint pojawi się na liście.

9. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, użytkownik urządzenia mobilnego będzie mógł bezprzewodowo drukować dokumenty na drukarce AirPrint.

Konfigurowanie Nazwy punktu dostępu (APN)

Aby połączyć urządzenie mobilne z usługami przesyłania danych w sieci mobilnej, należy skonfigurować ustawienia APN (Nazwa punktu dostępu).

Konfigurowanie APN na urządzeniach Android (tylko Samsung)

Konfiguracja APN jest możliwa tylko dla urządzeń Samsung.

Karta SIM musi być umieszczona w urządzeniu, aby możliwe było użycie punktu dostępu na urządzeniu mobilnym użytkownika. Ustawienia punktu dostępu są dostarczane przez operatora sieci telefonii mobilnej. Niepoprawne ustawienia punktu dostępu mogą spowodować dodatkowe zmiany w telefonii mobilnej.

W celu skonfigurowania ustawień Nazwy punktu dostępu (APN):

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.

4. W oknie **Właściwości** wybierz sekcję **Zarządzaj Samsung KNOX → APN**.

5. W sekcji **APN** kliknij przycisk **Konfiguruj**.

   Zostanie otwarte okno **Ustawienia APN**.

6. Na zakładce **Ogólne** określ następujące ustawienia punktu dostępu:

   a. Z listy rozwijalnej **Typ APN** wybierz typ punktu dostępu.

   b. W polu **Nazwa APN** określ nazwę punktu dostępu.

   c. W polu **MCC** wybierz kod identyfikujący kraj (MCC).

   d. W polu **MNC** wprowadź kod identyfikujący sieć mobilną (MNC).

   e. Jeśli jako typ punktu dostępu wybrałeś **MMS** lub **Internet i MMS**, określ następujące dodatkowe ustawienia MMS:

      - W polu **Serwer MMS** określ pełną nazwę domeny serwera dostawcy mobilnego, używanego do wymiany MMS.
      - W polu **Serwer proxy MMS** określ nazwę sieci lub adres IP serwera proxy i numer portu serwera dostawcy mobilnego, używanego do wymiany MMS.

7. Na zakładce **Dodatkowe** skonfiguruj ustawienia dodatkowe Nazwy punktu dostępu (APN):

   a. Z listy rozwijalnej **Typ uwierzytelniania** wybierz typ autoryzacji użytkownika urządzenia mobilnego na serwerze dostawcy mobilnego.

   b. W polu **Adres serwera** określ nazwę sieci serwera dostawcy mobilnego, poprzez który uzyskiwany jest dostęp do usług transmisji danych.

   c. W polu **Adres serwera proxy** określ nazwę sieci lub adres IP i numer portu serwera proxy dostawcy mobilnego.

   d. W polu **Nazwa użytkownika** wprowadź nazwę użytkownika dla autoryzacji w sieci komórkowej.

   e. W polu **Hasło** wprowadź hasło do autoryzacji użytkownika w sieci komórkowej.

8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie APN na urządzeniach iOS MDM

Nazwa punktu dostępu (APN) musi zostać skonfigurowana w celu włączenia usługi przesyłania danych sieci mobilnej na urządzeniu iOS MDM użytkownika.

Sekcja **APN** jest przestarzała. Zalecane jest skonfigurowanie ustawień APN w sekcji **Komunikacja przez sieci komórkowe**. Przed skonfigurowaniem ustawień sieci komórkowej upewnij się, że ustawienia z sekcji **APN** nie zostały zastosowane na urządzeniu (pole **Zastosuj ustawienia na urządzeniu** jest odznaczone). Ustawienia z sekcji **APN** i **Komunikacja przez sieci komórkowe** nie mogą być używane jednocześnie.

W celu skonfigurowania punktu dostępowego na urządzeniu iOS MDM użytkownika:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie **Właściwości** wybierz sekcję **Komunikacja przez sieci komórkowe**.
5. W sekcji **Ustawienia sieci komórkowej** zaznacz pole **Zastosuj ustawienia na urządzeniu**.
6. Na liście **Typ APN** wybierz typ punktu dostępu do przesyłania danych w sieci komórkowej GPRS/3G/4G:
   - **Wbudowany APN** – konfiguracja ustawień komunikacji przez sieci komórkowe dla transmisji danych za pomocą operatora sieci komórkowej, który obsługuje operacje z wbudowaną kartą Apple SIM. Aby uzyskać więcej szczegółów dotyczących urządzeń z wbudowaną kartą Apple SIM należy odwiedzić stronę Pomocy technicznej Apple.
   - **APN** – konfiguracja ustawień sieci komórkowej do przesyłania danych za pośrednictwem operatora sieci komórkowej włożonej karty SIM.
   - **Wbudowany APN i APN** – konfiguracja ustawień komunikacji przez sieci komórkowe dla transmisji danych za pomocą operatorów sieci komórkowych włożonych kart sim i wbudowanych kart Apple SIM. Aby uzyskać więcej szczegółów dotyczących urządzeń z wbudowaną kartą Apple SIM i gniazdem karty SIM należy odwiedzić stronę Pomocy technicznej Apple.
7. W polu **Nazwa APN** określ nazwę punktu dostępu.
8. Z listy rozwijalnej **Typ uwierzytelniania** wybierz typ uwierzytelniania użytkownika urządzenia mobilnego na serwerze operatora sieci mobilnej w celu uzyskania dostępu (internet i MMS):
9. W polu **Nazwa użytkownika** wprowadź nazwę użytkownika dla autoryzacji w sieci komórkowej.
10. W polu **Hasło** wprowadź hasło do autoryzacji użytkownika w sieci komórkowej.
11. W polu **Adres serwera proxy i port** wprowadź nazwę hosta lub adres IP serwera proxy oraz numer portu serwera proxy.
12. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, na urządzeniu mobilnym użytkownika zostanie skonfigurowana nazwa punktu dostępu (APN).

Konfigurowanie profilu roboczego Android

Ta sekcja zawiera informacje odnośnie pracy z profilem roboczym Android.

Informacje o profilu roboczym Android

Android Enterprise to platforma do zarządzania firmową infrastrukturą mobilną, oferująca pracownikom firmy środowisko pracy, w którym mogą korzystać z urządzeń mobilnych. Więcej informacji na temat korzystania z Android Enterprise można znaleźć na stronie pomocy technicznej Google.

Profil roboczy Android (zwany dalej również "profil roboczy") można utworzyć na urządzeniu mobilnym użytkownika. *Profil roboczy Android* to bezpieczne środowisko na urządzeniu użytkownika, w którym administrator może zarządzać aplikacjami i kontami użytkownika bez ograniczania użytkownikowi możliwości korzystania ze swoich danych. Po utworzeniu profilu roboczego na urządzeniu mobilnym użytkownika, automatycznie instalowane są w nim następujące aplikacje: Sklep Google Play, Google Chrome, Pobrane, Kaspersky Endpoint Security for Android i inne. Aplikacje firmowe zainstalowane w profilu roboczym oraz powiadomienia tych aplikacji są oznaczone ikoną. Dla aplikacji Google Play należy utworzyć oddzielne konto firmowe Google. Aplikacje zainstalowane w profilu roboczym pojawią się na ogólnej liście aplikacji.

Konfigurowanie profilu roboczego

W celu skonfigurowania ustawień profilu roboczego Android:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz **Profil roboczy Android**.
5. W sekcji **Profil roboczy Android** zaznacz pole **Utwórz profil roboczy**.
6. Określ ustawienia profilu roboczego:

   - Aby włączyć Kontrolę aplikacji w profilu roboczym Android i wyłączyć ją w profilu osobistym, zaznacz pole **Włącz Kontrolę aplikacji tylko w profilu roboczym**.

     W sekcji **Użytkownicy** możesz wybrać Kontrola aplikacji i użyć obszaru roboczego do utworzenia list dozwolonych, blokowanych, zalecanych i wymaganych aplikacji, a także dozwolonych i blokowanych kategorii aplikacji.

   - Aby włączyć Ochronę WWW dla Google Chrome w profilu roboczym i wyłączyć w profilu osobistym, w obszarze roboczym sekcji **Profil roboczy Android** zaznacz pole **Włącz Ochronę WWW tylko w profilu roboczym**.

     Ochrona WWW dla Samsung Internet Browser blokuje strony w profilach: roboczym i osobistym. Nie możesz włączyć Ochrony WWW dla Samsung Internet Browser tylko w profilu roboczym. Aby użyć Ochrony WWW dla Samsung Internet Browser w profilu roboczym, wyłącz opcję **Włącz Ochronę WWW tylko w profilu roboczym**. Jeśli ta opcja jest włączona, Ochrona WWW dla Samsung Internet Browser nie zostaje uruchomiona. Ochrona WWW w profilu roboczym jest wyłączona domyślnie.

     > Ochrona WWW na urządzeniach z systemem Android działa tylko w przeglądarkach: Google Chrome i Samsung Internet Browser.

     Ustawienia dostępu do strony internetowej można określić (utworzyć listę blokowanych kategorii stron internetowych lub listę dozwolonych stron internetowych) w sekcji **Ochrona WWW**.

   - Aby zablokować użytkownikowi możliwość kopiowania danych przy użyciu Schowka z aplikacji profilu roboczego do aplikacji prywatnych, zaznacz pole **Zabroń przesyłania danych z profilu roboczego do profilu**

osobistego.

- Aby zablokować użytkownikowi możliwość korzystania z trybu debugowania USB na urządzeniu mobilnym w profilu roboczym, zaznacz pole **Zabroń aktywacji trybu debugowania USB**.

  W trybie debugowania USB użytkownik może, na przykład, pobrać aplikację za pośrednictwem stacji roboczej.

- Aby zabronić użytkownikowi instalowania aplikacji w profilu roboczym Android ze wszystkich źródeł za wyjątkiem Google Play, zaznacz pole **Zabroń instalacji w profilu roboczym aplikacji z nieznanych źródeł**.

- Aby zabronić użytkownikowi usuwania aplikacji z profilu roboczego Android, zaznacz pole **Zabroń usuwania aplikacji z profilu roboczego**.

7. Aby skonfigurować ustawienia profilu roboczego na urządzeniu mobilnym użytkownika, zablokuj możliwość wprowadzania zmian w ustawieniach.

8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center. Obszar urządzenia mobilnego użytkownika jest podzielony na profil roboczy i profil osobisty.

Dodawanie konta LDAP

Aby umożliwić użytkownikowi urządzenia iOS MDM uzyskanie dostępu do kontaktów firmowych na serwerze LDAP, dodaj konto LDAP.

W celu dodania konta LDAP użytkownika urządzenia iOS MDM:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.

4. W oknie **Właściwości** wybierz sekcję **LDAP**.

5. W sekcji **Konta LDAP** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Konto LDAP**.

6. W polu **Opis** wpisz opis konta LDAP użytkownika. Możesz użyć makr dostępnych na liście **Dostępne makra**.

7. W polu **Nazwa konta** wprowadź nazwę konta dla autoryzacji na serwerze LDAP. Możesz użyć makr dostępnych na liście **Dostępne makra**.

8. W polu **Hasło** wpisz hasło do konta LDAP do autoryzacji na serwerze LDAP.

9. W polu **Adres serwera** wpisz nazwę domeny serwera LDAP. Możesz użyć makr dostępnych na liście **Dostępne makra**.

10. Aby używać protokołu przesyłania danych SSL (Secure Sockets Layer) do ochrony przesyłania wiadomości, zaznacz pole **Użyj połączenia SSL**.

11. Utwórz listę wyszukiwanych zwrotów wykorzystywanych podczas dostępu użytkownika urządzenia mobilnego iOS MDM do danych firmowych na serwerze LDAP:

    a. W sekcji **Ustawienia wyszukiwania** kliknij przycisk **Dodaj**.

    W tabeli z wyszukiwanymi zapytaniami pojawi się pusty rząd.

    b. W kolumnie **Nazwa** wprowadź nazwę wyszukiwanego zapytania.

    c. W kolumnie **Zakres wyszukiwania** wybierz poziom zagnieżdżenia folderu dla wyszukiwania danych firmowych na serwerze LDAP:

    - **Baza** – wyszukiwanie w folderze podstawowym na serwerze LDAP.
    - **Jeden poziom** – wyszukiwanie w folderach na pierwszym poziomie zagnieżdżenia, począwszy od folderu podstawowego.
    - **Poddrzewo** – wyszukiwanie w folderach na wszystkich poziomach zagnieżdżenia, począwszy od folderu podstawowego.

    d. W kolumnie **Baza wyszukiwania** wprowadź ścieżkę do folderu na serwerze LDAP, od którego rozpoczyna się wyszukiwanie (na przykład: "ou=people", "o=example corp").

    e. Powtórz czynności z kroków a-d dla wszystkich wyszukiwanych zapytań, które chcesz dodać do urządzenia iOS MDM.

12. Kliknij **OK**.

    Nowe konto LDAP pojawi się na liście.

13. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, konta LDAP z utworzonej listy zostaną dodane na urządzeniu mobilnym użytkownika. Użytkownik może uzyskać dostęp do kontaktów firmowych w standardowych aplikacjach iOS: Kontakty, Wiadomości i Poczta.

Dodawanie konta kalendarza

Aby umożliwić użytkownikowi urządzenia iOS MDM uzyskanie dostępu do zdarzeń w kalendarzu użytkownika na serwerze CalDAV, dodaj konto CalDAV. Synchronizacja z serwerem CalDAV umożliwi użytkownikowi tworzenie i otrzymywanie zaproszeń, pobieranie uaktualnień zdarzeń oraz synchronizowanie zadań z aplikacją Reminders.

W celu dodania konta CalDAV użytkownika urządzenia iOS MDM:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie **Właściwości** wybierz sekcję **Kalendarz**.
5. W sekcji **Konta CalDAV** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Konto CalDAV**.

6. W polu **Opis** wpisz opis konta CalDAV użytkownika.

7. W polu **Adres serwera i port** wprowadź nazwę hosta lub adres IP serwera CalDAV oraz numer portu serwera CalDAV.

8. W polu **Główny adres URL** określ adres URL konta CalDAV użytkownika urządzenia iOS MDM na serwerze CalDAV (na przykład: http://example.com/caldav/users/mycompany/user).

   Adres URL powinien rozpoczynać się od `"http://"` lub `"https://"`.

9. W polu **Nazwa konta** wprowadź nazwę konta dla autoryzacji na serwerze CalDAV.

10. W polu **Hasło** ustaw hasło do konta CalDAV w celu autoryzacji na serwerze CalDAV.

11. Aby używać protokołu przesyłania danych SSL (Secure Sockets Layer) do ochrony transmisji danych zdarzenia pomiędzy serwerem CalDAV a urządzeniem mobilnym, zaznacz pole **Użyj połączenia SSL**.

12. Kliknij **OK**.

    Nowe konto CalDAV pojawi się na liście.

13. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, konta CalDAV z utworzonej listy zostaną dodane na urządzeniu mobilnym użytkownika.

Dodawanie konta kontaktów

Aby umożliwić użytkownikowi urządzenia iOS MDM synchronizowanie danych z serwerem CardDAV, dodaj konto CardDAV. Synchronizacja z serwerem CardDAV umożliwia użytkownikowi uzyskanie dostępu do szczegółów kontaktów z dowolnego urządzenia.

W celu dodania konta CardDAV użytkownika urządzenia iOS MDM:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.

4. W oknie **Właściwości** wybierz sekcję **Kontakty**.

5. W sekcji **Konta CardDAV** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Konto CardDAV**.

6. W polu **Opis** wpisz opis konta CardDAV użytkownika. Możesz użyć makr dostępnych na liście **Dostępne makra**.

7. W polu **Adres serwera i port** wprowadź nazwę hosta lub adres IP serwera CardDAV oraz numer portu serwera CardDAV.

8. W polu **Główny adres URL** określ adres URL konta CardDAV użytkownika urządzenia iOS MDM na serwerze CardDAV (na przykład: http://example.com/carddav/users/mycompany/user).

   Adres URL powinien rozpoczynać się od `"http://"` lub `"https://"`.

9. W polu **Nazwa konta** wprowadź nazwę konta dla autoryzacji na serwerze CardDAV. Możesz użyć makr dostępnych na liście **Dostępne makra**.

10. W polu **Hasło** ustaw hasło do konta CardDAV w celu autoryzacji na serwerze CardDAV.

11. Aby używać protokołu przesyłania danych SSL (Secure Sockets Layer) do ochrony transmisji kontaktów pomiędzy serwerem CardDAV a urządzeniem mobilnym, zaznacz pole **Użyj połączenia SSL**.

12. Kliknij **OK**.

    Nowe konto CardDAV pojawi się na liście.

13. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, konta CardDAV z utworzonej listy zostaną dodane na urządzeniu mobilnym użytkownika.

Konfigurowanie subskrypcji kalendarza

Aby umożliwić użytkownikowi urządzenia iOS MDM dodawanie zdarzeń z kalendarzy udostępnionych (np. kalendarza firmowego) do kalendarza użytkownika, należy dodać subskrypcję do tego kalendarza. *Kalendarze udostępnione* to kalendarze innych użytkowników, którzy posiadają konto CalDAV, kalendarze iCal i inne otwarcie publikowane kalendarze.

W celu dodania subskrypcji kalendarza:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.

4. W oknie **Właściwości** wybierz sekcję **Subskrypcja kalendarza**.

5. W sekcji **Subskrypcje kalendarza** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Subskrypcja kalendarza**.

6. W polu **Opis** wprowadź opis subskrypcji kalendarza.

7. W polu **Adres internetowy serwera** określ adres internetowy kalendarza innego podmiotu.

   W tym polu możesz wprowadzić główny adres URL konta CalDAV użytkownika, którego kalendarz subskrybujesz. Możesz także określić adres URL kalendarza iCal lub innego otwarcie opublikowanego kalendarza.

8. W polu **Nazwa użytkownika** wprowadź nazwę konta użytkownika dla autoryzacji na serwerze kalendarza innego podmiotu.

9. W polu **Hasło** wprowadź hasło do subskrypcji kalendarza dla autoryzacji na serwerze kalendarza innego podmiotu.

10. Aby używać protokołu przesyłania danych SSL (Secure Sockets Layer) do ochrony transmisji danych zdarzenia pomiędzy serwerem CalDAV a urządzeniem mobilnym, zaznacz pole **Użyj połączenia SSL**.

11. Kliknij **OK**.

12. Nowa subskrypcja kalendarza pojawi się na liście.

13. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

    W rezultacie, po zastosowaniu zasady, zdarzenia z kalendarza udostępnionego znajdującego się na liście zostaną dodane do kalendarza na urządzeniu mobilnym użytkownika.

Dodawanie web clips

Web clip to aplikacja, która otwiera stronę internetową z ekranu głównego urządzenia mobilnego. Klikając ikony web clip na ekranie głównym urządzenia, użytkownik może szybko otwierać strony internetowe (takie, jak firmowe strony internetowe). Można dodać web clips na urządzeniach użytkowników oraz skonfigurować wygląd ikony web clip wyświetlanej na ekranie.

Domyślnie, stosowane są następujące ograniczenia korzystania z web clip:

- Użytkownik nie może ręcznie usunąć web clips z urządzenia mobilnego.
- Strony internetowe otwierane, gdy użytkownik kliknie ikonę web clip, nie są otwierane w trybie pełnoekranowym.
- Do ikony web clip na ekranie stosowane są zaokrąglone rogi, cień i efekty wizualne.

W celu dodania web clip na urządzeniu iOS MDM użytkownika:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.
4. W oknie **Właściwości** zasady wybierz sekcję **Web Clips**.
5. W sekcji **Web Clips** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Web Clip**.
6. W polu **Nazwa** wprowadź nazwę web clip, jaka ma być wyświetlana na ekranie urządzenia iOS MDM.
7. W polu **Adres internetowy** wprowadź adres strony internetowej, która zostanie otwarta po kliknięciu ikony web clip. Adres powinien rozpoczynać się od `"http://"` lub `"https://"`.
8. Aby zezwolić użytkownikowi na usunięcie web clip z urządzenia iOS MDM, zaznacz opcję **Zezwól na usuwanie**.
9. Kliknij przycisk **Wybierz** i określ plik z obrazem dla ikony web clip.

   Ikona jest wyświetlana na ekranie głównym urządzenia iOS MDM. Obrazek musi spełniać następujące wymagania:

   - Rozmiar obrazu nie powinien przekraczać 400 x 400 pikseli.
   - Format pliku: GIF, JPEG lub PNG.
   - Rozmiar pliku powinien być mniejszy niż 1 MB.

   Podgląd ikony web clip jest dostępny w polu **Ikona**. Jeśli nie wybierzesz obrazu dla web clip, jako ikona zostanie wyświetlony pusty kwadrat.

Jeśli chcesz, żeby ikona web clip była wyświetlana bez specjalnych efektów wizualnych (zaokrąglone rogi ikony, połysk), zaznacz pole **Ikona typu precomposed**.

10. Jeśli chcesz, żeby po kliknięciu ikony strona internetowa była otwierana w trybie pełnoekranowym na urządzeniu iOS MDM, zaznacz pole **Pełnoekranowy Web Clip**.

11. Kliknij **OK**.

    Nowy web clip pojawi się na liście.

12. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, ikony web clip z utworzonej listy zostaną dodane na ekranie głównym urządzenia mobilnego użytkownika.

Dodawanie czcionek

W celu dodania czcionki na urządzeniu iOS MDM użytkownika:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia iOS MDM.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie.

4. W oknie **Właściwości** wybierz sekcję **Czcionki**.

5. W sekcji **Czcionki** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Czcionka**.

6. W polu **Nazwa pliku** określ ścieżkę do pliku czcionki (plik z rozszerzeniem .ttf lub .otf).

   Czcionki posiadające rozszerzenie ttc lub otc nie są obsługiwane.

   Czcionki są identyfikowane po nazwie PostScript. Nie instaluj czcionek z tą samą nazwą PostScript nawet wtedy, gdy ich zawartość się różni. Instalacja czcionek z tą samą nazwą PostScript spowoduje wystąpienie niezdefiniowanego błędu.

7. Kliknij **Otwórz**.

   Nowa czcionka pojawi się na liście.

8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

W rezultacie, po zastosowaniu zasady, zostanie wyświetlone pytanie o zainstalowanie czcionek z utworzonej listy.

Zarządzanie aplikacją za pomocą systemów EMM innych firm (tylko Android)

Możesz używać aplikacji Kaspersky Endpoint Security for Android bez systemów zarządzania Kaspersky. Użyj rozwiązań innych dostawców usług EMM (Enterprise Mobility Management) do wdrożenia i zarządzania aplikacją Kaspersky Endpoint Security for Android. Kaspersky uczestniczy w AppConfig Community, aby zapewnić, że aplikacja działa z rozwiązaniami EMM firm trzecich.

Aplikacją Kaspersky Endpoint Security for Android można zarządzać za pomocą rozwiązań EMM innych firm tylko na urządzeniach z systemem Android.

Możesz użyć rozwiązań EMM innych firm do wdrożenia tylko aplikacji Kaspersky Endpoint Security for Android. Podłącz urządzenie do Kaspersky Security Center i zarządzaj aplikacją w Konsoli administracyjnej. W tym przypadku zarządzanie aplikacją Kaspersky Endpoint Security for Android w konsoli EMM będzie niedostępne.

Jeśli wdrożyłeś aplikację Kaspersky Endpoint Security for Android przy użyciu systemu EMM innej firmy, niemożliwe jest zarządzanie aplikacją w Kaspersky Endpoint Security Cloud. Możesz zarządzać aplikacją Kaspersky Endpoint Security for Android w konsoli EMM.

Następujące rozwiązania EMM obsługują korzystanie z aplikacji Kaspersky Endpoint Security for Android:

- VMware AirWatch
- MobileIron
- IBM Maas360
- Microsoft Intune
- SOTI MobiControl

W konsoli EMM możesz wykonać następujące czynności:

- Dodać aplikację do profilu roboczego Android na urządzeniach użytkowników.
- Aktywować aplikację.
- Skonfigurować ustawienia aplikacji:
  - Włączyć ochronę przed szkodliwymi i phishingowymi stronami internetowymi.
  - Skonfigurować ustawienia podłączania urządzenia do Kaspersky Security Center.
  - Skonfigurować ustawienia Antywirusa.
  - Skonfigurować terminarz uruchamiania skanowania antywirusowego na urządzeniu.
  - Włączyć wykrywanie adware i aplikacji, które mogą być wykorzystywane przez cyberprzestępców do uszkodzenia urządzenia lub kradzieży danych osobowych użytkownika.
  - Skonfigurować terminarz aktualizacji baz danych aplikacji.

Rozpoczęcie pracy

Aby zainstalować aplikację na urządzeniach mobilnych użytkowników, musisz dodać Kaspersky Endpoint Security for Android do magazynu aplikacji EMM. Możesz dodać Kaspersky Endpoint Security for Android do magazynu aplikacji EMM, korzystając z odnośnika Google Play. Więcej informacji na temat pracy z aplikacjami w konsoli EMM można znaleźć na *stronie pomocy technicznej dostawcy usługi EMM*.

Aplikacja Kaspersky Endpoint Security for Android jest wdrażana w profilu roboczym Android. Aplikacja jest odizolowana od osobistych danych użytkownika i chroni tylko dane firmowe w profilu roboczym. Zalecane jest zapewnienie ochrony Kaspersky Endpoint Security for Android przed usuwaniem przy użyciu narzędzi konsoli EMM.

Instalowanie aplikacji

W zależności od konsoli EMM, wybierz metodę instalacji aplikacji na urządzeniach: cicha instalacja, wyślij wiadomość e-mail zawierającą odnośnik do aplikacji w Google Play lub inna dostępna metoda.

Do działania aplikacji wymagane są następujące uprawnienia:

- Uprawnienie Pamięć do uzyskania dostępu do pliku, gdy uruchomiony jest Antywirus (tylko dla systemu Android 6.0 lub nowszej wersji).
- Uprawnienie telefonu do identyfikowania urządzenia, na przykład, podczas aktywowania aplikacji.
- Żądanie dodania programu Kaspersky Endpoint Security for Android do listy aplikacji, które są uruchamiane podczas uruchamiania systemu operacyjnego (na niektórych urządzeniach, takich jak Huawei, Meizu i Xiaomi). Jeśli żądanie dodania nie zostanie wyświetlone, ręcznie dodaj Kaspersky Endpoint Security for Android do tej listy. Żądanie może nie zostać wyświetlone, jeśli aplikacja nie jest zainstalowana w profilu roboczym.

Teraz możesz nadać wymagane uprawnienia w konsoli EMM przed rozpoczęciem wdrażania aplikacji Kaspersky Endpoint Security for Android. Więcej informacji na temat nadawania uprawnień w konsoli EMM można znaleźć na *stronie pomocy technicznej dostawcy usługi EMM*. Uprawnienia możesz nadać także podczas kończenia działania Kreatora wstępnej konfiguracji Kaspersky Endpoint Security for Android na urządzeniu.

Aplikacja Kaspersky Endpoint Security for Android zostanie zainstalowana w profilu roboczym Android.

W celu zapewnienia działania Ochrony WWW, należy skonfigurować serwer proxy w ustawieniach Google Chrome:

- Tryb konfiguracji serwera proxy: ręcznie.
- Port i adres serwera proxy: 127.0.0.1:3128.
- Obsługa protokołu SPDY: wyłączona.
- Kompresja danych poprzez serwer proxy: wyłączona.

Aktywowanie aplikacji

Informacje o licencji są wysyłane na urządzenie mobilne wraz z innymi ustawieniami w pliku konfiguracyjnym.

Jeśli aplikacja nie zostanie aktywowana w ciągu 30 dni od jej zainstalowania na urządzeniu mobilnym, licencja testowa utraci ważność. Po wygaśnięciu licencji testowej, wszystkie funkcje aplikacji mobilnej Kaspersky Endpoint Security for Android zostają wyłączone.

Po wygaśnięciu licencji komercyjnej, aplikacja mobilna działa, ale z ograniczoną funkcjonalnością (na przykład, aktualizacje baz danych Kaspersky Endpoint Security for Android są niedostępne). Aby kontynuować korzystanie z aplikacji w trybie pełnej funkcjonalności, musisz odnowić licencję komercyjną.

W celu aktywowania Kaspersky Endpoint Security for Android:

1. W konsoli EMM otwórz ustawienia aplikacji Kaspersky Endpoint Security for Android.
2. W polu `LicenseActivationCode` wprowadź kod aktywacyjny aplikacji.

   Aby aktywować aplikację na urządzeniu, musisz mieć dostęp do serwerów aktywacji Kaspersky.

Jak podłączyć urządzenie do Kaspersky Security Center?

Po zainstalowaniu Kaspersky Endpoint Security for Android na urządzeniu mobilnym, możesz podłączyć urządzenie do Kaspersky Security Center. Dane niezbędne do podłączenia urządzenia do Kaspersky Security Center są przesyłane na urządzenie mobilne wraz z innymi ustawieniami umieszczonymi w pliku konfiguracji. Po podłączeniu urządzenia do Kaspersky Security Center, możesz użyć zasad grupowych do scentralizowanego konfigurowania ustawień aplikacji. Możesz także pobierać raporty i statystyki dotyczące działania Kaspersky Endpoint Security for Android.

Przed podłączeniem urządzeń do Kaspersky Security Center, upewnij się, że spełnione są następujące warunki:

- Wtyczka zarządzająca Kaspersky Endpoint Security for Android jest zainstalowana na stacji roboczej administratora.
- Port do podłączania urządzeń mobilnych jest otwarty we właściwościach Serwera administracyjnego.
- Wyświetlanie folderu **Zarządzanie urządzeniami mobilnymi** jest włączone w Konsoli administracyjnej.
- Certyfikat ogólny do identyfikacji użytkownika urządzenia mobilnego został utworzony w magazynie certyfikatów Kaspersky Security Center.

Przed podłączeniem urządzeń do Kaspersky Security Center, zalecane jest wykonanie następujących czynności:

- Jeśli chcesz utworzyć zadania i zasady dla urządzeń mobilnych, utwórz oddzielną grupę administracyjną dla urządzeń mobilnych.
- Jeśli chcesz automatycznie przenieść urządzenia mobilne do oddzielnej grupy administracyjnej, utwórz regułę dla automatycznego przenoszenia urządzeń z folderu **Urządzenia nieprzypisane**.
- Jeśli chcesz skonfigurować Kaspersky Endpoint Security for Android w sposób scentralizowany, utwórz zasadę grupową.

W celu podłączenia urządzenia do Kaspersky Security Center:

1. W konsoli EMM otwórz ustawienia aplikacji Kaspersky Endpoint Security for Android.
2. W polu `KscServer` wprowadź nazwę DNS lub adres IP Serwera administracyjnego Kaspersky Security Center. Domyślny port to 13292.
3. Jeśli nie chcesz, aby powiadomienia Kaspersky Endpoint Security for Android rozpraszały użytkownika, wyłącz powiadomienia aplikacji. W tym celu, określ ustawienie `DisableNotification = True`.

Po nawiązaniu połączenia, aplikacja wyświetli wszystkie powiadomienia. Możesz wyłączyć pewne powiadomienia aplikacji w ustawieniach zasady.

Nie wyłączaj powiadomień aplikacji, jeśli nie korzystasz z Kaspersky Security Center. Może to spowodować, że użytkownik nie będzie otrzymywał powiadomień o wygaśnięciu licencji. W rezultacie aplikacja przestanie wykonywać swoje funkcje.

Po skonfigurowaniu ustawień połączenia, Kaspersky Endpoint Security for Android wyświetli powiadomienie z pytaniem o nadanie następujących dodatkowych uprawnień:

- Uprawnienie do korzystania z Aparatu, niezbędne do działania Anti-Theft (polecenie **Zdjęcie**).
- Uprawnienie do użycia Lokalizacji, niezbędne do działania z zakresu Anti-Theft (polecenie **Zlokalizuj urządzenie**).
- Uprawnienie administratora urządzenia (właściciel profilu roboczego Android), niezbędne do działania następujących funkcji aplikacji:
  - Instalowanie certyfikatu bezpieczeństwa.
  - Konfigurowanie Wi-Fi.
  - Konfigurowanie Exchange ActiveSync.
  - Ograniczenie korzystania z aparatu, Bluetooth i Wi-Fi.

Ze względu na specyficzną charakterystykę profilu roboczego Android (brak usługi dostępności), funkcje Kontrola aplikacji i Anti-Theft są niedostępne w aplikacji.

Jeśli użytkownik nada niezbędne uprawnienia, urządzenie zostanie podłączone do Kaspersky Security Center. Jeśli reguła automatycznego przenoszenia urządzeń do grupy administracyjnej nie została utworzona, urządzenie zostanie automatycznie dodane do folderu **Urządzenia nieprzypisane**. Jeśli reguła automatycznego przenoszenia urządzeń do grupy administracyjnej została utworzona, urządzenie zostanie automatycznie dodane do zdefiniowanej grupy.

Kaspersky Endpoint Security oferuje następujący format nazwy urządzeń:

- Model urządzenia [e-mail, ID urządzenia].
- Model urządzenia [e-mail (jeśli jest) lub ID urządzenia].

ID urządzenia to unikatowy numer ID, który jest generowany przez Kaspersky Endpoint Security for Android z danych otrzymanych z urządzenia. W przypadku urządzeń mobilnych działających pod kontrolą systemu Android 10 lub nowszego, Kaspersky Endpoint Security for Android używa SSAID (Android ID) lub sumy kontrolnej innych danych otrzymanych z urządzenia. Dla wcześniejszych wersji systemu Android aplikacja używa IMEI. Możesz skonfigurować format nazwy urządzenia w zasadzie grupy. Możesz także dodać znacznik do nazwy urządzenia. Ułatwia to znalezienie i posortowanie urządzeń w Kaspersky Security Center. Ten znacznik jest dostępny tylko dla VMware AirWatch.

W celu dodania znacznika do nazwy urządzenia:

1. W konsoli EMM otwórz ustawienia aplikacji Kaspersky Endpoint Security for Android.
2. W polu `KscDeviceNameTag` wybierz wartości:

- `{DeviceSerialNumber}` – numer seryjny urządzenia.
- `{DeviceUid}` – unikatowy identyfikator urządzenia (UDID).
- `{DeviceAssetNumber}` – numer wyposażenia urządzenia. Ten numer jest tworzony wewnętrznie z poziomu organizacji.

Zalecamy użycie tylko tych wartości. VMware AirWatch obsługuje inne wartości, ale Kaspersky Endpoint Security nie może zagwarantować pracy z tymi wartościami.

Możesz dodać niektóre wartości (na przykład: `{DeviceSerialNumber} {DeviceUid}`). Znacznik zostanie dodany do nazwy urządzenia w Kaspersky Security Center. Spacja oddziela znacznik od nazwy urządzenia. Na przykład, `Google Pixel 2 a10c6b75f7b31de9 22:7D:78:9E:C5:1E`, wówczas `22:7D:78:9E:C5:1E` to znacznik UDID. Jeśli używasz Kaspersky Security Center i VMwareAirWatch, znacznik umożliwia zidentyfikowanie urządzeń w obu konsolach. Aby dopasować urządzenie, wybierz takie same wartości dla nazwy urządzenia (na przykład: numer seryjny urządzenia).

Po podłączeniu urządzenia do Kaspersky Security Center, ustawienia aplikacji zostaną zmienione zgodnie z zasadą grupy. Kaspersky Endpoint Security for Android ignoruje ustawienia aplikacji z pliku konfiguracji, które zostały skonfigurowane w konsoli EMM. Możesz skonfigurować wszystkie sekcje zasady, za wyjątkiem następujących sekcji:

- **Anti-Theft** (Blokada urządzenia)
- **Kontenery**
- **Zarządzanie urządzeniem** (Blokada ekranu)
- **Kontrola aplikacji** (Blokada zabronionych aplikacji)
- **Profil roboczy Android**
- **Zarządzaj Samsung KNOX**

Ze względu na metodę użytą do wdrażania profilu roboczego nie możesz zastosować ustawień zasady grupy z sekcji **Profil roboczy Android**. Te ustawienia mogą być stosowane tylko wtedy, gdy profil roboczy został utworzony przy użyciu Kaspersky Security Center.

Plik AppConfig

Plik konfiguracyjny jest generowany do skonfigurowania aplikacji w konsoli EMM. Ustawienia aplikacji w pliku konfiguracyjnym przedstawiono w poniższej tabeli.

Konfigurowanie ustawień pliku

Klucz konfiguracji	Opis	Typ	Wartość
`LicenseActivationCode`	Kod aktywacyjny aplikacji	String	Kod aktywacyjny aplikacji składający si dwudziestu łacińskich liter i cyfr. Aby aktywować aplikację kodem aktywacyjnym, potrzebny jest dostęp internetu w celu nawiązania połączenia serwerami aktywacji Kaspersky.

			Jeśli pozostawisz to pole puste, aplika zostanie aktywowana przy użyciu licer testowej. Okres ważności licencji testowej wynosi 30 dni. Po wygaśnięci licencji testowej, wszystkie funkcje aplikacji mobilnej Kaspersky Endpoint Security for Android zostają wyłączon Aby kontynuować korzystanie z aplika musisz zakupić licencję komercyjną.
`EulaAcceptanceConfirmationV1`	<Odnośnik do Umowy licencyjnej>	Choice	To ustawienie jest dostępne tylko dla VMware AirWatch. `Accepted` – Potwierdzam, że w pełni przeczytałem, zrozumiałem i akceptuję warunki niniejszej Umowy licencyjnej. `Declined` – Nie akceptuję warunków i postanowień tej Umowy Licencyjnej. Aby zaakceptować warunki Umowy licencyjnej dla wszystkich urządzeń mobilnych, potrzebny jest dostęp do internetu w celu nawiązania połączenia serwerami Kaspersky. Jeśli wybierzesz opcję `Declined`, aplikacja wyświetli pytanie o zaakceptowanie warunków Umowy licencyjnej. Użytkownicy urządzeń mobilnych mogą zaakceptować warun w Kreatorze wstępnej konfiguracji.
`EulaAcceptanceCodeV1`	Kod Umowy licencyjnej	String	Te ustawienia są dostępne tylko dla VMware AirWatch. Użyj `EulaAcceptanceCodeV1`, jeśli chcesz zaakceptować pojedynczą Umowę licencyjną użytkownika końcowego (EULA). Użyj `EulaAcceptanceCodesV2`, jeśli chces zaakceptować kilka umów EULA w tym samym czasie. Pole `EulaAcceptanceCodesV2` musi zawierać rozdzieloną średnikami listę kodów EULA: `"<EULAid1>;<EULAid2 <EULAid3>;..."`. Kod Umowy licencyjnej znajduje się w Umowie licencyjnej. *W celu poznania kodu Umowy licencyj* 1. Skopiuj link Umowy licencyjnej (`EulaAcceptanceConfirmation` z konsoli EMM.
`EulaAcceptanceCodesV2`	Kody Umowy licencyjnej	String	

			2. Wklej odnośnik w przeglądarce. Zostanie otwarta Umowa licencyjna 3. Przeczytaj warunki tej Umowy licencyjnej i odszukaj kod Umowy licencyjnej. Aby zaakceptować warunki Umowy licencyjnej dla wszystkich urządzeń mobilnych, potrzebny jest dostęp d internetu w celu nawiązania połączenia z serwerami Kaspersky. Jeśli pozostawisz pola puste, aplikacja wyświetli pytanie o zaakceptowanie warunków Umowy licencyjnej. Użytkow urządzenia mobilnego może zaakceptować warunki w Kreatorze wstępnej konfiguracji. Jeśli określisz wartości obu pól, warunl wszystkich zawartych w nich umów EULA zostaną zaakceptowane.
`KscServer`	Port i adres Serwera administracyjnego Kaspersky Security Center	String	Nazwa DNS lub adres IP Serwera administracyjnego Kaspersky Security Center i numer portu. Wprowadź adre w następujący sposób: `<adres serwera>:<port>`. Jeśli wprowadzisz adres serwera bez określania portu, aplikacja użyje domyślnego portu 1329
`DisableNotification`	Przed nawiązaniem połączenia z Kaspersky Security Center wyłącz powiadomienia aplikacji.	Boolean	`True` – Kaspersky Endpoint Security f Android ukrywa wszystkie powiadomienia aplikacji. Kaspersky Endpoint Security for Android ukrywa powiadomienia, dopóki urządzenie nie nawiąże połączenia z Kaspersky Secur Center. Po nawiązaniu połączenia, aplikacja wyświetli wszystkie powiadomienia. Możesz wyłączyć pew powiadomienia aplikacji w ustawieniach zasady. Nie wyłączaj powiadomień aplikacji, jeśli nie korzystasz z Kaspersky Security Center. Może to spowodować, że użytkownik nie będzie otrzymywał powiadomień o wygaśnięciu licencji. W tym przypadku aplikacja przestanie wykonywać swoje funkcje. `False` – Kaspersky Endpoint Security for Android wyświetla wszystkie powiadomienia aplikacji.
`ScanScheduleType`	Tryb uruchamiania skanowania	Choice	`AfterUpdate` – uruchomienie skanowania antywirusowego po

			aktualizacji bazy danych. Aplikacja aktualizuje antywirusowe bazy danych zgodnie z określonym terminarzem (`UpdateScheduleType`). `Daily` – uruchamianie skanowania antywirusowego raz dziennie. Skonfigu czas rozpoczęcia skanowania (`ScanScheduleTime`). `Weekly` – uruchamianie skanowania antywirusowego raz w tygodniu. Wybi dzień tygodnia, aby rozpocząć skanowanie antywirusowe (`ScanScheduleDay`) i skonfiguruj czas (`ScanScheduleTime`). `Off` – automatyczne uruchamianie skanowania antywirusowego jest wyłączone. Niezależnie od ustawionej wartości użytkownik urządzenia może ręcznie uruchomić skanowanie antywirusowe.
`ScanScheduleDay`	Dzień skanowania	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` Możesz wybrać tylko jedną wartość dl tego ustawienia.
`ScanScheduleTime`	Czas skanowania	String	Czas można wyświetlić w formacie 24-godzinnym (na przykład 13:00) lub 12-godzinnym (na przykład 10:30 P.M.).
`ScanScheduleLock`	Zablokuj konfigurację trybu uruchamiania skanowania	Boolean	`True` – użytkownik nie może uzyskać dostępu do ustawień trybu uruchamia skanowania antywirusowego w ustawieniach aplikacji. `False` – użytkownik może skonfigurować tryb uruchamiania skanowania antywirusowego i, na przykład, wyłączyć autostart skanowa antywirusowego.
`ScanOnlyExecutableFiles`	Rodzaje plików do skanowania (skanowanie antywirusowe)	Choice	`AllFiles` – skanuj wszystkie pliki. `OnlyExecutables` – skanuj tylko pliki wykonywalne. Pliki wykonywalne to plik rozszerzeniami .apk (.zip), .dex lub .so. W Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1 nie możesz włączyć skanowa tylko plików wykonywalnych.
`ScanArchives`	Skanuj archiwa bez rozpakowywania	Boolean	`True` – aplikacja rozpakowuje archiwa skanuje ich zawartość. `False` – aplikacja skanuje tylko pliki archiwum. Aplikacja skanuje tylko archiwa z rozszerzeniem .zip (.apk).

			W Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1 nie możesz wyłączyć skanowania zawartości archiwów.
`ScanActionOnThreatFound`	Działania dotyczące wykrywania zagrożeń (Skanowanie antywirusowe)	Choice	`Quarantine` – aplikacja umieszcza wykryte obiekty w Kwarantannie. Kwarantanna przechowuje pliki w archiwum, więc nie mogą one uszkodzi urządzenia. Kwarantanna umożliwia usunięcie lub przywrócenie plików, któ zostały przeniesione do odizolowaneg magazynu. `Delete` – aplikacja usuwa wykryte obiekty. `Skip` – aplikacja pozostawia wykryte obiekty w niezmienionej postaci. Jeśli wykryte obiekty zostaną pominięte, Kaspersky Endpoint Security for Andr ostrzeże użytkownika o problemach z ochroną urządzenia. Gdy nastąpi prób uzyskania dostępu do obiektu na urządzeniu (np. Próba jego skopiowani lub otwarcia), aplikacja blokuje dostęp obiektu. `AskUser` – aplikacja prosi użytkownika wybranie akcji dla każdego wykrytego obiektu: pomiń, poddaj kwarantannie lu usuń. Po wykryciu wielu obiektów użytkownik może zastosować wybrana akcję do wszystkich obiektów. Informacje o wykrytych zagrożeniach i podjętych działaniach są rejestrowane raportach aplikacji.
`ScanLock`	Blokuj konfigurację ustawień skanowania	Boolean	`True` – następujące ustawienia skanowania nie są dostępne dla użytkownika w ustawieniach aplikacji: t plików do skanowania, skanowanie archiwów i działanie podjęte po wykryc zagrożenia. `False` – użytkownik może skonfigurować ustawienia skanowania na przykład, wybrać akcję `Skip` dla wykrytych zagrożeń.
`ScanAndProtectionAdwareRiskware`	Blokuj oprogramowanie reklamowe, autodialery i aplikacje, które mogą być wykorzystywane przez przestępców do uszkodzenia urządzenia i danych użytkownika	Boolean	`True` – aplikacja wykrywa adware i inn aplikacje, które mogą być użyte przez przestępców do uszkodzenia urządzer użytkownika i jego danych. `False` – aplikacja pomija adware i inne aplikacje, które mogą być użyte przez przestępców do uszkodzenia urządzer użytkownika i jego danych.

`ProtectionMode`	Tryb Ochrony w czasie rzeczywistym	Choice	`Recommended` – aplikacja skanuje tylk nowe aplikacje zaraz po ich zainstalowaniu, a także pliki z folderu Pobrane. `Extended` – aplikacja skanuje wszystk pliki, które użytkownik otwiera, modyfikuje, kopiuje, uruchamia i zapisu na urządzeniu. Aplikacja skanuje równie nowe aplikacje i pliki z folderu Pobrane `Disabled` – Ochrona w czasie rzeczywistym jest wyłączona.
`UseKsnMode`	Tryb Kaspersky Security Network	Choice	`Recommended` – aplikacja wymienia da z Kaspersky Security Network (KSN). Kaspersky Endpoint Security for Andr używa KSN do ochrony urządzenia prz zagrożeniami w czasie rzeczywistym (Ochrona w chmurze) oraz do działania Ochrony WWW w internecie. `Extended` – aplikacja wymienia dane z Kaspersky Security Network i wysyła również do Laboratorium antywirusowego statystyki działania z Kaspersky Endpoint Security for Android. Te informacje umożliwiają śledzenie zagrożeń w czasie rzeczywistym. Żadne dane osobowe n są gromadzone, przetwarzane ani przechowywane przez usługi KSN. `Disabled` – aplikacja nie korzysta z danych z Kaspersky Security Network Nie można włączyć Ochrony WWW (`EnableWebFilter`). Komponent Ochrona w chmurze nie jest dostępny dla Antywirusa.
`ProtectScanOnlyExecutableFiles`	Rodzaje plików do skanowania (ochrona w czasie rzeczywistym)	Boolean	`AllFiles` – skanuj wszystkie pliki. `OnlyExecutables` – skanuj tylko pliki wykonywalne. Pliki wykonywalne to plik rozszerzeniami .apk (.zip), .dex lub .so. W Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1 nie możesz włączyć skanowa tylko plików wykonywalnych.
`ProtectionActionOnThreatFound`	Działania podejmowane po wykryciu zagrożeń (ochrona w czasie rzeczywistym)	Choice	`Quarantine` – aplikacja umieszcza wykryte obiekty w Kwarantannie. Kwarantanna przechowuje pliki w archiwum, więc nie mogą one uszkodzi urządzenia. Kwarantanna umożliwia usunięcie lub przywrócenie plików, któ zostały przeniesione do odizolowaneg magazynu. `Delete` – aplikacja usuwa wykryte obiekty.

			`Skip` – aplikacja pozostawia wykryte obiekty w niezmienionej postaci. Jeśli wykryte obiekty zostaną pominięte, Kaspersky Endpoint Security for Andr ostrzeże użytkownika o problemach z ochroną urządzenia. Jeśli zostanie podjęta próba uzyskania dostępu do obiektu na urządzeniu (np. Próba jego skopiowania lub otwarcia), aplikacja blokuje dostęp do obiektu. Informacje o wykrytych zagrożeniach i podjętych działaniach są rejestrowane raportach aplikacji.
`ProtectionLock`	Zablokuj konfigurację ustawień ochrony w czasie rzeczywistym	Boolean	`True` – następujące ustawienia ochro w czasie rzeczywistym nie są dostępn dla użytkownika w ustawieniach aplikac tryb ochrony w czasie rzeczywistym, typy plików do skanowania oraz akcja, która ma zostać podjęta po wykryciu zagrożenia. `False` – użytkownik może skonfigurować ustawienia ochrony w czasie rzeczywistym i, na przykład, wybrać akcję `Skip` dla wykrytych zagrożeń.
`UpdateScheduleType`	Tryb uruchamiania aktualizacji baz danych	Choice	`Daily` – sprawdzaj dostępność nowyc antywirusowych baz danych i pobieraj na urządzenia raz dziennie. Skonfiguruj czas rozpoczęcia aktualizacji bazy danych (`UpdateScheduleTime`). `Weekly` – sprawdzaj dostępność nowych antywirusowych baz danych i pobieraj je na urządzenia raz w tygodn Wybierz dzień tygodnia, aby rozpoczą aktualizację bazy danych (`UpdateScheduleDay`) i skonfiguruj c (`UpdateScheduleTime`). `Off` – automatyczna aktualizacja antywirusowych baz danych jest wyłączona. Niezależnie od ustawionej wartości użytkownik urządzenia może ręcznie uruchomić aktualizację antywirusowyc baz danych.
`UpdateScheduleDay`	Dzień uruchomienia aktualizacji baz danych	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` Możesz wybrać tylko jedną wartość dl tego ustawienia.
`UpdateScheduleTime`	Czas uruchomienia aktualizacji baz danych	String	Czas można wyświetlić w formacie 24- godzinnym (na przykład 13:00) lub 12- godzinnym (na przykład 10:30 P.M.).
`UpdateScheduleLock`	Blokuj	Boolean	`True` – użytkownik nie może uzyskać

	konfigurację trybu uruchamiania aktualizacji baz danych		dostępu do ustawień trybu uruchamia aktualizacji baz danych w ustawieniach aplikacji. `False` – użytkownik może skonfigurować tryb uruchamiania aktualizacji baz danych i, na przykład, wyłączyć automatyczne uruchamianie aktualizacji baz danych.
`AllowUpdateInRoaming`	Aktualizacja baz danych podczas roamingu	Boolean	`True` – aplikacja pobiera antywirusow bazy danych, jeśli urządzenie znajduje w strefie roamingu. Aplikacja pobiera antywirusowe bazy danych zgodnie z określonym terminarzem (`UpdateScheduleType`). `False` – aplikacja nie pobiera antywirusowych baz danych, jeśli urządzenie znajduje się w sieci domow

`EnableWebFilter`	Ochrona WWW	Boolean	`True` – aplikacja używa komponentu Ochrona WWW do blokowania szkodliwych i phishingowych stron internetowych. Ochrona WWW obsługuje tylko przeglądarkę Google Chrome.
			Szkodliwe i phishingowe strony internetowe wykorzystujące protokół HTTPS mogą pozostać niezablokowane, jeśli domena jest zaufana. Jeśli domena jest niezaufana, Ochrona WWW zablokuje szkodliwe i phishingowe strony internetowe.
			`False` – ochrona przed szkodliwymi i phishingowymi stronami internetowym jest wyłączona.
			W celu zapewnienia działania komponentu Ochrona WWW muszą b spełnione następujące warunki:
			• Użytkownicy urządzeń akceptują Politykę prywatności i Oświadczeni dotyczące modułu Ochrona WWW Kreatorze wstępnej konfiguracji lub ustawieniach aplikacji.
			• Serwer proxy jest skonfigurowany w ustawieniach przeglądarki:
			`ProxyMode = "fixed_servers"`
			`ProxyServer = "127.0.0.1:3128"`
			`DisableSpdy = true`
			`DataCompressionProxyEnabled false`

			Konfiguracja serwera proxy może różnić się w zależności od wersji Google Chrome. Więcej informacji dotyczących konfigurowania Goog Chrome można znaleźć na stronie Projektu Chromium. Po usunięciu aplikacji Kaspersky Endpoint Security for Android z urządzenia mobilnego, zresetuj ustawienia serwera proxy. • Korzystanie z KSN jest włączone w ustawieniach aplikacji: `UseKsnMode Recommended` lub `UseKsnMode = Extended`. • Zalecane jest wybranie Google Chrome jako domyślnej przeglądarl w ustawieniach systemu operacyjnego.
`EnableWebFilterLock`	Blokuj konfigurację Ochrony WWW	Boolean	`True` – użytkownik nie może uzyskać dostępu do ustawień Ochrony WWW ustawieniach aplikacji. `False` – użytkownik może skonfigurować ustawienia Ochrony WWW, a także na przykład, wyłączyć ochronę przed szkodliwymi i phishingowymi stronami internetowym
`UpdateServer`	Adres serwera źródła uaktualnień baz danych	String	Adres serwera, na którym znajdują się uaktualnienia baz danych, na przykład, `http://update.server.com`. Jeśli pozostawisz pole puste, Kaspersk Endpoint Security for Android będzie korzystał z serwerów aktualizacji baz danych Kaspersky.
`AllowGoogleAnalytics`	Wysyłanie danych do usług Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics	Boolean	`True` – aplikacja automatycznie wysył dane dotyczące działania Kaspersky Endpoint Security for Android do usłu Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics. dane są niezbędne do udoskonalenia działania aplikacji i przeanalizowania zadowolenia użytkownika. Dane są przesyłane do usług Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics poprzez bezpieczne połączenie. Ochrona i dostęp do dany są regulowane zgodnie z warunkami korzystania z usług Google Analytics f Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics.

			`False` – wysyłanie danych do usług Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics jest wyłączone.
`KscDeviceNameTag`	Znacznik nazwy urządzenia dla Kaspersky Security Center	String	To ustawienie jest dostępne tylko dla VMware AirWatch. Znacznik zostanie dodany do nazwy urządzenia w Kaspersky Security Center. Spacja oddziela znacznik od nazwy urządzenia. Ułatwia to znalezier posortowanie urządzeń w Kaspersky Security Center. • `{DeviceSerialNumber}` – numer seryjny urządzenia. • `{DeviceUid}` – unikatowy identyfikator urządzenia (UDID). • `{DeviceAssetNumber}` – numer wyposażenia urządzenia. Ten nume jest tworzony wewnętrznie w obrębi organizacji. Możesz dodać niektóre wartości (n przykład: `{DeviceSerialNumber}` `{DeviceUid}`). Zalecamy użycie tylko tych wartośc VMware AirWatch obsługuje inne wartości, ale Kaspersky Endpoint Security nie może zagwarantować, że te wartości działają.
`KscGroup`	Nazwa grupy urządzeń	String	Możesz określić grupy urządzeń w konsoli EMM. Kiedy urządzenie zostani podłączone do Kaspersky Security Center, zostanie automatycznie dodar do podfolderu w folderze Nieprzypisar urządzenia. Nazwa podfolderu będzie zgodna z nazwą grupy określoną w tyn parametrze. Następnie można utworzy reguły automatycznego przenoszenia urządzeń z podfolderów w folderze Nieprzypisane urządzenia do grup administracyjnych w folderze Zarządza urządzenia. Jeśli pozostawisz to pole puste, urządzenie zostanie automatycznie dodane do katalogu głównego w folderze Nieprzypisane urządzenia.

`KscCorporateEmail`	Poczta firmowa użytkownika	String	Możesz określić firmowy adres e-mail użytkownika w konsoli EMM. Te adresy mail będą wyświetlane w Kaspersky Security Center. Wpisywany tekst musi być ważnym adresem e-mail. Pozostałe wartości są ignorowane.

Obciążenie sieci

Ta sekcja zawiera informacje na temat natężenia ruchu sieciowego wymienianego między urządzeniami mobilnymi i Kaspersky Security Center.

Natężenie ruchu

Zadanie	Wychodzący ruch sieciowy	Przychodzący ruch sieciowy	Całkowity ruch
Początkowe wdrożenie aplikacji, Mb	0.08	17.76	17.84
Początkowa aktualizacja antywirusowych baz danych (wielkość ruchu może się różnić ze względu na rozmiar antywirusowych baz danych), MB	0.04	2.21	2.25
Synchronizacja urządzenia mobilnego z Kaspersky Security Center, MB	0.03	0.02	0.05
Regularna aktualizacja antywirusowych baz danych (wielkość ruchu może się różnić ze względu na rozmiar antywirusowych baz danych), MB	0.08	3.06	3.14
Wykonywanie poleceń Anti-Theft. Lokalizacja urządzenia (natężenie ruchu może się różnić ze względu na specyfikację wbudowanej kamery i jakość zdjęć), MB	0.09	0.8	0.17
Wykonywanie poleceń Anti-Theft. Zrób zdjęcie (mugshot), MB	1.0	0.02	1.02
Wykonywanie poleceń Anti-Theft. Blokada urządzenia, MB	0.06	0.05	0.11
Średnia dzienna liczba, MB	0.22	6.96	7.18

Uczestnictwo w Kaspersky Security Network

W celu zapewnienia bardziej efektywnej ochrony, Kaspersky Endpoint Security for Android używa danych zebranych od użytkowników na całym świecie. Usługa *Kaspersky Security Network* została zaprojektowana do przetwarzania tych danych.

Kaspersky Security Network (KSN) jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacjom Kaspersky na zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów.

Uczestnictwo użytkownika w Kaspersky Security Network pomaga firmie Kaspersky uzyskać informacje o typach i źródłach nowych zagrożeń w czasie rzeczywistym, rozwijać metody ich neutralizacji, a także zmniejszyć liczbę fałszywych alarmów Kaspersky Endpoint Security for Android. Uczestnictwo w Kaspersky Security Network pozwala również uzyskać dostęp do statystyk reputacji dla aplikacji i stron internetowych.

Jeżeli uczestniczysz w Kaspersky Security Network, zbierane są pewne statystyki programu Kaspersky Endpoint Security for Android, które następnie są automatycznie wysyłane do Kaspersky. Te informacje umożliwiają śledzenie zagrożeń w czasie rzeczywistym. Pliki lub ich fragmenty, które mogły zostać wykorzystane przez cyberprzestępców do uszkodzenia komputera lub danych również mogą zostać przesłane do Kaspersky w celu przeprowadzenia dodatkowej analizy.

Korzystanie z Kaspersky Security Network jest wymagane do działania Kaspersky Endpoint Security for Android. KSN jest używany przez główne składniki aplikacji: Antywirusa, Ochronę WWW i Kontrolę aplikacji. Odrzucenie możliwości uczestniczenia w KSN zmniejsza poziom ochrony urządzenia, co może doprowadzić do infekcji urządzenia i utraty danych. Aby rozpocząć korzystanie z Kaspersky Security Network, podczas instalowania aplikacji musisz zaakceptować warunki Umowy licencyjnej. W Umowie licencyjnej opisano, które dane są przesyłane do Kaspersky Security Network przez Kaspersky Endpoint Security for Android.

Aby udoskonalić działanie aplikacji, możesz dodatkowo przesłać dane statystyczne do Kaspersky Security Network. Udostępnianie powyższych informacji KSN jest dobrowolne. Aby zacząć korzystać z Kaspersky Security Network, należy zaakceptować warunki specjalnej umowy – *Oświadczenia Kaspersky Security Network*. Możesz zakończyć uczestnictwo w Kaspersky Security Network w dowolnym momencie Oświadczenie Kaspersky Security Network opisuje typy danych, które Kaspersky Endpoint Security for Android przesyła do Kaspersky Security Network.

Wymiana informacji z Kaspersky Security Network

W celu udoskonalenia ochrony w czasie rzeczywistym, Kaspersky Security for Mobile wykorzystuje usługę chmury Kaspersky Security Network podczas działania następujących komponentów:

- **Antywirus.** Aplikacja uzyska dostęp do internetowej bazy wiedzy firmy Kaspersky, zawierającej reputację plików i aplikacji. Skanowanie wyszukuje zagrożenia, o których informacje nie zostały jeszcze dodane do antywirusowych baz danych, ale są już dostępne w KSN. Usługa chmury Kaspersky Security Network zapewnia pełne działanie Antywirusa i zmniejsza prawdopodobieństwo fałszywych alarmów.

- **Ochrona WWW.** Aplikacja wykorzystuje dane pobrane z KSN do uruchomienia skanowania stron internetowych przed ich otwarciem. Aplikacja określa także kategorię strony internetowej do kontrolowania dostępu użytkowników do internetu w oparciu o listy dozwolonych i blokowanych kategorii (na przykład, kategoria "Komunikacja przez internet").

- **Kontrola aplikacji.** Aplikacja określa kategorię aplikacji do ograniczenia uruchamiania aplikacji, które nie spełniają firmowych wymagań bezpieczeństwa, w oparciu o listy dozwolonych i blokowanych kategorii (na przykład, kategoria "Gry").

Informacje dotyczące typu danych wysyłanych do Kaspersky podczas korzystania z KSN w trakcie działania Antywirusa i Kontroli aplikacji są dostępne w Umowie licencyjnej. Akceptując warunki i postanowienia Umowy licencyjnej, wyrażasz zgodę na wysyłanie tych informacji.

Informacje o typie danych przesyłanych do Kaspersky podczas korzystania z KSN w trakcie działania Ochrony WWW są dostępne w Oświadczeniu dotyczącym przetwarzania danych w ramach Ochrony WWW. Akceptując warunki i postanowienia Oświadczenia, wyrażasz zgodę na wysyłanie tych informacji.

W celu zidentyfikowania pojawiających się zagrożeń bezpieczeństwa informacji, wniknięcia zagrożeń do systemu, a także zagrożeń trudnych do wykrycia (wraz z ich źródłami), a także zwiększenia ochrony informacji przechowywanych i przetwarzanych na urządzeniu, możesz rozszerzyć swoje uczestnictwo w Kaspersky Security Network.

W celu wymiany danych z KSN w celu udoskonalenia działania aplikacji, muszą być spełnione następujące warunki:

- Ty lub użytkownik urządzenia musicie przeczytać i zaakceptować warunki Oświadczenia Kaspersky Security Network. Jeśli zdecydujesz się na akceptację Oświadczenia przez użytkowników, na ekranie głównym aplikacji zostanie wyświetlona prośba o zaakceptowanie warunków Oświadczenia. Użytkownicy mogą również zaakceptować Oświadczenia w sekcji **Informacje o aplikacji** w ustawieniach Kaspersky Endpoint Security for Android.

  Jeśli zdecydujesz się akceptować wyciągi globalnie, wersje oświadczeń zaakceptowane przez Kaspersky Security Center muszą być zgodne z wersjami już zaakceptowanymi przez użytkowników. W przeciwnym razie użytkownicy zostaną poinformowani o problemie i poproszeni o zaakceptowanie wersji oświadczenia zgodnej z wersją zaakceptowaną globalnie przez administratora. Stan urządzenia we wtyczce Kaspersky Security for Mobile (Devices) również zmieni się na *Ostrzeżenie*.

- Musisz skonfigurować ustawienia zasady grupy, aby zezwolić na wysłanie statystyk do KSN.

Możesz zakończyć wysyłanie danych statystycznych do Kaspersky Security Network w dowolnym momencie. Informacje dotyczące typu danych statystycznych wysyłanych do Kaspersky podczas korzystania z KSN w trakcie działania aplikacji mobilnej Kaspersky Endpoint Security for Android są dostępne w Oświadczeniu Kaspersky Security Network.

Więcej informacji na temat przekazywania danych do KSN można znaleźć w sekcji "Przekazywanie danych".

Podanie danych do KSN jest dobrowolne. Jeśli chcesz, możesz wyłączyć wymianę danych z KSN.

Włączanie i wyłączanie korzystania z Kaspersky Security Network

W celu obsługi komponentów Kaspersky Endpoint Security for Android korzystających z Kaspersky Security Network, aplikacja wysyła żądania do usług w chmurze. Żądania zawierają dane opisane w sekcji "Dostarczanie danych".

Jeśli korzystanie z Kaspersky Security Network jest wyłączone na urządzeniu, komponenty Ochrona w chmurze, Ochrona WWW i Kontrola aplikacji są wyłączone automatycznie.

W celu włączenia lub wyłączenia korzystania z Kaspersky Security Network:

1. Otwórz okno z ustawieniami zasady zarządzania dla urządzeń mobilnych, na którym jest zainstalowany produkt Kaspersky Endpoint Security for Android.
2. W oknie **Właściwości** wybierz sekcję **Dodatkowe**.
3. W sekcji **Ustawienia Kaspersky Security Network (KSN)** skonfiguruj ustawienia korzystania z Kaspersky Security Network:
   - Zaznacz pole wyboru **Używaj Kaspersky Security Network** do działania następujących komponentów: Antywirus (Ochrona w chmurze), Ochrona WWW i Kontrola aplikacji (Kategorie aplikacji).
   - Zaznacz pole **Zezwól na przesyłanie statystyk do KSN**, aby przesłać dane do Kaspersky. Te dane pomogą aplikacji Kaspersky Endpoint Security for Android szybciej reagować na zagrożenia, poprawiać wydajność komponentów ochrony i zmniejszać prawdopodobieństwo fałszywych alarmów.
4. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center. Po zastosowaniu zasady, komponenty, które używają Kaspersky Security Network, zostają wyłączone, a ustawienia komponentów stają się niedostępne.

Używaj Kaspersky Private Security Network

Kaspersky Private Security Network (zwany dalej również *Private KSN* lub *KPSN)* to rozwiązanie, które zapewnia dostęp do baz danych reputacji Kaspersky Security Network, bez wysyłania danych z urządzeń użytkowników do Kaspersky Security Network.

Baza danych reputacji obiektów (plików lub adresów URL) jest przechowywana na serwerze Kaspersky Private Security Network, ale nie na serwerach Kaspersky Security Network. Bazy danych reputacji KPSN są przechowywane w sieci firmowej i zarządzane przez administratora firmy.

Gdy KPSN jest włączony, Kaspersky Endpoint Security nie wysyła żadnych danych statystycznych z urządzeń użytkowników do KSN.

Aby włączyć korzystanie z Private KSN za pośrednictwem Kaspersky Security Center:

1. W oknie głównym Kaspersky Security Center Web Console lub Cloud Console, kliknij **Ustawienia** ( ).

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na karcie **Ogólne** wybierz sekcję **Ustawienia proxy KSN.**

3. Ustaw przełącznik do pozycji **Użyj Kaspersky Private Security Network WŁĄCZONE**.

4. Kliknij przycisk **Wybierz plik z ustawieniami** serwera proxy KSN, a następnie wyszukaj plik konfiguracyjny z rozszerzeniem pkcs7 lub pem (dostarczonym przez Kaspersky).

5. Kliknij **Otwórz**.

6. Jeśli we właściwościach Serwera administracyjnego skonfigurowano ustawienia serwera proxy, ale architektura sieci wymaga bezpośredniego korzystania z prywatnego KSN, włącz opcję **Ignoruj ustawienia serwera proxy KSC podczas łączenia się z Prywatną siecią KSN**. W przeciwnym razie żądania z zarządzanych aplikacji nie mogą dotrzeć do Prywatnej sieci KSN.

7. Kliknij przycisk **Save**.

Po pobraniu ustawień interfejs wyświetla nazwę i kontakty dostawcy, a także datę utworzenia pliku z ustawieniami Prywantej sieci KSN. Ustawienia KPSN są stosowane do urządzeń mobilnych.

Po przełączeniu się na Private KSN, Kontrola aplikacji nie obsługuje kategorii aplikacji dostępnych podczas korzystania z Global KSN. Kategoryzacja aplikacji będzie dostępna, jeśli zdecydujesz się wrócić do KSN.

Dostarczanie danych usługom innych firm

Kaspersky Endpoint Security for Android używa usług Google™ znanych jako Firebase Cloud Messaging, Google Analytics for Firebase™, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics. Kaspersky Endpoint Security for Android używa usługi Firebase Cloud Messaging (FCM) do zapewnienia dostarczenia poleceń na urządzenia mobilne i wymuszonej synchronizacji, gdy ustawienia zasady zostaną zmienione, w odpowiednim czasie. Kaspersky Endpoint Security for Android używa usług Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics do udoskonalenia działania aplikacji i pomocy Kaspersky w przygotowaniu odpowiednich materiałów reklamowych.

Wymiana informacji z Firebase Cloud Messaging

Kaspersky Endpoint Security for Android używa usługi Firebase Cloud Messaging (FCM) do zapewnienia dostarczenia poleceń na urządzenia mobilne i wymuszonej synchronizacji, gdy ustawienia zasady zostaną zmienione, w odpowiednim czasie. Aplikacja używa także powiadomień typu push.

Aby korzystać z usługi Firebase Cloud Messaging, należy skonfigurować ustawienia usługi w Kaspersky Security Center. Więcej informacji na temat Firebase Cloud Messaging w Kaspersky Security Center można znaleźć pod adresem *pomocy Kaspersky Security Center*. Jeśli ustawienia Firebase Cloud Messaging nie zostały skonfigurowane, polecenia na urządzeniu mobilnym i ustawienia zasady zostaną dostarczone po zsynchronizowaniu urządzenia z Kaspersky Security Center zgodnie z terminarzem ustawionym w zasadzie (na przykład, co 24 godziny). Innymi słowy, polecenia i ustawienia zasady zostaną dostarczone z opóźnieniem.

W celu zapewnienia obsługi głównej funkcjonalności produktu, wyrażasz zgodę na automatyczne dostarczenie do usługi Firebase Cloud Messaging unikatowego numeru ID instalacji aplikacji (ID instancji) oraz następujących danych:

- Informacji o zainstalowanym oprogramowaniu: wersji aplikacji, ID aplikacji, wersji kompilacji aplikacji i nazwy pakietu aplikacji.
- Informacji o komputerze, na którym jest zainstalowane oprogramowanie: wersję systemu operacyjnego, ID urządzenia, wersję usług Google.
- Informacji o FCM: ID aplikacji w FCM, ID użytkownika FCM, wersji protokołu.

Dane są przesyłane do usług Firebase poprzez bezpieczne połączenie. Ochrona i dostęp do informacji są regulowane zgodnie z warunkami korzystania z usługi Firebase: https://firebase.google.com/terms/data-processing-terms/, https://firebase.google.com/support/privacy/.

Aby zapobiec wymianie informacji z usługą Firebase Cloud Messaging:

1. W drzewie konsoli wybierz **Zarządzanie urządzeniami mobilnymi** → **Urządzenia mobilne**.
2. Z menu kontekstowego folderu **Urządzenia mobilne** wybierz **Właściwości**.
3. W oknie właściwości folderu **Urządzenia mobilne** wybierz sekcję **Ustawienia Google Firebase Cloud Messaging**.
4. Kliknij przycisk **Resetuj ustawienia**.

Wymiana informacji z Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics

Jeśli korzystasz z wtyczki zarządzającej we wcześniejszej wersji i włączyłeś wymianę danych z usługą Google Analytics, Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3 przeprowadzi wymianę danych z usługą Google Analytics dla Firebase. Obsługa Google Analytics nie jest już kontynuowana.

Kaspersky Security for Mobile wymienia dane z usługami Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics w następujących celach:

- W celu udoskonalenia działania aplikacji.

  W celu wymiany danych z usługami Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics w celu udoskonalenia działania aplikacji, muszą być spełnione następujące warunki:

  - Administrator lub użytkownik urządzenia musi przeczytać i zaakceptować warunki Oświadczenia Kaspersky Security Network. Jeśli zdecydujesz się na akceptację Oświadczenia przez użytkowników, na ekranie głównym aplikacji zostanie wyświetlona prośba o zaakceptowanie warunków Oświadczenia. Użytkownicy mogą również zaakceptować Oświadczenia w sekcji **Informacje o aplikacji** w ustawieniach Kaspersky Endpoint Security for Android.

    Jeśli zdecydujesz się akceptować wyciągi globalnie, wersje oświadczeń zaakceptowane przez Kaspersky Security Center muszą być zgodne z wersjami już zaakceptowanymi przez użytkowników. W przeciwnym razie użytkownicy zostaną poinformowani o problemie i poproszeni o zaakceptowanie wersji oświadczenia zgodnej z wersją zaakceptowaną globalnie przez administratora. Stan urządzenia we wtyczce Kaspersky Security for Mobile (Devices) również zmieni się na *Ostrzeżenie*.

  - Administrator musi skonfigurować ustawienia zasady grupy, aby zezwolić na wysłanie statystyk do KSN (patrz poniżej).

- Aby pomóc Kaspersky w przygotowaniu odpowiednich materiałów reklamowych.

  W celu wymiany danych z usługami Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics w celu pomocy Kaspersky w przygotowaniu odpowiednich materiałów reklamowych, muszą być spełnione następujące warunki:

  - Administrator lub użytkownik urządzenia musi przeczytać i zaakceptować warunki Oświadczenia dotyczącego przetwarzania danych w celach marketingowych. Jeśli zdecydujesz się zaakceptować Oświadczenie, użytkownicy mogą zaakceptować warunki Oświadczenia podczas instalacji aplikacji lub w sekcji **Informacje o aplikacji** w ustawieniach Kaspersky Endpoint Security for Android.

  - Administrator musi skonfigurować ustawienia zasady grupy, aby zezwolić na wysłanie danych do Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics (patrz poniżej).

[Dostarczenie danych do Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics zgodnie z Oświadczeniem dotyczącym przetwarzania danych w celach marketingowych]

Do przetwarzania danych Posiadacz praw używa systemów informacyjnych stron trzecich. Przetwarzanie danych przez strony trzecie podlega zapisom oświadczeń o ochronie prywatności dotyczących takich systemów informacyjnych stron trzecich. Poniżej wskazano usługi używane przez Posiadacza praw oraz przetwarzane w nich dane:

Google Analytics dla Firebase

Podczas korzystania z Oprogramowania następujące dane są automatycznie i regularnie wysyłane do usługi Google Analytics dla Firebase w celu spełnienia zadeklarowanego celu:

- informacje o aplikacji (wersja aplikacji, identyfikator aplikacji i identyfikator aplikacji w usłudze Firebase, identyfikator instancji w usłudze Firebase, nazwa sklepu, w którym zakupiono aplikację, znacznik czasowy pierwszego uruchomienia Oprogramowania)
- ID instalacji aplikacji na urządzeniu i metody instalacji na urządzeniu
- informacja o regionie i wersji językowej
- informacja o rozdzielczości ekranu urządzenia
- informacja o uzyskaniu przez użytkownika dostępu do konta root
- informacje diagnostyczne dotyczące urządzenia, pochodzące z usługi SafetyNet Attestation
- informacja o ustawieniu aplikacji Kaspersky Endpoint Security for Android jako funkcji ułatwień dostępu.
- informacje o przejściach między ekranami aplikacji, czasie trwania sesji, rozpoczęciu i zakończeniu sesji na ekranie, nazwie ekranu
- protokoł używany do przesyłania danych do usługi Firebase, jego wersja oraz ID używanej metody przesyłania danych
- szczegółowe informacje o typie i parametrach zgłaszanego zdarzenia
- informacje o licencji na aplikację, jej dostępności i liczbie urządzeń
- informacje o częstotliwości aktualizacji antywirusowej bazy danych i synchronizacji z Serwerem administracyjnym
- informacje o Konsoli administracyjnej (Kaspersky Security Center lub zewnętrzne systemy EMM)
- Android ID
- identyfikator treści reklamowych.
- informacje dotyczące Użytkownika: kategoria wiekowa i płeć, identyfikator kraju zamieszkania oraz lista zainteresowań
- informacje dotyczące komputera Użytkownika, na którym Oprogramowanie jest zainstalowane: nazwa producenta komputera, typ komputera, model, wersja i wersja językowa systemu operacyjnego, informacje o aplikacji pierwszy raz otwartej w ciągu ostatnich 7 dni oraz o aplikacji pierwszy raz otwartej ponad 7 dni temu

  Do usługi Firebase dane są przekazywane za pośrednictwem bezpiecznego połączenia. Informacje dotyczące sposobu przetwarzania danych w usłudze Firebase są dostępne na stronie internetowej https://firebase.google.com/support/privacy.

Usługa zaświadczania SafetyNet Attestation

Podczas korzystania z Oprogramowania następujące dane będą regularnie przesyłane automatycznie do usługi SafetyNet Attestation w celu realizacji deklarowanego celu:

- Czas kontroli urządzenia
- Informacja o oprogramowaniu, nazwy i dane certyfikatów oprogramowania
- Wyniki kontroli urządzenia
- Losowe kontrole ID w celu weryfikacji wyników kontroli urządzenia

  Do usługi SafetyNet Attestation dane są przekazywane za pośrednictwem bezpiecznego kanału. Informacje dotyczące sposobu przetwarzania danych w usłudze SafetyNet Attestation są dostępne na stronie internetowej: https://policies.google.com/privacy.

Firebase Performance Monitoring

Podczas korzystania z Oprogramowania następujące dane będą regularnie przesyłane automatycznie do usługi Firebase Performance Monitoring w celu realizacji deklarowanego celu:

- unikatowy identyfikator instalacji;
- nazwa pakietu aplikacji;
- wersję zainstalowanego Oprogramowania;
- poziom baterii i stan naładowania baterii;
- operator;
- stan aplikacji na pierwszym planie lub w tle;
- geografia;
- Adres IP
- kod języka urządzenia;
- informacje o połączeniu sieciowym/radiowym;
- pseudonimowy identyfikator instancji Oprogramowania;
- rozmiar dysku i pamięci RAM;
- flaga wskazująca, czy usunięto zabezpieczenia producenta w urządzeniu lub czy urządzenie było rootowane;
- siła sygnału;
- czas trwania automatycznego śledzenia;
- sieć, a także następujące odpowiednie informacje: kod odpowiedzi, rozmiar ładunku w bajtach, czas odpowiedzi
- opis urządzenia.

Do usługi Firebase Performance Monitoring dane są przekazywane za pośrednictwem bezpiecznego połączenia. Informacje dotyczące sposobu przetwarzania danych w usłudze Firebase Performance Monitoring są dostępne na stronie internetowej: https://firebase.google.com/support/privacy.

Crashlytics

Podczas korzystania z Oprogramowania następujące dane będą regularnie przesyłane automatycznie do usługi Crashlytics w celu realizacji deklarowanego celu:

- ID oprogramowania;
- wersję zainstalowanego Oprogramowania;
- flaga wskazująca, czy Oprogramowanie było uruchomione w tle;
- architektura procesora;
- unikatowy identyfikator zdarzenia;
- data i godzina zdarzenia;
- modelu urządzenia;
- całkowity rozmiar dysku oraz przestrzeń aktualnie używana;
- nazwa i wersja systemu operacyjnego;
- całkowity rozmiar pamięci RAM oraz rozmiar aktualnie używany;
- flaga wskazująca, czy urządzenie było rootowane;
- orientacja ekranu w momencie wystąpienia zdarzenia;
- producent produktu/sprzętu;
- unikatowy identyfikator instalacji;
- wersja przesyłanych statystyk;
- typ wyjątku Oprogramowania;
- treść komunikatu o błędzie;
- flaga wskazująca, czy wyjątek Oprogramowania był spowodowany przez zagnieżdżony wyjątek;
- ID wątku;
- flaga wskazująca, czy ramka była przyczyną błędu Oprogramowania;
- flaga wskazująca, czy wątek spowodował niespodziewane zakończenie działania Oprogramowania;
- informacje o sygnale, który spowodował niespodziewane zakończenie działania Oprogramowania: nazwa sygnału, kod sygnału, adres sygnału
- dla każdej ramki skojarzonej z wątkiem, wyjątkiem lub błędem: nazwa pliku ramki, numer wiersza pliku ramki, symbole debugowania, adres i przesunięcie w obrazie binarnym, nazwa wyświetlana biblioteki z ramką, typ

ramki, flaga wskazująca, czy ramka była przyczyną błędu

- identyfikator systemu operacyjnego;
- ID problemu skojarzonego ze zdarzeniem;
- informacje o zdarzeniach, które wystąpiły przed niespodziewanym zakończeniem działania Oprogramowania: identyfikator zdarzenia, data i godzina zdarzenia, typ i wartość zdarzenia
- wartości rejestru procesora;
- typ zdarzenia oraz wartość.

  Dane są przekazywane do usługi Crashlytics za pośrednictwem bezpiecznego kanału. Informacje na temat sposobu przetwarzania danych w usłudze Crashlytics są dostępne pod adresem: https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

Podanie powyższych informacji na potrzeby przetwarzania w celach marketingowych nie jest obowiązkowe.

W celu wyłączenia wymiany danych z usługami Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics:

1. Otwórz okno konfiguracji zasady zarządzania dla urządzeń mobilnych, na których zainstalowana jest aplikacja Kaspersky Endpoint Security for Android.
2. W oknie **Właściwości** wybierz sekcję **Dodatkowe**.
3. W sekcji **Przesyłanie danych** odznacz pole **Zezwól na przesyłanie danych, aby pomóc w udoskonaleniu jakości, wyglądu i działania aplikacji**.
4. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Globalna akceptacja dodatkowych oświadczeń

Aby włączyć ochronę zapewnianą przez Kaspersky Endpoint Security for Android, należy zaakceptować warunki Umowy licencyjnej użytkownika końcowego, a także dodatkowe Oświadczenia (patrz poniżej). Zasady można skonfigurować tak, aby globalnie akceptować wymienione poniżej oświadczenia dla wszystkich użytkowników. Użytkownicy nie zostaną poproszeni o przeczytanie i zaakceptowanie warunków następujących umów i oświadczeń, które zostały już zaakceptowane globalnie:

- Oświadczenie Kaspersky Security Network
- Oświadczenie dotyczące przetwarzania danych na potrzeby modułu Ochrona WWW
- Oświadczenie dotyczące przetwarzania danych w celach marketingowych

Jeśli zdecydujesz się akceptować wyciągi globalnie, wersje oświadczeń zaakceptowane przez Kaspersky Security Center muszą być zgodne z wersjami już zaakceptowanymi przez użytkowników. W przeciwnym razie użytkownicy zostaną poinformowani o problemie i poproszeni o zaakceptowanie wersji oświadczenia zgodnej z wersją zaakceptowaną globalnie przez administratora. Stan urządzenia we wtyczce Kaspersky Security for Mobile (Devices) również zmieni się na *Ostrzeżenie*.

Aby wybrać, czy warunki mają być akceptowane globalnie, czy przez użytkowników, stosując zasady grupy:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Dodatkowe**.
5. W sekcji **Przenoszenie danych** wybierz, czy Oświadczenie dotyczące przetwarzania danych w celach marketingowych będzie akceptowane globalnie czy przez użytkowników.
6. W sekcji **Ustawienia Kaspersky Security Network (KSN)** wybierz, czy Oświadczenie Kaspersky Security Network będzie akceptowane globalnie, czy przez użytkowników.
7. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Użytkownik może zaakceptować warunki Oświadczenia lub je odrzucić w dowolnym momencie w sekcji **Informacje o aplikacji** w ustawieniach Kaspersky Endpoint Security for Android.

Samsung KNOX

Samsung KNOX to rozwiązanie mobilne do konfiguracji i ochrony urządzeń mobilnych Samsung działających pod kontrolą systemu operacyjnego Android. Więcej informacji na temat Samsung KNOX można znaleźć na *stronie pomocy technicznej firmy Samsung*.

Instalacja aplikacji Kaspersky Endpoint Security for Android za pośrednictwem KNOX Mobile Enrollment

Aplikacja KNOX Mobile Enrollment (KME) jest częścią rozwiązania mobilnego Samsung KNOX. Służy do instalacji wsadowej i początkowej konfiguracji aplikacji na nowych urządzeniach Samsung zakupionych od oficjalnych dostawców.

Instalacja aplikacji Kaspersky Endpoint Security for Android za pomocą KNOX Mobile Enrollment składa się z następujących kroków:

1. Tworzenie profilu KNOX MDM za pomocą aplikacji Kaspersky Endpoint Security for Android.
2. Dodawanie urządzeń w KNOX Mobile Enrollment.
3. Instalowanie aplikacji Kaspersky Endpoint Security for Android na urządzeniach mobilnych użytkownika.

Więcej informacji na temat pracy z KNOX Mobile Enrollment można znaleźć w *podręczniku użytkownika KNOX Mobile Enrollment*.

Wdrożenie za pośrednictwem KNOX Mobile Enrollment jest możliwe tylko dla urządzeń Samsung. Listę obsługiwanych urządzeń znajdziesz na *stronie pomocy technicznej firmy Samsung*.

Tworzenie profilu KNOX MDM

Profil *KNOX MDM* to profil zawierający odnośniki do aplikacji umożliwiające ich szybkie zainstalowanie i przeprowadzenie wstępnej konfiguracji na urządzeniach mobilnych.

W celu utworzenia profilu KNOX MDM:

1. Zaloguj się do konsoli Samsung KNOX → **KNOX Mobile Enrollment**.
2. Wybierz sekcję **profili MDM**.
3. Kliknij **Dodaj**.

   Zostanie uruchomiony kreator tworzenia nowego profilu KNOX MDM.
4. W kroku **MDM server connection** wybierz **Server URI is not required for my MDM service** i kliknij **Next**.
5. W kroku **MDM profile info**:

   a. Wprowadź ogólne informacje o profilu KNOX MDM: **nazwę profilu** i **opis**.

   b. Kliknij przycisk **Add MDM apps** i wprowadź ścieżkę do pliku instalacyjnego pakietu APK.

   Plik instalacyjny dla Kaspersky Endpoint Security for Android znajduje się w pakiecie dystrybucyjnym Kaspersky Security for Mobile. Wcześniej umieść plik instalacyjny APK na serwerze WWW Kaspersky Security Center lub na innym serwerze, który jest dostępny do pobrania z urządzenia.

   c. Wprowadź ustawienia połączenia urządzenia z Kaspersky Security Center w polu **danych użytkownika JSON** w następującym formacie:
   `{"serverAddress":"ksc.server.com","serverPort":"12345","groupName":"MOBILE GROUP"}`

   Urządzenie musi być połączone z Kaspersky Security Center, aby aktywować aplikację, skonfigurować urządzenie i wysyłać polecenia.

   d. Zaznacz pole **Add Knox agreements**.

   Aby zainstalować Kaspersky Endpoint Security for Android za pośrednictwem KNOX Mobile Enrollment, użytkownik urządzenia mobilnego musi zaakceptować umowę licencyjną Samsung License Agreement. Warunki umowy licencyjnej Samsung License Agreement są dostępne w sekcji **End User License Agreements, Terms of Service, and User Agreements**. Możesz także dodać inne dokumenty prawne firmy, które są niezbędne do wdrożenia profilu KNOX MDM, klikając przycisk **Add user agreement**.

   e. Odznacz pole **Bind Knox license to this profile**.

   Informacje o licencji Samsung KNOX są dostarczane na urządzenie mobilne wraz z zasadą, gdy urządzenie zostaje zsynchronizowane z Kaspersky Security Center.
6. Kliknij przycisk **Save**.

W rezultacie nowy profil KNOX MDM z aplikacją Kaspersky Endpoint Security for Android zostanie dodany do listy w konsoli KME.

Dodawanie urządzeń do KNOX Mobile Enrollment

Urządzenia można dodawać do konsoli KNOX Mobile Enrollment (KME) w następujący sposób:

- Dostawca automatycznie dodaje urządzenia do konsoli KME po zakupie urządzeń.

  Wybierz tę metodę, jeśli Twoja organizacja współpracuje z oficjalnym dostawcą urządzeń Samsung.

- Administrator instaluje aplikację KNOX Deployment z Google Play na swoim urządzeniu mobilnym i przenosi profil KNOX MDM na urządzenia użytkowników za pośrednictwem Bluetooth lub NFC (Near Field Communication). Po wdrożeniu profilu KNOX MDM urządzenie zostanie automatycznie dodane do konsoli KME.

  Wybierz tę metodę, jeśli urządzenia Samsung nie zostały zakupione od oficjalnego dostawcy.

Dodawanie urządzenia przez dostawcę

Oficjalny sprzedawca urządzeń Samsung jest zarejestrowany w Samsung KNOX. Listę oficjalnych dostawców można znaleźć na *stronie pomocy technicznej firmy Samsung*. Dostawca automatycznie dodaje urządzenia w konsoli KME do konta Samsung natychmiast po zakupie urządzeń. Aby urządzenia zostały dodane przez sprzedawcę, musisz zarejestrować dostawcę w konsoli KME dla swojego konta Samsung. Będziesz potrzebować identyfikatora odsprzedawcy, aby dodać dostawcę urządzeń Samsung w konsoli KME. Aby otrzymać identyfikator odsprzedawcy, musisz wysłać żądanie do dostawcy. W żądaniu podaj swój identyfikator klienta KNOX.

W celu wyświetlenia swojego identyfikatora klienta KNOX:

1. Zaloguj się do konsoli Samsung KNOX → **KNOX Mobile Enrollment**.
2. Wybierz sekcję **Resellers**.
3. Twój identyfikator jest wyświetlany w polu **KNOX client ID**.

Po otrzymaniu odpowiedzi od dostawcy z identyfikatorem odsprzedawcy, zarejestruj dostawcę w konsoli KME. Przed zarejestrowaniem dostawcy można utworzyć profil KNOX MDM, aby profil mógł zostać automatycznie wdrożony podczas dodawania nowych urządzeń.

W celu zarejestrowania oficjalnego dostawcy w konsoli KME:

1. Zaloguj się do konsoli Samsung KNOX → **KNOX Mobile Enrollment**.
2. Wybierz sekcję **Resellers**.
3. Kliknij przycisk **Register reseller**.

   Spowoduje to otwarcie okna rejestracji dostawcy urządzenia.
4. W polu **Reseller ID** wprowadź identyfikator otrzymany od oficjalnego dostawcy urządzeń Samsung.
5. Jeśli utworzyłeś profil KNOX MDM, wybierz profil KNOX MDM w oknie rejestracji dostawcy.

   Po dodaniu nowych urządzeń, profil KNOX MDM jest instalowany automatycznie.
6. Na liście **Preferred download confirmation method** wybierz metodę potwierdzenia dodania urządzenia dla dostawcy.

- **All downloads must be confirmed**. Po dodaniu urządzenia przez sprzedawcę, musisz potwierdzić operację.
- **Automatically confirm all downloads of this reseller**. Urządzenia dostawcy zostaną automatycznie dodane w konsoli KME.

7. Kliknij **OK**.

Dostawca urządzeń Samsung zostanie dodany do listy dostawców w konsoli KME.

Po zakupie nowych urządzeń od oficjalnego dostawcy, aplikacja Kaspersky Endpoint Security for Android zostanie automatycznie zainstalowana na urządzeniach po podłączeniu urządzeń do internetu. Więcej informacji na temat pracy z KNOX Mobile Enrollment można znaleźć w podręczniku *użytkownika KNOX Mobile Enrollment*. Jeśli masz już listę urządzeń w konsoli KME, dodaj profil KNOX MDM z aplikacją KNOX MDM do urządzenia.

W celu dostarczenia profilu KNOX MDM na urządzenia:

1. Zaloguj się do konsoli Samsung KNOX → **KNOX Mobile Enrollment**.
2. Wybierz **Devices** → **All devices**.
3. Wybierz urządzenia, na których chcesz zainstalować profil KNOX MDM.
4. Kliknij przycisk **Configure**.

   Zostanie otwarte okno **Device info**.
5. Na liście **profili MDM** wybierz profil KNOX MDM z aplikacją Kaspersky Endpoint Security for Android.
6. W polu **Tags** wprowadź znaczniki grupowania i etykietowania urządzeń oraz optymalizacji wyszukiwania w konsoli KME.
7. Wprowadź poświadczenia konta użytkownika urządzenia w polach **User ID** i **Password**.

   Dane konta są wymagane do otrzymania ogólnego certyfikatu. Identyfikator użytkownika i hasło muszą być zgodne z poświadczeniami konta użytkownika w Kaspersky Security Center (pełna nazwa i hasło we właściwościach konta użytkownika).
8. Wybierz profil KNOX MDM dla pozostałych urządzeń.
9. Kliknij przycisk **Save**.

Po podłączeniu urządzenia do internetu, użytkownik zostanie poproszony o zainstalowanie profilu KNOX MDM.

Dodawanie urządzenia za pośrednictwem aplikacji do wdrażania KNOX

Jeśli nie kupiłeś urządzenia Samsung od oficjalnego dostawcy, możesz dodać urządzenie do KNOX Mobile Enrollment przez Bluetooth lub NFC. Będzie to wymagało urządzenia mobilnego administratora, które będzie używane do dostarczania profili KNOX MDM na urządzenia mobilne użytkowników.

W celu dodania urządzenia przy użyciu aplikacji KNOX Deployment, muszą być spełnione następujące warunki:

- W zależności od wybranego trybu dostawy, moduły Bluetooth lub NFC muszą być włączone na urządzeniach mobilnych.
- Urządzenie mobilne musi być podłączone do internetu.

W celu dostarczenia profilu KNOX MDM przy użyciu aplikacji KNOX Deployment:

1. Zainstaluj aplikację KNOX Deployment z Google Play na urządzeniu mobilnym administratora.
2. Uruchom aplikację KNOX Deployment.
3. Wprowadź dane uwierzytelniające swojego konta Samsung.
4. W oknie **KNOX Deployment** skonfiguruj ustawienia wdrażania profilu KNOX MDM:
   - Wybierz profil KNOX MDM.
   - Wybierz tryb wdrażania: **Bluetooth** lub **NFC**.

     Korzystając z Bluetooth, możesz dodać profil KNOX MDM do kilku urządzeń naraz.
5. Kliknij **Start deployment**:
   - **Bluetooth**. Na urządzeniu mobilnym użytkownika otwórz witrynę https://configure.samsungknox.com.

     Spowoduje to uruchomienie kreatora rejestracji urządzenia Samsung KNOX Device Registration Wizard. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

     Po zainstalowaniu profilu KNOX MDM, nowe urządzenie ze znacznikiem **Bluetooth** zostanie dodane do konsoli KME.
   - **NFC**. Zbliż urządzenie mobilne administratora do urządzenia mobilnego użytkownika i prześlij profil KNOX MDM.

     Na urządzeniu mobilnym użytkownika pojawi się monit o zainstalowanie profilu KNOX MDM. Nowe urządzenie ze znacznikiem **NFC** zostanie dodane do konsoli KME.

Instalowanie aplikacji

Przed zainstalowaniem aplikacji Kaspersky Endpoint Security for Android należy wydać certyfikat ogólny dla użytkowników urządzeń mobilnych w Konsoli administracyjnej Kaspersky Security Center. Certyfikat ogólny jest wymagany do identyfikacji użytkownika urządzenia mobilnego w Konsoli administracyjnej Kaspersky Security Center.

Po uruchomieniu wdrażania profilu KNOX MDM, plik instalacyjny APK zostanie automatycznie pobrany na urządzenie mobilne. Instalacja aplikacji Kaspersky Endpoint Security for Android jest uruchamiana automatycznie. Użytkownik musi zaakceptować umowę licencyjną Samsung KNOX i umowę licencyjną Kaspersky Endpoint Security for Android. Nie jest wymagana żadna dodatkowa konfiguracja aplikacji. Po zainstalowaniu aplikacji, synchronizacja z Kaspersky Security Center zostanie przeprowadzona automatycznie. Urządzenie mobilne zostanie dodane do Konsoli administracyjnej Kaspersky Security Center do grupy administracyjnej określonej w ustawieniach profilu KNOX MDM (`groupName`).

Konfiguracja kontenerów KNOX

Ta sekcja zawiera informacje dotyczące pracy kontenerów KNOX na urządzeniach Samsung działających pod kontrolą systemu Android.

Używanie kontenerów KNOX jest dostępne tylko na urządzeniach Samsung działających pod kontrolą systemu Android w wersji 6.0 lub nowszej.

Informacje o kontenerach KNOX

Kontener KNOX to bezpieczne środowisko na urządzeniu użytkownika, które posiada swój własny pulpit, panel uruchamiania, aplikacje i widgety. Kontener KNOX umożliwia odizolowanie danych i aplikacji firmowych od danych i aplikacji prywatnych. Kontener KNOX to komponent rozwiązania mobilnego Samsung KNOX.

Samsung KNOX to rozwiązanie mobilne do konfiguracji i ochrony urządzeń mobilnych Samsung działających pod kontrolą systemu operacyjnego Android. Więcej informacji na temat Samsung KNOX można znaleźć na *stronie pomocy technicznej firmy Samsung*.

Kontenery KNOX umożliwiają oddzielenie danych osobistych i firmowych na urządzeniu mobilnym. Na przykład, niemożliwe jest używanie osobistej skrzynki pocztowej do wysyłania pliku, który zlokalizowany jest w kontenerze KNOX. Zalecane jest zainstalowanie kontenera KNOX, jeśli osobiste urządzenia mobilne pracowników są używane do pracy z danymi firmowymi.

Aby używać kontenerów KNOX, należy aktywować Samsung KNOX. Po synchronizacji urządzenia z Kaspersky Security Center, użytkownik urządzenia mobilnego zostanie poproszony o zainstalowanie kontenera KNOX. Przed instalacją kontenera KNOX użytkownik musi zaakceptować warunki Umowy Licencyjnej od firmy Samsung.

Po zainstalowaniu kontenera KNOX, ikona KNOX zostanie dodana do pulpitu urządzenia mobilnego. Lub obszar roboczy zostanie dodany do listy aplikacji na urządzeniu mobilnym. Aby pracować z danymi firmowymi, użytkownik potrzebuje uruchomić aplikację z kontenera KNOX.

Kaspersky Endpoint Security for Android nie jest instalowany w kontenerze KNOX i nie chroni danych firmowych. Kaspersky Endpoint Security for Android nie wykrywa pobierania szkodliwych plików i blokuje szkodliwe strony w kontenerze KNOX. Nie możesz kontrolować uruchamiania aplikacji lub zabronić korzystania z aparatu w kontenerze KNOX. Kaspersky Endpoint Security for Android chroni tylko prywatne dane. Możesz chronić dane firmowe przy użyciu narzędzi Samsung KNOX. Więcej informacji na temat Samsung KNOX można znaleźć na *stronie pomocy technicznej firmy Samsung*.

Aktywowanie Samsung KNOX

Aby użyć kontenera KNOX na urządzeniu mobilnym użytkownika, należy aktywować Samsung KNOX. Procedura aktywacji Samsung KNOX zależy od wersji Kaspersky Endpoint Security for Android zainstalowanej na urządzeniach użytkowników:

- Jeśli na urządzeniach jest zainstalowana bieżąca wersja Kaspersky Endpoint Security for Android, do aktywacji Samsung KNOX nie są potrzebne żadne klucze.
- Jeśli na urządzeniach jest zainstalowana stara wersja Kaspersky Endpoint Security for Android (10.8.3.174 lub starsza), musisz uzyskać klucz KNOX License Manager (zwany dalej kluczem KLM) od firmy Samsung. *Klucz KNOX License Manager* to unikatowy kod, który jest używany przez system licencjonowania Samsung KNOX. Szczegółowe informacje na temat klucza KLM można znaleźć na stronie pomocy technicznej Samsung KNOX.

Korzystanie z kontenerów KNOX jest możliwe tylko na urządzeniach Samsung.

W celu aktywowania Samsung KNOX:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Zarządzaj Samsung KNOX → Kontenery KNOX**.
5. W polu **Klucz KNOX License Manager** określ następujące dane:
   - Jeżeli na urządzeniach jest zainstalowana bieżąca wersja Kaspersky Endpoint Security for Android, wpisz dowolny znak.
   - Jeśli na urządzeniach jest zainstalowana stara wersja Kaspersky Endpoint Security for Android (10.8.3.174 lub wcześniejsza), wprowadź klucz KLM otrzymany od firmy Samsung.
6. Ustaw atrybut Blokada na zablokowaną pozycję  .
7. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Samsung KNOX zostanie aktywowany po następnej synchronizacji z Kaspersky Security Center. Użytkownik zostanie zapytany o akceptację warunków Umowy licencyjnej firmy Samsung i zainstalowanie kontenera KNOX.

W celu dezaktywowania Samsung KNOX:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Zarządzaj Samsung KNOX → Kontenery KNOX**.
5. Wyczyść wartość pola **Klucz KNOX License Manager**.
6. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Samsung KNOX zostanie dezaktywowany po następnej synchronizacji urządzenia z Kaspersky Security Center. Dostęp do kontenera KNOX zostanie zablokowany.

Ograniczenia Samsung KNOX

- Korzystanie z kontenerów KNOX jest dostępne tylko na urządzeniach Samsung.
- Na urządzeniach Samsung obsługujących KNOX 2.6, 2.7 i 2.7.1 Ochrona WWW i Kontrola aplikacji nie działają w kontenerze KNOX. Ten problem jest związany z brakiem wymaganych uprawnień w kontenerze KNOX (usługa

dostępności). Na urządzeniach obsługujących KNOX 2.8 lub nowszy wszystkie składniki aplikacji działają bez ograniczeń.

- Wersje Kaspersky Endpoint Security for Android poprzedzające Service Pack 4 Maintenance Release 3 Update 2 mogą działać niestabilnie na urządzeniach Samsung Android 10 ze względu na aktualizacje Samsung KNOX. Zalecane jest zaktualizowanie Kaspersky Endpoint Security for Android do wersji Service Pack 4 Maintenance Release 3 Update 2.

Konfigurowanie Zapory sieciowej w KNOX

Należy skonfigurować ustawienia Zapory sieciowej do monitorowania połączeń sieciowych w kontenerze KNOX.

W celu skonfigurowania Zapory sieciowej w kontenerze KNOX:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Zarządzaj Samsung KNOX → Kontenery KNOX**.
5. W oknie **Zapora sieciowa** kliknij **Konfiguruj**.

   Zostanie otwarte okno **Zapora sieciowa**.
6. Wybierz tryb Zapory sieciowej:
   - Aby zezwolić na wszystkie połączenia przychodzące i wychodzące, przesuń suwak na **Zezwól na wszystko**.
   - Aby blokować całą aktywność sieciową za wyjątkiem aplikacji na liście wykluczeń, przesuń suwak na **Blokuj wszystkie, za wyjątkiem wykluczonych**.
7. Jeśli ustawiłeś tryb Zapory sieciowej na **Blokuj wszystkie, za wyjątkiem wykluczonych**, utwórz listę wykluczeń:
   a. Kliknij **Dodaj**.

      Zostanie otwarte okno **Wykluczenie dla Zapory sieciowej**.

   b. W polu **Nazwa aplikacji** wprowadź nazwę aplikacji mobilnej.

   c. W polu **Nazwa pakietu** wprowadź nazwę systemową pakietu aplikacji mobilnej (na przykład `com.mobileapp.example`).

   d. Kliknij **OK**.
8. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Konfigurowanie skrzynki pocztowej Exchange w KNOX

Aby pracować z pocztą firmową, kontaktami i kalendarzem w kontenerze KNOX, powinieneś skonfigurować ustawienia skrzynki pocztowej Exchange.

W celu skonfigurowania skrzynki pocztowej Exchange w kontenerze KNOX:

1. W drzewie konsoli, w folderze **Zarządzane urządzenia** wybierz grupę administracyjną, do której należą urządzenia Android.
2. W obszarze roboczym wybierz zakładkę **Zasady**.
3. Otwórz okno właściwości zasady poprzez dwukrotne kliknięcie dowolnej kolumny.
4. W oknie **Właściwości** wybierz sekcję **Zarządzaj Samsung KNOX → Kontenery KNOX**.
5. W oknie **Exchange ActiveSync** kliknij przycisk **Konfiguruj**.

   Zostanie otwarte okno **Ustawienia serwera pocztowego Exchange**.
6. W polu **Adres serwera** wprowadź adres IP lub nazwę DNS serwera, na którym znajduje się serwer pocztowy.
7. W polu **Domena** wprowadź nazwę domeny użytkownika mobilnego w sieci firmowej.
8. Na liście rozwijalnej **Okres synchronizacji** wybierz żądany przedział synchronizacji dla urządzenia mobilnego z serwerem Microsoft Exchange.
9. Aby korzystać z protokołu przesyłania danych SSL (Secure Sockets Layer), zaznacz pole **Użyj połączenia SSL**.
10. Aby korzystać z cyfrowych certyfikatów w celu ochrony transferu danych pomiędzy urządzeniem mobilnym i serwerem Microsft Exchange, zaznacz pole **Weryfikuj certyfikat serwera**.
11. Aby zapisać wprowadzone zmiany, kliknij przycisk **Zastosuj**.

Ustawienia urządzenia mobilnego są konfigurowane po kolejnej synchronizacji urządzenia z Kaspersky Security Center.

Dodatki

Ta sekcja zawiera informacje uzupełniające treść dokumentu.

Uprawnienia do konfigurowania profili grupowych

Administratorzy Kaspersky Security Center mogą konfigurować uprawnienia dostępu użytkowników Konsoli administracyjnej dla różnych funkcji aplikacji w zależności od obowiązków użytkowników.

Dla każdego obszaru działania administrator może przydzielić następujące uprawnienia:

- **Zezwól na modyfikację**. Użytkownik Konsoli administracyjnej może zmieniać ustawienia zasady w oknie właściwości.
- **Blokuj modyfikację**. Użytkownik Konsoli administracyjnej nie może zmieniać ustawień zasady w oknie właściwości. Zakładki zasady należące do zakresu funkcji, dla którego to uprawnienie zostało przydzielone, nie są wyświetlane w interfejsie.

Uprawnienia dostępu do sekcji wtyczki zarządzającej Kaspersky Endpoint Security

Zakres funkcji	Sekcja Zasady
Android Enterprise	Profil roboczy Android
Anti-Theft	Anti-Theft
Kontrola aplikacji	Kontrola aplikacji
Ochrona	Ochrona, Skanowanie, Aktualizacja
Kontrola zgodności	Kontrola zgodności
Kontenery	Kontenery
Ustawienia urządzenia	Kontrola urządzeń, Synchronizacja
Zarządzanie urządzeniami Samsung	APN, Zarządzanie urządzeniami Samsung, Kontenery KNOX
Zarządzanie systemami	Zaawansowane, Wi-Fi
Ochrona WWW	Ochrona WWW

Uprawnienia dostępu do sekcji wtyczki zarządzającej Kaspersky Device Management for iOS

Zakres funkcji	Sekcja Zasady
Dodatkowe	Web clips, Czcionki, AirPlay, AirPrint
Exchange ActiveSync	Ogólne, Hasło, Synchronizacja, Ograniczenia funkcji, Ograniczenia aplikacji
Ogólne	Ogólne, Logowanie jednokrotne, Ochrona WWW, Wi-Fi, Nazwa punktu dostępu (APN), Exchange ActiveSync, E-mail, Niestandardowe obciążenie
LDAP (kalendarz / kontakty)	LDAP, Kalendarz, Kontakty, Subskrypcje kalendarza
Ograniczenia i bezpieczeństwo	Ograniczenia funkcji, Ograniczenia dla aplikacji, Ograniczenia dla multimediów, Hasło, VPN, Globalny serwer pośredniczący HTTP, Certyfikaty, SCEP

Kategorie aplikacji

Kontrola aplikacji obsługuje kategoryzację aplikacji. Tryb działania skonfigurowany dla kategorii aplikacji jest stosowany do wszystkich aplikacji w tej kategorii. Kategoria każdej aplikacji jest określana przez usługę chmury Kaspersky Security Network.

Kategorie aplikacji

Kategoria	Opis
Rozrywka	Aplikacje zapewniające interaktywną rozrywkę.
Komunikatory internetowe, aplikacje mobilne do komunikacji	Aplikacje służące do wymiany wiadomości tekstowych, głosowych i do komunikacji wideo.
Sieci społecznościowe	Aplikacje umożliwiające korzystanie z sieci społecznościowych i blogów.
Oprogramowanie biznesowe	Aplikacje służące do obliczania podatku, zarządzania operacjami bankowymi, zarządzania arkuszami kalkulacyjnymi, związane z księgowością oraz inne aplikacje przeznaczone dla biznesu. Edytory tekstu.

Dom, Rodzina, Styl życia, Zdrowie	Aplikacje oferujące przepisy, wskazówki dotyczące zdrowia i zdrowego odżywiania. Aplikacje przydatne do ćwiczeń, oferujące zapisywanie harmonogramu ćwiczeń, otrzymywanie wskazówek związanych z dietą, składnikami odżywczymi, bezpieczeństwem i zapobieganiem kontuzjom oraz wypadkom.
Tematy medyczne	Aplikacje zawierające katalogi opisujące symptomy i lekarstwa, aplikacje dla specjalistów służby zdrowia, aplikacje oferujące magazyny o zdrowiu oraz nowości.
Multimedia	Usługi filmowych abonamentów, odtwarzaczy muzyki i filmów wideo, musicali. Odtwarzacze i transmisje radiowe.
Oprogramowanie graficzne	Aplikacje współpracujące z aparatem, edytorami graficznymi, aplikacje do zarządzania i publikowania zdjęć.
Wtyczki do odczytywania nowości i kanałów RSS	Aplikacje do czytania gazet, magazynów, blogów oraz agregatory nowości.
Pogodę	Aplikacje wyświetlające prognozy pogody.
Oprogramowanie edukacyjne	Aplikacje do czytania książek, instrukcje, podręczniki, słowniki, słowniki synonimów, encyklopedie. Aplikacje pomagające w nauce, materiały szkoleniowe, słowniki, gry edukacyjne, narzędzia do nauki języków.
Zakupy online	Aplikacje przeznaczone do robienia zakupów internetowych i braniu udziału w aukcjach, karty podarunkowe, narzędzia do porównywania cen, aplikacje do robienia listy zakupów, aplikacje do odczytywania informacji o produktach.
Narzędzia autostartu	Aplikacje przeznaczone do zmiany pulpitu, widżetów, skrótów.
Systemy operacyjne i narzędzia użytkowe	Aplikacje systemowe oferujące zarządzeni systemem operacyjnym, interakcję z użytkownikiem i zarządzanie pamięcią RAM.
Oprogramowanie do obsługi map	Przewodniki po miastach, informacje o lokalnych firmach, narzędzia do planowania wycieczek.
Inne oprogramowanie	Biblioteki oprogramowania, techniczne wersje demo aplikacji. Aplikacje nie uwzględnione w żadnej innej kategorii.
Oprogramowanie transportowe	Aplikacje do korzystania z transportu publicznego, narzędzia nawigacyjne, aplikacje dla kierowców.
Gry	Gry z automatów, Hazardowe, Wyścigi, Inne, Kasynowe, Karcianki, Muzyczne, Planszowe, Tutoriale, Puzzle, Przygodowe, RPG, Symulatory, Gry słowne, Sportowe, Strategie, Gry akcji.
Przeglądarki	Aplikacje do wyświetlania stron internetowych, zawartości plików i dokumentów sieciowych. Aplikacje do zarządzania aplikacjami webowymi.
Narzędzia deweloperskie	Aplikacje przeznaczone do tworzenia oprogramowania. Debuggery, kompilatory, edytory kodów, edytory interfejsów graficznych.
Aplikacje systemu operacyjnego	Aplikacje dostarczone z systemem operacyjnym i wymagane do poprawnego działania systemu operacyjnego.
Oprogramowanie internetowe	Menedżery pobierania, klienty poczty elektronicznej, aplikacje do wyszukiwania w sieci oraz inne aplikacje ułatwiające surfowanie w internecie.
Oprogramowanie infrastruktury sieciowej	Aplikacje do zarządzania serwerami, urządzeniami do przechowywania danych, sprzętem sieciowym, oprogramowaniem w sieci firmowej, automatyzacją i integracją całej infrastruktury.

Oprogramowanie sieciowe	Aplikacje do organizacji współpracy grupy użytkowników na kilku urządzeniach, komunikacji między urządzeniami.
Narzędzia systemowe	Aplikacje dostarczone wraz z systemem operacyjnym: menedżery plików, narzędzia do archiwizacji, narzędzia do diagnostyki sprzętu i oprogramowania, narzędzia optymalizujące pamięć, dezinstalatory, narzędzia do zarządzania procesorem.
Oprogramowanie zabezpieczające	Aplikacje do ochrony danych na urządzeniu. Aplikacje wykrywające i neutralizujące zagrożenia na urządzeniu. Zapory sieciowe. Aplikacje do szyfrowania danych.
Menedżery pobierania	Aplikacje do pobierania plików z zewnętrznych źródeł.
Aplikacje do przechowywania plików w internecie	Aplikacje do zarządzania internetowym magazynem plików, notatek i multimediów.
Oprogramowanie referencyjne	Aplikacje do czytania książek, instrukcje, podręczniki, słowniki, słowniki synonimów, encyklopedie.
Klienty poczty e-mail	Aplikacje używane do wysyłania i odbierania wiadomości e-mail.

Korzystanie z aplikacji Kaspersky Endpoint Security for Android

W tej sekcji Pomocy opisano funkcje i operacje dostępne dla użytkowników aplikacji Kaspersky Endpoint Security for Android.

Artykuły w tej sekcji zawierają wszystkie opcje, które mogą być dostępne lub widoczne na urządzeniu mobilnym. Rzeczywisty układ i zachowanie aplikacji zależy od tego, który system zdalnego zarządzania jest wdrożony oraz od tego, jak administrator konfiguruje urządzenie zgodnie z firmowymi wymogami bezpieczeństwa. Niektóre funkcje i opcje opisane w tej sekcji mogą nie dotyczyć aktualnego wykorzystania aplikacji. Jeśli masz jakieś pytania dotyczące aplikacji na określonym urządzeniu, skontaktuj się z administratorem.

Funkcje aplikacji

Kaspersky Endpoint Security oferuje następujące kluczowe funkcje:

Ochrona przed wirusami i innym szkodliwym oprogramowaniem

Aplikacja używa komponentu Anti-Virus do ochrony urządzenia przed wirusami i innym szkodliwym oprogramowaniem.

Anti-Virus wykonuje następujące funkcje:

- Skanuje całe urządzenie, zainstalowane aplikacje lub wybrane foldery w poszukiwaniu zagrożeń
- Chroni urządzenie w czasie rzeczywistym
- Skanuje nowo zainstalowane aplikacje przed ich pierwszym uruchomieniem
- Aktualizuje antywirusowe bazy danych

Jeśli na urządzeniu mobilnym jest zainstalowana aplikacja, która gromadzi informacje i wysyła je do przetworzenia, Kaspersky Endpoint Security for Android może zaklasyfikować tę aplikację jako szkodliwe oprogramowanie.

Kontrola aplikacji

Zgodnie z firmowymi wymaganiami bezpieczeństwa, *administrator systemu zdalnej administracji* (zwany dalej również "administrator") tworzy listy zalecanych, blokowanych i wymaganych aplikacji. Komponent Kontrola aplikacji jest używany do instalacji zalecanych i wymaganych aplikacji, ich aktualizacji oraz do usuwania zablokowanych aplikacji.

Kontrola aplikacji umożliwia instalację zalecanych i wymaganych aplikacji na urządzeniu poprzez bezpośredni odnośnik do pakietu dystrybucyjnego lub odnośnik do Google Play. Kontrola aplikacji umożliwia usunięcie zablokowanych aplikacji, które naruszają firmowe wymagania bezpieczeństwa.

Kaspersky Endpoint Security musi być ustawiony jako usługa Ułatwień dostępu w celu zapewnienia poprawnego działania Kontroli aplikacji. Jeśli nie włączyłeś tej usługi w Kreatorze wstępnej konfiguracji, możesz włączyć Kaspersky Endpoint Security jako usługę Ułatwień dostępu w sekcji **Stan**, wybierając odpowiedni komunikat, lub w ustawieniach urządzenia (**Ustawienia** → **Ułatwienia dostępu** → **Usługi**).

Ochrona danych na skradzionym lub zagubionym urządzeniu

Komponent Anti-Theft chroni dane użytkownika przed nieautoryzowanym dostępem i pomaga zlokalizować urządzenie w przypadku jego zgubienia lub kradzieży.

Anti-Theft umożliwia zdalne wykonanie następujących czynności:

- Zablokowanie urządzenia.

  Aby uniemożliwić cyberprzestępcy odblokowanie urządzenia, Kaspersky Endpoint Security musi być włączony jako usługa Ułatwień dostępu na urządzeniach działających pod kontrolą systemu Android 7.0 lub nowszego.

- Włącz głośny alarm na urządzeniu nawet wtedy, gdy dźwięk jest wyłączony na urządzeniu.
- Uzyskaj współrzędne urządzenia.
- Usuń dane przechowywane na urządzeniu.
- Przywróć ustawienia fabryczne.
- Potajemnie wykonaj zdjęcie osobie aktualnie korzystającej z urządzenia.

Aby włączyć działania Anti-Theft, Kaspersky Endpoint Security musi być włączony jako administrator urządzenia. Jeśli podczas wstępnej konfiguracji aplikacji nie nadałeś jej uprawnień administratora urządzenia, możesz to zrobić w sekcji **Stan**, wybierając odpowiedni komunikat, lub w ustawieniach urządzenia (**Ustawienia** → **Zabezpieczenia** → **Administratorzy urządzenia**).

Ochrona przed zagrożeniami internetowymi

Moduł Ochrona WWW zapewnia ochronę przed zagrożeniami internetowymi.

Ochrona WWW blokuje szkodliwe strony internetowe rozpowszechniające szkodliwy kod oraz phishingowe strony internetowe, których celem jest kradzież Twoich poufnych danych, a także uzyskanie dostępu do kont finansowych. Ochrona WWW skanuje strony internetowe przed ich otwarciem, korzystając z usługi chmury Kaspersky Security Network.

W celu włączenia Ochrony WWW:

- Kaspersky Endpoint Security musi być włączony jako funkcja dostępności.
- Należy zaakceptować Oświadczenie dotyczące przetwarzania danych na potrzeby modułu Ochrona WWW (Oświadczenie dotyczące modułu Ochrona WWW). Kaspersky Endpoint Security używa Kaspersky Security Network (KSN) do skanowania stron internetowych. Oświadczenie dotyczące modułu Ochrona WWW zawiera warunki dotyczące wymiany danych z KSN.

Twój administrator może zaakceptować Oświadczenie dotyczące modułu Ochrona WWW w Twoim imieniu w Kaspersky Security Center. W tym przypadku nie jest wymagane podjęcie żadnego działania.

Jeśli Twój administrator nie zaakceptował Oświadczenia dotyczącego modułu Ochrona WWW i wysłał Ci prośbę, aby to zrobić, musisz przeczytać i zaakceptować Oświadczenie dotyczące modułu Ochrona WWW w ustawieniach aplikacji.

Jeśli Twój administrator zaakceptował Oświadczenie dotyczące modułu Ochrona WWW, moduł Ochrona WWW nie jest dostępny.

Ochrona WWW na urządzeniach z systemem Android działa tylko w przeglądarkach: Huawei Browser, Google Chrome (włączając funkcję Kart niestandardowych) i Samsung Internet Browser. Ochrona WWW dla przeglądarki Samsung Internet Browser nie blokuje stron na urządzeniu mobilnym, jeśli profil roboczy jest używany, a Ochrona WWW jest włączona tylko dla profilu roboczego.

Okno główne

Wygląd okna głównego różni się nieznacznie przy różnych rozdzielczościach ekranu.

Wygląd okna głównego zmieni się w przypadku problemów, które mogłyby doprowadzić do zmniejszenia poziomu ochrony, infekcji urządzenia lub utraty informacji.

Sekcja **Stan** wyświetla następujące informacje:

- Problemy z ochroną Twojego urządzenia
- Informacje dotyczące spełniania przez urządzenie firmowych wymagań bezpieczeństwa
- Informacje o stanie ochrony urządzenia

Sekcję **Stan** można otworzyć, dotykając górnej części okna głównego Kaspersky Endpoint Security.

Problemy z ochroną urządzenia

Problemy ochrony są pogrupowane według kategorii. Dla każdego problemu wyświetlone są akcje, które mogą zostać użyte do jego rozwiązania.

Sekcja **Stan** wyświetla również listę pominiętych obiektów wykrytych przez aplikację. Lista pominiętych obiektów może ulec zmianie, na przykład, jeśli szkodliwy plik został usunięty lub przeniesiony. Aby uzyskać aktualną listę zagrożeń, uruchom pełne skanowanie urządzenia. Aby zapewnić solidną ochronę danych, wyeliminuj wszystkie wykryte obiekty.

Istnieją dwa rodzaje problemów z ochroną:

- *Ostrzeżenia*. Oznaczone na żółto. Ostrzeżenia informują użytkownika o zdarzeniach, które mogą mieć wpływ na ochronę urządzenia (na przykład: ostatnie skanowanie zostało wykonane ponad 14 dni temu lub nowa aplikacja nie została przeskanowana). Możesz ukryć powiadomienie. Dostęp do informacji o problemie będzie można uzyskać poprzez menu **Ukryte problemy**.
- *Krytyczne*. Oznaczone na czerwono. Problemy krytyczne informują użytkownika o zdarzeniach z krytyczną istotnością dla ochrony urządzenia (na przykład: antywirusowe bazy danych nie były aktualizowane od

dłuższego czasu lub na urządzeniu jest zainstalowana zablokowana aplikacja). Problem krytyczny nie może zostać ukryty.

Kontrola zgodności

Aplikacja automatycznie sprawdzi, czy urządzenie odpowiada firmowym wymaganiom bezpieczeństwa. Informacje na temat spełniania przez urządzenie firmowych wymagań bezpieczeństwa są wyświetlane w sekcji **Stan**.

- Przyczyna niezgodności urządzenia z firmowymi wymaganiami bezpieczeństwa (na przykład, na urządzeniu wykryto zablokowane aplikacje).
- Przedział czasu, w trakcie którego należy wyeliminować te niezgodności (na przykład, 24 godziny).
- Działania, które zostaną podjęte na urządzeniu, jeśli nie usuniesz niezgodności w określonym czasie (na przykład urządzenie zostanie zablokowane).
- Działanie wykonywane w celu wyeliminowania niezgodności urządzenia z firmowymi wymaganiami bezpieczeństwa.

Ikona aplikacji na pasku stanu

Po zakończeniu działania Kreatora, ikona programu Kaspersky Endpoint Security pojawi się na pasku stanu.

Ikona odzwierciedla działanie aplikacji i zapewnia dostęp do jej okna głównego.

Ikona sygnalizuje działanie Kaspersky Endpoint Security i odzwierciedla stan ochrony urządzenia:

– Urządzenie jest chronione.

– Istnieją problemy z ochroną (na przykład antywirusowe bazy danych są przestarzałe lub nowo zainstalowana aplikacja nie została przeskanowana).

Skanowanie urządzenia

Antywirus posiada kilka ograniczeń:

- Jeśli Antywirus jest uruchomiony, zagrożenie wykryte w pamięci zewnętrznej urządzenia (takie jak karta SD) nie może zostać zneutralizowane automatycznie w profilu roboczym (Aplikacje z ikoną teczki, Konfigurowanie profilu roboczego Android). Kaspersky Endpoint Security for Android nie ma dostępu do pamięci zewnętrznej w profilu roboczym. Informacje o wykrytych obiektach są wyświetlane w sekcji **Stan** aplikacji. Aby zneutralizować obiekty wykryte w pamięci zewnętrznej, pliki obiektów muszą zostać usunięte ręcznie, a skanowanie urządzenia musi zostać uruchomione ponownie.
- Ze względu na ograniczenia techniczne, Kaspersky Endpoint Security for Android nie może skanować plików o rozmiarze 2 GB lub większym. Podczas skanowania aplikacja pomija takie pliki bez informowania o tym fakcie.

W celu uruchomienia skanowania urządzenia:

1. Na panelu szybkiego uruchamiania w oknie głównym Kaspersky Endpoint Security dotknij **Skanowanie**.
2. Wybierz obszar skanowania urządzenia:
   - **Skanuj całe urządzenie**. Aplikacja skanuje cały system plików urządzenia.

- **Skanuj zainstalowane aplikacje**. Aplikacja skanuje tylko zainstalowane aplikacje.
- **Skanowanie obiektów**. Aplikacja skanuje wybrany folder lub pojedynczy plik. Możesz wybrać pojedynczy obiekt (folder lub plik) lub jedną z następujących partycji pamięci urządzenia:
  - **Pamięć urządzenia**. Pamięć całego urządzenia przeznaczona do odczytu. Dotyczy to także partycji pamięci systemowej, w której przechowywane są pliki systemu operacyjnego.
  - **Pamięć wewnętrzna**. Partycja pamięci urządzenia przeznaczona do instalowania aplikacji i przechowywania multimediów, dokumentów i innych plików.
  - **Pamięć zewnętrzna**. Zewnętrzna karta pamięci SD. Jeśli nie ma zewnętrznej karty SD, ta opcja będzie ukryta.

Dostęp do ustawień skanowania antywirusowego może być ograniczony przez Twojego administratora.

Aby skonfigurować skanowanie w poszukiwaniu wirusów:

1. Na panelu szybkiego uruchamiania w oknie głównym Kaspersky Endpoint Security dotknij → **Ustawienia** → **Antywirus** → **Skanowanie**.
2. Jeśli chcesz, żeby podczas skanowania aplikacja wykrywała adware oraz aplikacje, które mogły zostać użyte przez hakerów do uszkodzenia urządzenia lub danych, przełącz przycisk przełącznika **Adware, auto-dialery i inne**.
3. Kliknij **Akcja po wykryciu zagrożenia**, a następnie wybierz akcję, jaką aplikacja wykona domyślnie:
   - **Kwarantanna**

     Kwarantanna przechowuje pliki w archiwum, więc nie mogą one uszkodzić urządzenia. Kwarantanna umożliwia usunięcie lub przywrócenie plików, które zostały przeniesione do odizolowanego magazynu.
   - **Pytaj o akcję**

     Aplikacja prosi użytkownika o wybranie akcji dla każdego wykrytego obiektu: pomiń, poddaj kwarantannie lub usuń. Po wykryciu wielu obiektów, możesz zastosować wybraną akcję do wszystkich obiektów.
   - **Usuń**

     Wykryte obiekty zostaną automatycznie usunięte. Nie są wymagane żadne dodatkowe działania. Przed usunięciem obiektu, Kaspersky Endpoint Security wyświetli tymczasowe powiadomienie o wykryciu obiektu.
   - **Pomiń**

     Jeśli wykryte obiekty zostaną pominięte, Kaspersky Endpoint Security ostrzeże użytkownika o problemach z ochroną urządzenia. Informacja na temat pominiętych obiektów jest wyświetlana w sekcji aplikacji **Stan**. Dla każdego pominiętego zagrożenia, aplikacja udostępnia działania, które użytkownik może wykonać w celu eliminacji zagrożenia. Lista pominiętych obiektów może ulec zmianie, na przykład, jeśli szkodliwy plik został usunięty lub przeniesiony. Aby uzyskać aktualną listę zagrożeń, uruchom pełne skanowanie urządzenia. Aby zapewnić solidną ochronę danych, wyeliminuj wszystkie wykryte obiekty.

Informacje o wykrytych zagrożeniach i podjętych działaniach są rejestrowane w raportach aplikacji (→ **Raporty**). Można wybrać wyświetlanie raportów dotyczących działań Antywirusa.

Uruchamianie zaplanowanego skanowania

Antywirus posiada kilka ograniczeń:

- Jeśli Antywirus jest uruchomiony, zagrożenie wykryte w pamięci zewnętrznej urządzenia (takie jak karta SD) nie może zostać zneutralizowane automatycznie w profilu roboczym (Aplikacje z ikoną teczki, Konfigurowanie profilu roboczego Android). Kaspersky Endpoint Security for Android nie ma dostępu do pamięci zewnętrznej w profilu roboczym. Informacje o wykrytych obiektach są wyświetlane w sekcji **Stan** aplikacji. Aby zneutralizować obiekty wykryte w pamięci zewnętrznej, pliki obiektów muszą zostać usunięte ręcznie, a skanowanie urządzenia musi zostać uruchomione ponownie.

- Ze względu na ograniczenia techniczne, Kaspersky Endpoint Security for Android nie może skanować plików o rozmiarze 2 GB lub większym. Podczas skanowania aplikacja pomija takie pliki bez informowania o tym fakcie.

W celu skonfigurowania terminarza pełnego skanowania urządzenia:

1. Na panelu szybkiego uruchamiania w oknie głównym Kaspersky Endpoint Security dotknij → **Ustawienia** → **Antywirus** → **Skanowanie**.

2. Dotknij **Terminarz**, a następnie wybierz częstotliwość pełnego skanowania:

   - **Co tydzień**
   - **Codziennie**
   - **Wyłączono**
   - **Po aktualizacji baz danych**

3. Kliknij **Dzień uruchomienia**, a następnie wybierz dzień tygodnia, w który chcesz uruchamiać pełne skanowanie.

4. Kliknij **Czas uruchomienia**, a następnie określ czas uruchomienia pełnego skanowania.

Pełne skanowanie urządzenia jest uruchamiane zgodnie z terminarzem.

W systemie Android 12 lub nowszych aplikacja może wykonać to zadanie później niż określono, jeśli urządzenie jest w trybie oszczędzania baterii.

Zmienianie trybu ochrony

Ochrona w czasie rzeczywistym umożliwia wykrywanie zagrożeń w otwieranych plikach oraz skanowanie aplikacji podczas ich instalowania na urządzeniu w czasie rzeczywistym. Antywirusowe bazy danych oraz usługa chmury Kaspersky Security Network (Ochrona w chmurze) są używane do automatycznego zapewnienia ochrony.

W celu zmiany trybu ochrony urządzenia:

1. Na panelu szybkiego uruchamiania w oknie głównym Kaspersky Endpoint Security dotknij → **Ustawienia** → **Antywirus** → **Tryb ochrony w czasie rzeczywistym**.

2. Wybierz tryb ochrony urządzenia:

   - **Wyłączono**. Ochrona jest wyłączona.

- **Zalecana**. Program skanuje tylko zainstalowane aplikacje oraz pliki z folderu Pobrane. Program skanuje nowe aplikacje natychmiast po ich zainstalowaniu.

- **Rozszerzona**. Antywirus skanuje wszystkie pliki urządzenia na obecność szkodliwych obiektów, gdy wykonywana jest na nich jakakolwiek akcja (na przykład, gdy są zapisywane, przenoszone lub modyfikowane). Program skanuje także nowe aplikacje natychmiast po ich zainstalowaniu.

Informacje o bieżącym trybie ochrony są wyświetlane pod opisem komponentu.

Dostęp do ustawień ochrony w czasie rzeczywistym może być ograniczony przez Twojego administratora.

W celu włączenia Ochrony w chmurze (KSN):

1. Na panelu szybkiego uruchamiania w oknie głównym Kaspersky Endpoint Security dotknij → **Ustawienia** **Antywirus**.

2. Przełącz przycisk przełącznika **Ochrona w chmurze (KSN)**.

   Przycisk przełącznika **Ochrona w chmurze (KSN)** zarządza używaniem Kaspersky Security Network tylko dla ochrony urządzenia w czasie rzeczywistym. Jeśli pole jest odznaczone, Kaspersky Endpoint Security dalej używa KSN do działania innych komponentów aplikacji.

W wyniku tego aplikacja uzyska dostęp do internetowej bazy wiedzy firmy Kaspersky, zawierającej reputację plików i aplikacji. Skanowanie wyszukuje zagrożenia, o których informacje nie zostały jeszcze dodane do antywirusowych baz danych, ale są już dostępne w KSN. Usługa chmury Kaspersky Security Network zapewnia pełne działanie Antywirusa i zmniejsza prawdopodobieństwo fałszywych alarmów. Tylko Twój administrator może w pełni wyłączyć korzystanie z Kaspersky Security Network.

W celu skonfigurowania ochrony w czasie rzeczywistym:

1. Na panelu szybkiego uruchamiania w oknie głównym Kaspersky Endpoint Security dotknij → **Ustawienia** → **Antywirus** → **Tryb ochrony w czasie rzeczywistym**.

2. Jeśli chcesz, żeby podczas skanowania aplikacja wykrywała adware oraz aplikacje, które mogły zostać użyte przez hakerów do uszkodzenia urządzenia lub danych, przełącz przycisk przełącznika **Adware, auto-dialery i inne**.

3. Kliknij **Akcja po wykryciu zagrożenia**, a następnie wybierz akcję, jaką aplikacja wykona domyślnie:

   - **Kwarantanna**

     Kwarantanna przechowuje pliki w archiwum, więc nie mogą one uszkodzić urządzenia. Kwarantanna umożliwia usunięcie lub przywrócenie plików, które zostały przeniesione do odizolowanego magazynu.

   - **Usuń**

     Wykryte obiekty zostaną automatycznie usunięte. Nie są wymagane żadne dodatkowe działania. Przed usunięciem obiektu, Kaspersky Endpoint Security wyświetli tymczasowe powiadomienie o wykryciu obiektu.

   - **Pomiń**

     Jeśli wykryte obiekty zostaną pominięte, Kaspersky Endpoint Security ostrzeże użytkownika o problemach z ochroną urządzenia. Informacja na temat pominiętych obiektów jest wyświetlana w sekcji aplikacji **Stan**. Dla każdego pominiętego zagrożenia, aplikacja udostępnia działania, które użytkownik może wykonać w celu eliminacji zagrożenia. Lista pominiętych obiektów może ulec zmianie, na przykład, jeśli szkodliwy plik został usunięty lub przeniesiony. Aby uzyskać aktualną listę zagrożeń, uruchom pełne skanowanie urządzenia. Aby zapewnić solidną ochronę danych, wyeliminuj wszystkie wykryte obiekty.

Informacje o wykrytych zagrożeniach i podjętych działaniach są rejestrowane w raportach aplikacji (→ **Ustawienia** → **Raporty**). Można wybrać wyświetlanie raportów dotyczących działań Antywirusa.

Aktualizowanie antywirusowych baz danych

W celu zaktualizowania antywirusowych baz danych aplikacji:

Na panelu szybkiego uruchamiania w oknie głównym Kaspersky Endpoint Security dotknij **Aktualizacja baz danych**.

Zaplanowane aktualizacje baz danych

Aplikacja może automatycznie aktualizować antywirusowe bazy danych zgodnie z określonym terminarzem.

W celu skonfigurowania terminarza aktualizacji:

1. Na panelu szybkiego uruchamiania w oknie głównym Kaspersky Endpoint Security dotknij → **Ustawienia** → **Antywirus** → **Aktualizacja baz danych**.
2. Kliknij **Terminarz**, a następnie wybierz częstotliwość aktualizacji:
   - **Co tydzień**
   - **Codziennie**
   - **Wyłączono**
3. Kliknij **Dzień uruchomienia**, a następnie wybierz dzień tygodnia, w który chcesz uruchamiać aktualizację.
4. Kliknij **Czas uruchomienia**, a następnie określ czas uruchomienia aktualizacji.

Aktualizacje antywirusowych baz danych są uruchamiane zgodnie z terminarzem.

W systemie Android 12 lub nowszych aplikacja może wykonać to zadanie później niż określono, jeśli urządzenie jest w trybie oszczędzania baterii.

Czynności, jakie należy wykonać w przypadku zgubienia lub kradzieży urządzenia

Jeśli urządzenie zostanie zgubione lub skradzione, skontaktuj się z administratorem systemu. Administrator może zdalnie wykonać polecenia Anti-Theft na urządzeniu użytkownika zgodnie z firmowymi wymaganiami bezpieczeństwa.

Jeśli do urządzenia zostanie wysłane polecenie pełnego resetu, kontrola nad urządzeniem zostanie utracona, a pozostałe polecenia modułu Anti-Theft nie będą działać.

Ochrona WWW

W celu włączenia Ochrony WWW:

- Kaspersky Endpoint Security musi być włączony jako funkcja dostępności.
- Należy zaakceptować Oświadczenie dotyczące przetwarzania danych na potrzeby modułu Ochrona WWW (Oświadczenie dotyczące modułu Ochrona WWW). Kaspersky Endpoint Security używa Kaspersky Security Network (KSN) do skanowania stron internetowych. Oświadczenie dotyczące modułu Ochrona WWW zawiera warunki dotyczące wymiany danych z KSN.

  Twój administrator może zaakceptować Oświadczenie dotyczące modułu Ochrona WWW w Twoim imieniu w Kaspersky Security Center. W tym przypadku nie jest wymagane podjęcie żadnego działania.

  Jeśli Twój administrator nie zaakceptował Oświadczenia dotyczącego modułu Ochrona WWW i wysłał Ci prośbę, aby to zrobić, musisz przeczytać i zaakceptować Oświadczenie dotyczące modułu Ochrona WWW w ustawieniach aplikacji.

  Jeśli Twój administrator zaakceptował Oświadczenie dotyczące modułu Ochrona WWW, moduł Ochrona WWW nie jest dostępny.

Ochrona WWW na urządzeniach z systemem Android działa tylko w przeglądarkach: Huawei Browser, Google Chrome (włączając funkcję Kart niestandardowych) i Samsung Internet Browser. Ochrona WWW dla przeglądarki Samsung Internet Browser nie blokuje stron na urządzeniu mobilnym, jeśli profil roboczy jest używany, a Ochrona WWW jest włączona tylko dla profilu roboczego.

Aby używać Ochrony WWW przez cały czas surfowania w internecie, ustaw Google Chrome lub Samsung Internet Browser jako domyślną przeglądarkę.

W celu ustawienia obsługiwanej przeglądarki jako domyślnej przeglądarki i użycia Ochrony WWW do skanowania stron internetowych przez cały czas:

1. Na panelu szybkiego uruchamiania w oknie głównym Kaspersky Endpoint Security dotknij → **Ustawienia** → **Ochrona WWW**.
2. Włącz **Ochrona WWW** za pomocą przełącznika.
3. Kliknij **Ustaw domyślną przeglądarkę**.

   Ten przycisk jest wyświetlany, gdy włączona jest ochrona WWW, a obsługiwana przeglądarka nie została ustawiona jako przeglądarka domyślna.

   Zostanie uruchomiony Kreator wyboru domyślnej przeglądarki.
4. Postępuj zgodnie z instrukcjami Kreatora.

Kreator ustawi Google Chrome, Huawei Browser lub Samsung Internet Browser jako domyślną przeglądarkę. Ochrona WWW nieprzerwanie skanuje strony internetowe podczas surfowania w internecie.

Kontrola aplikacji

Kontrola aplikacji sprawdza, czy aplikacje zainstalowane na urządzeniu mobilnym odpowiadają firmowym wymaganiom bezpieczeństwa. W Kaspersky Security Center administrator tworzy listy dozwolonych, blokowanych, obowiązkowych i zalecanych aplikacji zgodnie z firmowymi wymaganiami bezpieczeństwa. W wyniki pracy Kontroli aplikacji program Kaspersky Endpoint Security wyświetli pytanie o zainstalowanie obowiązkowych i zalecanych aplikacji i o usunięcie blokowanych aplikacji. Nie możesz uruchomić blokowanych aplikacji na swoim urządzeniu mobilnym.

W celu zainstalowania obowiązkowych i zalecanych aplikacji lub usunięcia blokowanych aplikacji:

1. Przejdź do sekcji **Stan** programu Kaspersky Endpoint Security.
2. Wybierz zadania Kontroli aplikacji.
3. Wykonaj zalecane działania.

Uzyskiwanie certyfikatu

W celu uzyskania certyfikatu dostępu do zasobów sieciowych firmy:

1. Na panelu szybkiego uruchamiania w oknie głównym Kaspersky Endpoint Security dotknij → **Ustawienia** → **Dodatkowe** → **Uzyskaj certyfikat**.
2. Określ dane uwierzytelniające konta sieci firmowej.
3. Jeśli otrzymałeś od administratora hasło jednorazowe, zaznacz pole **Hasło jednorazowe** i wprowadź otrzymane hasło.

   Zostanie uruchomiony Kreator instalacji certyfikatu.
4. Postępuj zgodnie z jego poleceniami.

Synchronizacja z Kaspersky Security Center

Synchronizacja urządzenia mobilnego z systemem zdalnej administracji Kaspersky Security Center jest wymagana do ochrony i konfiguracji urządzenia zgodnie z firmowymi wymaganiami bezpieczeństwa. Urządzenie jest automatycznie synchronizowane z Kaspersky Security Center. Użytkownik może także ręcznie uruchomić synchronizację. Po pierwszej synchronizacji urządzenie zostaje dodane do listy urządzeń mobilnych zarządzanych poprzez Kaspersky Security Center. Administrator może skonfigurować urządzenie zgodnie z firmowymi wymaganiami bezpieczeństwa.

Możesz skonfigurować ustawienia synchronizacji podczas działania Kreatora wstępnej konfiguracji lub w ustawieniach Kaspersky Endpoint Security. Ustawienia synchronizacji należy skonfigurować, jeśli aplikacja Kaspersky Endpoint Security została zainstalowana przy użyciu Google Play. Zapytaj administratora systemu o wartości, jakie należy określić w ustawieniach synchronizacji.

Zmodyfikuj ustawienia synchronizacji urządzenia z systemem zdalnej administracji Kaspersky Security Center tylko wtedy, gdy poprosi o to administrator.

W celu zsynchronizowania urządzenia z Kaspersky Security Center:

1. Na panelu szybkiego uruchamiania w oknie głównym Kaspersky Endpoint Security dotknij → **Ustawienia** → **Synchronizacja**.
2. W sekcji **Ustawienia synchronizacji** określ wartości następujących ustawień:
   - **Serwer**
   - **Port**
   - **Grupa**
   - **Firmowy adres e-mail**

   Administrator może ukryć ustawienia synchronizacji.
3. Dotknij **Synchronizuj**.

Aktywacja Kaspersky Endpoint Security for Android bez użycia Kaspersky Security Center

W większości przypadków aplikacja Kaspersky Endpoint Security for Android zainstalowana na Twoim urządzeniu jest aktywowana przez administratora centralnie w systemie zdalnej administracji Kaspersky Security Center. Jeśli Twoje urządzenie nie jest połączone z Kaspersky Security Center, możesz ręcznie wpisać kod aktywacyjny. Aby uzyskać kod aktywacyjny, skontaktuj się z administratorem.

Aktywuj aplikację ręcznie tylko na polecenie administratora.

W celu wpisania kodu aktywacyjnego:

1. W komunikacie o błędzie informującym, że Twoja licencja wkrótce utraci ważność lub utraciła ważność, a Twoje urządzenie nie jest połączone z Serwerem administracyjnym, wybierz **Aktywuj**.
2. W oknie aktywacji wpisz kod aktywacyjny otrzymany od administratora, a następnie wybierz **Aktywuj**.
3. Jeśli kod aktywacyjny jest poprawny, zostanie wyświetlone powiadomienie informujące, że aplikacja została aktywowana wraz z datą wygaśnięcia licencji.

Aplikacja Kaspersky Endpoint Security for Android na Twoim urządzeniu zostanie aktywowana.

Aktualizowanie aplikacji

Kaspersky Endpoint Security można zaktualizować w następujące sposoby:

- Ręcznie przez Google Play. Możesz pobrać najnowszą wersję aplikacji ze sklepu Google Play i zainstalować ją na swoim urządzeniu.
- Z pomocą administratora. Administrator może zdalnie zaktualizować wersję aplikacji na Twoim urządzeniu przy pomocy systemu do zdalnej administracji Kaspersky Security Center.

Aktualizowanie aplikacji z poziomu Google Play

Administrator może zablokować użytkownikowi możliwość aktualizacji aplikacji z poziomu Google Play.

Aplikacja może zostać zaktualizowana z poziomu Google Play zgodnie ze standardową procedurą aktualizacji platformy Android. Aby aplikacja została zaktualizowana, należy spełnić następujące warunki:

- Należy posiadać konto Google.
- Urządzenie musi być podpięte do konta Google.
- Urządzenie musi być podłączone do internetu.

Więcej informacji o tworzeniu konta Google, podpinaniu urządzenia do konta oraz korzystaniu ze sklepu Google Play znajdziesz na stronie pomocy technicznej Google.

Aktualizowanie aplikacji poprzez Kaspersky Security Center

Aktualizowanie aplikacji przy pomocy Kaspersky Security Center obejmuje następujące kroki:

1. Administrator wysyła na urządzenie mobilne użytkownika pakiet dystrybucyjny aplikacji, którego wersja spełnia firmowe wymagania bezpieczeństwa.

   Zostanie wyświetlony monit o zainstalowanie Kaspersky Endpoint Security na Twoim urządzeniu.

2. Zaakceptuj warunki i postanowienia aktualizacji.

   Nowe wersja aplikacji zostanie zainstalowana na urządzeniu. Aplikacja nie wymaga dodatkowej konfiguracji po aktualizacji.

Dezinstalowanie aplikacji

Administrator może zablokować użytkownikowi możliwość usunięcia aplikacji. W takiej sytuacji nie będziesz mógł usunąć Kaspersky Endpoint Security.

Kaspersky Endpoint Security można usunąć przy użyciu następujących metod:

- Ręcznie w ustawieniach aplikacji.
- Ręcznie w ustawieniach urządzenia.
- Z pomocą administratora. Administrator może zdalnie usunąć aplikację z Twojego urządzenia przy pomocy systemu do zdalnej administracji Kaspersky Security Center.

Dezinstalacja z poziomu ustawień aplikacji

W celu usunięcia Kaspersky Endpoint Security z urządzenia:

1. Na panelu szybkiego uruchamiania w oknie głównym Kaspersky Endpoint Security dotknij → **Odinstaluj aplikację**.

   Zostanie uruchomiony Kreator dezinstalacji aplikacji.

2. Postępuj zgodnie z jego poleceniami.

Dezinstalacja z poziomu ustawień urządzenia

Aplikacja jest usuwana zgodnie ze standardową procedurą platformy Android. Aby usunąć aplikację, w ustawieniach zabezpieczeń urządzenia należy wyłączyć uprawnienia administratora dla Kaspersky Endpoint Security.

Na urządzeniach działających pod kontrolą systemu Android 7.0 lub nowszego, jeśli administrator zablokował możliwość dezinstalacji, urządzenie zostanie zablokowane, gdy zostanie podjęta próba usunięcia aplikacji z poziomu ustawień systemu Android. Aby odblokować urządzenie, skontaktuj się ze swoim administratorem.

Dezinstalacja poprzez Kaspersky Security Center

Odinstalowanie aplikacji przy pomocy Kaspersky Security Center obejmuje następujące kroki:

1. Administrator wysyła polecenie odinstalowania aplikacji na urządzenie mobilne użytkownika.

   Twoje urządzenie mobilne wyświetla monit o potwierdzenie usunięcia Kaspersky Endpoint Security.

2. Potwierdź dezinstalację aplikacji.

   Aplikacja zostanie usunięta z urządzenia.

Aplikacje z ikoną teczki

Ikona aplikacji w profilu roboczym Android

Aplikacje oznaczone ikoną teczki (aplikacje korporacyjne) są przechowywane na urządzeniu w profilu roboczym Android (zwany dalej również "profil roboczy"). *Profil roboczy Android* to bezpieczne środowisko na urządzeniu, w którym administrator może zarządzać aplikacjami i kontami bez ograniczenia możliwości pracy z danymi osobowymi.

Profil roboczy umożliwia przechowywanie danych firmowych oddzielnie od danych osobowych. Zapewnia to bezpieczne przechowywanie danych firmowych i chroni je przed szkodliwym oprogramowaniem. Po utworzeniu profilu roboczego na urządzeniu, automatycznie instalowane są w profilu roboczym następujące aplikacje: Sklep Google Play, Google Chrome, Pobrane, Kaspersky Endpoint Security for Android i inne.

Aplikacja KNOX

Ikona KNOX

Aplikacja KNOX otwiera kontener KNOX na urządzeniu. *Kontener KNOX* to bezpieczne środowisko na urządzeniu, które posiada swój własny pulpit, panel uruchamiania, aplikacje i widgety. Administrator może zarządzać aplikacjami i kontami w kontenerze KNOX bez ograniczania użytkownikowi możliwości pracy z danymi osobowymi.

Kontener KNOX umożliwia przechowywanie danych firmowych oddzielnie od danych osobowych. Zapewnia to bezpieczne przechowywanie danych firmowych i chroni je przed szkodliwym oprogramowaniem.

W kontenerze KNOX możesz mieć dostęp do firmowej skrzynki pocztowej, informacji kontaktowych pracowników firmy, repozytorium plików i innych aplikacji.

Więcej informacji o pracy z KNOX można znaleźć na *stronie pomocy technicznej firmy Samsung*.

Korzystanie z aplikacji Kaspersky Security for iOS

W tej sekcji Pomocy opisano funkcje i operacje dostępne dla użytkowników aplikacji Kaspersky Security for iOS.

Artykuły w tej sekcji zawierają wszystkie opcje, które mogą być dostępne lub widoczne na urządzeniu mobilnym. Rzeczywisty układ i zachowanie aplikacji zależy od tego, który system zdalnego zarządzania jest wdrożony oraz od tego, jak administrator konfiguruje urządzenie zgodnie z firmowymi wymogami bezpieczeństwa. Niektóre funkcje i opcje opisane w tej sekcji mogą nie dotyczyć aktualnego wykorzystania aplikacji. Jeśli masz jakieś pytania dotyczące aplikacji na określonym urządzeniu, skontaktuj się z administratorem.

Funkcje aplikacji

Kaspersky Security for iOS oferuje następujące kluczowe funkcje.

Ochrona przed zagrożeniami internetowymi

Moduł Ochrona WWW zapewnia ochronę przed zagrożeniami internetowymi.

Ochrona WWW blokuje szkodliwe strony internetowe rozpowszechniające szkodliwy kod oraz phishingowe strony internetowe, których celem jest kradzież Twoich poufnych danych, a także uzyskanie dostępu do kont finansowych. Ochrona WWW skanuje strony internetowe przed ich otwarciem, korzystając z usługi chmury Kaspersky Security Network. Ochrona WWW sprawdza również działania w Internecie aplikacji na Twoim urządzeniu.

Aby aplikacja Ochrona WWW mogła działać, musisz dodać ją do konfiguracji sieci VPN.

Wykrywanie zdjęcia zabezpieczeń systemu

Gdy aplikacja Kaspersky Security for iOS wykryje zdjęcie zabezpieczeń systemu, wyśle komunikat o znaczeniu krytycznym i poinformuje administratora o problemie.

Aplikacja nie może zagwarantować bezpieczeństwa urządzenia, bo zdjęcie zabezpieczeń omija funkcje bezpieczeństwa i może powodować wiele problemów, m.in.:

- Luki w zabezpieczeniach
- Problemy ze stabilnością
- Zakłócenia usług Apple
- Potencjalne awarie i zawieszanie się
- Krótszy czas pracy baterii
- Przeszkody w instalacji aktualizacji systemu iOS

Instalowanie aplikacji

W celu instalacji aplikacji Kaspersky Security for iOS:

1. Znajdź wiadomość e-mail od administratora zawierającą zaproszenie do instalacji aplikacji Kaspersky Security for iOS ze sklepu App Store.
2. Możesz przejść do sklepu App Store na jeden z następujących sposobów:
   - Dotknij łącza w wiadomości, jeśli czytasz ją na urządzeniu z systemem iOS, na którym chcesz zainstalować aplikację.
   - Zeskanuj kod QR za pomocą urządzenia z systemem iOS, na którym chcesz zainstalować aplikację, jeśli czytasz wiadomość na komputerze.

   Łącze z zaproszeniem jest ważne przez 24 godziny. Jeśli nie zdążysz zainstalować aplikacji na czas, skontaktuj się z administratorem, aby otrzymać nowe zaproszenie.
3. Pobierz i zainstaluj aplikację ze sklepu App Store, zgodnie ze standardową procedurą instalacji na platformie iOS.

Aplikacja Kaspersky Security for iOS zostanie zainstalowana na Twoim urządzeniu. Aby chronić urządzenie, aktywuj aplikację.

Aktywowanie aplikacji

W celu aktywowania aplikacji Kaspersky Security for iOS:

1. Uruchom aplikację na urządzeniu.
2. Zaakceptuj umowy i oświadczenia, zaznaczając pola wyboru **Umowa licencyjna** i **Polityka prywatności dla produktów i usług**.

   Możesz opcjonalnie zaakceptować **Oświadczenie w sprawie usługi Kaspersky Security Network**, aby zezwolić na wysyłanie statystyk do sieci Kaspersky Security Network. Poprawia to wydajność aplikacji i zapewnia jej nieprzerwane działanie.
3. Dotknij **Dalej**. Aplikacja połączy się ze zdalnym systemem administracyjnym Kaspersky Security Center i uzyska informacje o licencji.
4. Zezwól aplikacji na dodanie konfiguracji VPN. Aplikacja używa konfiguracji VPN do wykrywania phishingu w witrynach i ochrony urządzenia przed złośliwym oprogramowaniem.
5. Zezwól aplikacji na wysyłanie powiadomień typu push. Aplikacja korzysta z powiadomień, aby informować Cię o problemach z bezpieczeństwem i statusie Twojej licencji.

Aplikacja Kaspersky Security for iOS na Twoim urządzeniu jest aktywowana.

Aktywacja aplikacji za pomocą kodu aktywacyjnego

Kiedy instalujesz aplikację Kaspersky Security for iOS na urządzeniu, aplikacja łączy się ze zdalnym systemem administracyjnym Kaspersky Security Center i automatycznie uzyskuje informacje o licencji. Jeśli Twoje urządzenie nie jest połączone z Kaspersky Security Center, możesz ręcznie wpisać kod aktywacyjny. Aby uzyskać kod aktywacyjny, skontaktuj się z administratorem.

Aktywuj aplikację ręcznie tylko na polecenie administratora.

W celu wpisania kodu aktywacyjnego:

1. W komunikacie informującym, że aplikacja nie jest aktywna, dotknij opcji **Aktywuj aplikację**.
2. W oknie aktywacji wpisz kod aktywacyjny otrzymany od administratora, a następnie wybierz **Aktywuj**.

   Jeśli kod aktywacyjny jest poprawny, zostanie wyświetlone powiadomienie informujące, że aplikacja została aktywowana wraz z datą wygaśnięcia licencji.

Aplikacja Kaspersky Security for iOS na Twoim urządzeniu jest aktywowana.

Okno główne

Wygląd okna głównego różni się nieznacznie przy różnych rozdzielczościach ekranu.

Główne okno wyświetla:

- Ogólny stan ochrony Twojego urządzenia.
- Komunikaty pokazujące status składników aplikacji i problemy z ochroną.

Istnieją trzy rodzaje wiadomości:

- Oznaczone na zielono. Komunikaty statusu informujące, że ochrona danego obszaru jest aktywna.
- Oznaczone na żółto. Komunikaty informacyjne informujące o zdarzeniach, które mogą mieć wpływ na bezpieczeństwo urządzenia.
- Oznaczone na czerwono. Komunikaty krytyczne informujące o zdarzeniach o krytycznym znaczeniu dla bezpieczeństwa urządzenia.

Możesz dotknąć komunikatu, aby uzyskać szczegółowe informacje.

Aktualizowanie aplikacji

Możesz pobrać najnowszą wersję aplikacji Kaspersky Security for iOS ze sklepu App Store i zainstalować ją na urządzeniu za pomocą standardowej procedury aktualizacji na platformie iOS. Możesz także włączyć automatyczne aktualizacje. Aplikacja nie wymaga dodatkowej konfiguracji po aktualizacji.

Aby aplikacja została zaktualizowana, należy spełnić następujące warunki:

- Wymagane jest konto Apple ID.
- Urządzenie musi być podpięte do konta Apple ID.

- Urządzenie musi być podłączone do internetu.

Więcej informacji o tworzeniu identyfikatora Apple ID, łączeniu z nim urządzenia lub korzystaniu ze sklepu App Store można znaleźć w witrynie pomocy Apple.

Dezinstalowanie aplikacji

Aby usunąć aplikację Kaspersky Security for iOS, wykonaj standardową procedurę na platformie iOS:

1. Na ekranie głównym dotknij i przytrzymaj ikonę aplikacji.
2. Odinstaluj aplikację.

Aplikacja Kaspersky Security for iOS zostanie usunięta z Twojego urządzenia.

Licencjonowanie aplikacji

Ta sekcja zawiera informacje o ogólnych warunkach związanych z licencjonowaniem Kaspersky Security for Mobile.

Informacje o Umowie licencyjnej

Umowa licencyjna to wiążąca umowa prawna zawierana pomiędzy Tobą a firmą AO Kaspersky Lab, która określa zasady i warunki korzystania z Kaspersky Security for Mobile.

Przed rozpoczęciem korzystania z Kaspersky Security for Mobile należy dokładnie przeczytać warunki i zasady Umowy licencyjnej.

Warunki i zasady Umowy licencyjnej można przejrzeć w następujące sposoby:

- Podczas instalacji komponentów Kaspersky Security for Mobile.
- Poprzez odcytanie pliku license.txt zawartego w automatycznie wyodrębnianych archiwum zestawu dystrybucyjnego do instalowania aplikacji Kaspersky Endpoint Security for Android.
- W sekcji **Informacje o aplikacji** w Kaspersky Endpoint Security for Android.
- W sekcji **Informacje o aplikacji** → **Umowy i oświadczenia** w Kaspersky Security for iOS.
- W sekcji **Zaawansowane** → **Zaakceptowane Umowy licencyjne** właściwości Serwera administracyjnego. Ta funkcja jest dostępna w Kaspersky Security Center w wersji 12 i nowszej.

Potwierdzenie akceptacji treści Umowy licencyjnej podczas instalacji komponentów Kaspersky Security for Mobile jest równoznaczne z akceptacją warunków i zasad tejże umowy. Jeśli nie zaakceptujesz warunków Umowy licencyjnej, musisz anulować instalację komponentów Kaspersky Security for Mobile i zrezygnować z korzystania z nich.

Informacje o licencji

Licencja to czasowo ograniczone prawo do korzystania z zintegrowanego rozwiązania Kaspersky Security for Mobile zgodnie z warunkami Umowy licencyjnej.

Bieżąca licencja upoważnia do korzystania z następujących usług:

- Korzystania z aplikacji na urządzeniach mobilnych zgodnie z warunkami Umowy licencyjnej.
- Uzyskiwania pomocy technicznej.

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 Kaspersky Security for Mobile.

Okres ważności licencji testowej wynosi 30 dni. Po wygaśnięciu licencji testowej aplikacja mobilna Kaspersky Endpoint Security for Android oraz Kaspersky Security for iOS przestaje wykonywać większość swoich funkcji poza synchronizacją z Serwerem administracyjnym. Aby kontynuować korzystanie z aplikacji, musisz zakupić licencję komercyjną.

- *Komercyjna*.

  Licencja dostarczana przy zakupie Kaspersky Security for Mobile.

  Po wygaśnięciu licencji komercyjnej aplikacja mobilna nadal działa, ale z ograniczoną funkcjonalnością.

  W trybue ograniczonej funkcjonalności dostępne są następujące komponenty w zależności od aplikacji.

  - Aplikacja Kaspersky Endpoint Security for Android:

    - **Anti-Virus**. Ochrona w czasie rzeczywistym i skanowanie antywirusowe urządzenia są dostępne, ale aktualizacje antywirusowych baz danych nie są dostępne.
    - **Anti-Theft**. Dostępne jest tylko wysyłanie poleceń na urządzenie mobilne.
    - **Synchronizacja z Serwerem administracyjnym**.

    Kaspersky Endpoint Security for Android przestaje wymieniać informacje z Kaspersky Security Network, Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring i Crashlytics, jeśli klucz Kaspersky jest zablokowany, gdy licencja testowa wygaśnie lub jeśli brakuje licencji (kod aktywacyjny został usunięty z zasady grupy).

  - Aplikacja Kaspersky Security for iOS:

    - **Synchronizacja z Serwerem administracyjnym**.

    Kaspersky Security for iOS przestanie wymieniać informacje z Kaspersky Security Network, jeśli licencja próbna wygaśnie lub jeśli jej nie ma (kod aktywacyjny zostanie usunięty z zasady grupy).

  Pozostałe składniki aplikacji mobilnej nie są dostępne dla użytkownika urządzenia. Administrator może używać zasad grupy do zarządzania tymi komponentami w trybie ograniczonej funkcjonalności. Nie można używać zasad grupy do konfigurowania innych składników aplikacji.

  Aby kontynuować korzystanie z aplikacji w trybie pełnej funkcjonalności, musisz odnowić licencję komercyjną. Zalecamy odnowienie okresu licencjonowania lub zakupienie nowej licencji przed wygaśnięciem bieżącej licencji, aby zapewnić maksymalną ochronę komputera przed wszystkimi zagrożeniami bezpieczeństwa.

Informacje o subskrypcji

Subskrypcja dla Kaspersky Security for Mobile oznacza zamówienie aplikacji mobilnej z wybranymi parametrami (data wygaśnięcia subskrypcji, liczba chronionych urządzeń mobilnych). Możesz zamówić subskrypcję dla Kaspersky Security for Mobile 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 Security for Mobile działał po wygaśnięciu ograniczonej subskrypcji, należy ją odnowić. Nieograniczona subskrypcja jest odnawiana automatycznie, pod warunkiem, że przedpłata została dokonana na czas.

W przypadku ograniczonej subskrypcji, w momencie jej wygaśnięcia może zostać zaoferowany okres karencji dla odnowienia subskrypcji, w trakcie którego aplikacje zachowają swoją funkcjonalność. Dostępność i czas trwania okresu karencji są definiowane przez dostawcę usługi.

Aby używać Kaspersky Security for Mobile z subskrypcją, należy użyć kodu aktywacyjnego otrzymanego od dostawcy usługi. Po wprowadzeniu kodu aktywacyjnego, klucz jest instalowany dla licencji w celu korzystania z aplikacji z subskrypcją.

Możliwe opcje zarządzania subskrypcją mogą różnić się w zależności od dostawcy usługi. Dostawca usługi może nie zaoferować okresu karencji na odnowienie subskrypcji, w trakcie którego aplikacje zachowują swoją funkcjonalność.

Kody aktywacyjne zakupione dla subskrypcji nie mogą zostać użyte do aktywowania wcześniejszych wersji Kaspersky Security for Mobile.

Informacje o kluczu

Klucz jest to sekwencja bitów, które możesz zastosować w celu aktywacji, a następnie używania zintegrowanego rozwiązania Kaspersky Security for Mobile zgodnie z warunkami Umowy licencyjnej. Klucze są generowane przez specjalistów z Kaspersky.

Klucz dla aplikacji mobilnej można dodać za pomocą pliku klucza lub kodu aktywacyjnego:

- Jeśli w organizacji jest wdrożony pakiet Kaspersky Security Center, należy zastosować plik klucza i rozesłać go do aplikacji mobilnych z systemem Android. Klucz będzie wyświetlany w interfejsie Kaspersky Security Center i w interfejsie aplikacji mobilnej na Androida jako unikatowa sekwencja alfanumeryczna.

  Po dodaniu kluczy można je zastąpić innymi kluczami.

  Nie możesz aktywować aplikacji Kaspersky Security for iOS bez pliku z kluczem.

- Jeśli Twoja organizacja nie używa Kaspersky Security Center, musisz udostępnić kod aktywacyjny użytkownikowi. Użytkownik wprowadza kod aktywacyjny w aplikacji mobilnej na system Android lub iOS. Klucz wyświetlany jest w interfejsie aplikacji mobilnej jako unikalna sekwencja alfanumeryczna.

Klucz może zostać zablokowany przez Kaspersky, jeśli, na przykład, warunki Umowy licencyjnej zostaną naruszone. Jeśli klucz zostanie zablokowany, aplikacja mobilna przestaje wykonywać wszystkie swoje funkcje poza synchronizacją z Serwerem administracyjnym. Aby kontynuować korzystanie z aplikacji, musisz zakupić inny klucz.

Informacje o kodzie aktywacyjnym

Kod aktywacyjny to unikatowa sekwencja 20 znaków alfanumerycznych. Możesz wprowadzić kod aktywacyjny, aby dodać klucz, który spowoduje aktywację aplikacji mobilnej Kaspersky Endpoint Security for Android lub Kaspersky Security for iOS. Kod aktywacyjny otrzymasz na adres e-mail, który określiłeś podczas składania zamówienia, po zakupieniu zintegrowanego rozwiązania Kaspersky Security for Mobile lub po zamówieniu wersji testowej Kaspersky Security for Mobile.

Aby aktywować aplikację mobilną kodem aktywacyjnym, potrzebny jest dostęp do internetu w celu nawiązania połączenia z serwerami aktywacji Kaspersky.

Jeśli zgubiłeś swój kod aktywacyjny po aktywowaniu aplikacji, będziesz mógł go odzyskać. Kod aktywacyjny może być potrzebny, na przykład, do rejestracji w Kaspersky CompanyAccount. Aby przywrócić kod aktywacyjny, należy skontaktować się z działem pomocy technicznej Kaspersky.

Informacje o pliku klucza

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

Nie możesz aktywować aplikacji Kaspersky Security for iOS bez pliku z kluczem.

Plik klucza otrzymasz na adres e-mail, który określono podczas składania zamówienia, po zakupieniu zintegrowanego rozwiązania Kaspersky Security for Mobile lub po zamówieniu wersji testowej Kaspersky Security for Mobile.

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 Kaspersky CompanyAccount.

W celu odzyskania pliku klucza:

- Skontaktuj się ze sprzedawcą licencji.
- Uzyskaj plik klucza poprzez stronę internetową Kaspersky, korzystając ze swojego kodu aktywacyjnego.

Zapewnianie danych w Kaspersky Endpoint Security for Android

Produkt Kaspersky Security for Mobile jest zgodny z wymaganiami Rozporządzenia o Ochronie Danych Osobowych (GDPR - General Data Protection Regulation).

Aby zainstalować aplikację, Ty lub użytkownik urządzenia musicie przeczytać i zaakceptować warunki Umowy licencyjnej użytkownika końcowego. Ponadto można skonfigurować zasady, aby akceptować wymienione poniżej Oświadczenia globalnie dla wszystkich użytkowników. W przeciwnym razie użytkownicy zostaną poproszeni przez powiadomienie na głównym ekranie aplikacji o zaakceptowaniu następujących Oświadczeń dotyczących przetwarzania danych osobowych użytkownika:

- Oświadczenie Kaspersky Security Network
- Oświadczenie dotyczące przetwarzania danych na potrzeby modułu Ochrona WWW
- Oświadczenie dotyczące przetwarzania danych w celach marketingowych

Jeśli zdecydujesz się akceptować wyciągi globalnie, wersje oświadczeń zaakceptowane przez Kaspersky Security Center muszą być zgodne z wersjami już zaakceptowanymi przez użytkowników. W przeciwnym razie użytkownicy zostaną poinformowani o problemie i poproszeni o zaakceptowanie wersji oświadczenia zgodnej z wersją zaakceptowaną globalnie przez administratora. Stan urządzenia we wtyczce Kaspersky Security for Mobile (Devices) również zmieni się na *Ostrzeżenie*.

Użytkownik może zaakceptować warunki Oświadczenia lub je odrzucić w dowolnym momencie w sekcji **Informacje o aplikacji** w ustawieniach Kaspersky Endpoint Security for Android.

Wymiana informacji z Kaspersky Security Network

W celu udoskonalenia ochrony w czasie rzeczywistym, Kaspersky Endpoint Security for Android wykorzystuje usługę chmury Kaspersky Security Network podczas działania następujących komponentów:

- **Anti-Virus.** Aplikacja uzyska dostęp do internetowej bazy wiedzy firmy Kaspersky, zawierającej reputację plików i aplikacji. Skanowanie wyszukuje zagrożenia, o których informacje nie zostały jeszcze dodane do antywirusowych baz danych, ale są już dostępne w KSN. Usługa chmury Kaspersky Security Network zapewnia pełne działanie Antywirusa i zmniejsza prawdopodobieństwo fałszywych alarmów.

- **Ochrona WWW.** Aplikacja wykorzystuje dane pobrane z KSN do skanowania stron internetowych przed ich otwarciem. Aplikacja określa także kategorię strony internetowej do kontrolowania dostępu użytkowników do internetu w oparciu o listy dozwolonych i blokowanych kategorii (na przykład, kategoria "Komunikacja przez internet").

- **Kontrola aplikacji.** Aplikacja określa kategorię aplikacji do ograniczenia uruchamiania aplikacji, które nie spełniają firmowych wymagań bezpieczeństwa, w oparciu o listy dozwolonych i blokowanych kategorii (na przykład, kategoria "Gry").

Informacje dotyczące typu danych wysyłanych do Kaspersky podczas korzystania z KSN w trakcie działania Antywirusa i Kontroli aplikacji są dostępne w Umowie licencyjnej. Akceptując warunki i postanowienia Umowy licencyjnej, wyrażasz zgodę na wysyłanie tych informacji.

Informacje o typie danych przesyłanych do Kaspersky podczas korzystania z KSN w trakcie działania Ochrony WWW są dostępne w Oświadczeniu dotyczącym przetwarzania danych w ramach Ochrony WWW. Akceptując warunki i postanowienia Oświadczenia, wyrażasz zgodę na wysyłanie tych informacji.

Informacje dotyczące typu danych statystycznych wysyłanych do Kaspersky podczas korzystania z KSN w trakcie działania aplikacji mobilnej Kaspersky Endpoint Security for Android są dostępne w Oświadczeniu Kaspersky Security Network. Akceptując warunki i postanowienia Oświadczenia, wyrażasz zgodę na wysyłanie tych informacji.

Dostarczanie danych zgodnie z Umową licencyjną

Jeżeli do aktywacji Oprogramowania jest używany Kod aktywacyjny, w celu weryfikacji uprawnionego wykorzystania Oprogramowania, Użytkownik końcowy wyraża zgodę na okresowe przekazywanie Posiadaczowi praw następujących informacji:

- format danych w żądaniu wysłanym do infrastruktury Posiadacza praw; adres iPv4 usługi sieciowej, do którego uzyskiwano dostęp; rozmiar zawartości żądania wysłanego do infrastruktury Posiadacza praw; ID protokołu; kod aktywacyjny oprogramowania; typ kompresji danych; ID oprogramowania; zestaw identyfikatorów Oprogramowania, które może być aktywowane na urządzeniu użytkownika; wersja językowa Oprogramowania; pełna wersja Oprogramowania; unikatowy identyfikator urządzenia; data i godzina na urządzeniu użytkownika; ID instalacji Oprogramowania (PCID); wersję systemu operacyjnego, numer wersji systemu operacyjnego, numer aktualizacji systemu operacyjnego, wydanie systemu operacyjnego, rozszerzone informacje o wydaniu systemu operacyjnego; model urządzenia; rodzinę systemu operacyjnego; format danych w żądaniu wysłanym do infrastruktury Posiadacza praw; typ sumy kontrolnej przetwarzanego obiektu; nagłówek licencji Oprogramowania; ID regionalnego centrum aktywacji; dat i godzina utworzenia klucza licencyjnego Oprogramowania; identyfikator licencji Oprogramowania; ID modelu informacji użytego do dostarczenia licencji dla Oprogramowania; data i godzina wygaśnięcia licencji dla Oprogramowania; bieżący stan klucza licencyjnego Oprogramowania; typ użytej licencji dla Oprogramowania; typ licencji użytej do aktywowania Oprogramowania; identyfikator Oprogramowania pochodzący z licencji;

W celu ochrony Komputera przed zagrożeniami dla bezpieczeństwa informacji Użytkownik końcowy zobowiązuje się do okresowego dostarczania Posiadaczowi praw następujących informacji:

- typ sumy kontrolnej przetwarzanego obiektu; suma kontrolna przetwarzanego obiektu; identyfikator komponentu Oprogramowania;
- identyfikator wyzwolonego wpisu w antywirusowych bazach danych Oprogramowania; znacznik czasu wyzwolonego wpisu w antywirusowych bazach danych Oprogramowania; typ wyzwolonego wpisu w antywirusowych bazach danych Oprogramowania; nazwa wykrytego szkodliwego programu lub legalnego oprogramowania, które może zostać użyte do uszkodzenia urządzenia lub danych użytkownika;
- nazwa sklepu, z którego zainstalowano aplikację; nazwa pakietu aplikacji; klucz publiczny wykorzystywany do podpisywania pliku APK; suma kontrolna certyfikatu wykorzystywanego do podpisywania pliku APK; znacznik czasu certyfikatu cyfrowego;
- pełna wersja Oprogramowania; ID aktualizacji Oprogramowania; typ zainstalowanego Oprogramowania; identyfikator konfiguracji; wynik działania Oprogramowania; kod błędu;
- numery, które są wydzielone z pliku APK aplikacji dla systemu Android zgodnie z pewnymi regułami matematycznymi i które nie pozwalają na przywrócenie zawartości oryginalnego pliku; te dane nie zawierają nazw plików, ścieżek do plików, adresów, numerów telefonów lub innych informacji osobowych użytkowników.

Jeżeli Użytkownik wykorzystuje serwery aktualizacji Posiadacza praw do pobrania Aktualizacji, Użytkownik końcowy w celu zwiększenia wydajności procedury wyraża zgodę na okresowe dostarczanie Posiadaczowi praw następujących informacji

- identyfikator Oprogramowania pochodzący z licencji; pełna wersja Oprogramowania; identyfikator licencji Oprogramowania; typ użytej licencji dla Oprogramowania; ID instalacji Oprogramowania (PCID); ID uruchomienia aktualizacji Oprogramowania; przetwarzany adres internetowy.

Posiadacz praw może użyć takich informacji także do otrzymywania statystycznych informacji o dystrybucji i użyciu Oprogramowania.

Uzyskane informacje są chronione przez Kaspersky zgodnie z wymogami wynikającymi z przepisów prawa. Uzyskane informacje są przechowywane w postaci zaszyfrowanej i są niszczone w miarę ich gromadzenia (dwa razy do roku) lub na żądanie Użytkownika. Ogólne statystyki są przechowywane cały czas.

Dostarczenia danych zgodnie z Oświadczeniem Kaspersky Security Network

Korzystanie z KSN może prowadzić do zwiększania skuteczności ochrony przed zagrożeniami dla bezpieczeństwa sieci i informacji, którą to ochronę zapewnia Oprogramowanie.

Jeśli używasz licencji na 5 lub więcej węzłów, Posiadacz praw automatycznie otrzyma i przetworzy następujące dane podczas korzystania z KSN:

- identyfikator wyzwolonego wpisu w antywirusowych bazach danych Oprogramowania; znacznik czasu wyzwolonego wpisu w antywirusowych bazach danych Oprogramowania; typ wyzwolonego wpisu w antywirusowych bazach danych Oprogramowania; data i godzina publikacji baz danych Oprogramowania; wersję systemu operacyjnego, numer wersji systemu operacyjnego, numer aktualizacji systemu operacyjnego, wydanie systemu operacyjnego, rozszerzone informacje o wydaniu systemu operacyjnego; wersja pakietu Service Pack dla systemu operacyjnego; charakterystyka wykrycia; suma kontrolna (MD5) przetwarzanego obiektu; nazwa przetwarzanego obiektu; flaga wskazująca, czy przetwarzany obiekt to plik PE; suma kontrolna (MD5) maski, która zablokowała usługę sieciową; sumę kontrolną (SHA256) przetwarzanego obiektu; rozmiar przetwarzanego obiektu; kod typu obiektów; decyzja Oprogramowania odnośnie przetwarzanego obiektu; ścieżka do przetwarzanego obiektu; kod katalogu; wersja komponentu Oprogramowania; wersja przesyłanych statystyk; ostatnio używany adres usługi sieciowej (URL, IP); typ klienta użytego do uzyskania dostępu do usługi sieciowej;

adres iPv4 usługi sieciowej, do którego uzyskiwano dostęp; adres iPv6 usługi sieciowej, do którego uzyskiwano dostęp; adres internetowy źródła żądania usługi sieciowej (odnośnik); przetwarzany adres internetowy;

- informacje o przeskanowanych obiektach (wersja aplikacji z AndroidManifest.xml; decyzja Oprogramowania odnośnie aplikacji; metoda użyta do uzyskania decyzji Oprogramowania odnośnie aplikacji; nazwa pakietu instalatora w sklepie; nazwa pakietu (lub nazwa zestawu danych) z pliku AndroidManifest.xml; kategoria Google SafetyNet; flaga wskazująca, czy SafetyNet jest włączony na urządzeniu; wartość SHA256 z odpowiedzi Google SafetyNet; APK Signature Scheme dla certyfikatu APK; kod wersji zainstalowanego Oprogramowania; numer seryjny certyfikatu wykorzystywanego do podpisywania pliku APK; nazwa instalowanego pliku APK; ścieżka do instalowanego pliku APK; wystawca certyfikatu wykorzystywanego do podpisywania pliku APK; klucz publiczny wykorzystywany do podpisywania pliku APK; suma kontrolna certyfikatu wykorzystywanego do podpisywania pliku APK; data i godzina wygaśnięcia certyfikatu; data i godzina wydania certyfikatu; wersja przesyłanych statystyk; algorytm wyliczania odcisku palca certyfikatu cyfrowego; Suma kontrolna MD5 zainstalowanego pliku APK; Suma kontrolna MD5 pliku DEX znajdującego się w pliku APK; zgody udzielane aplikacji w sposób dynamiczny; wersja oprogramowania innej firmy; flaga wskazująca, że aplikacja jest domyślnym komunikatorem SMS; flaga wskazująca, że aplikacja posiada uprawnienia Administratora urządzenia; flaga wskazująca, że aplikacja znajduje się w katalogu systemowym; flaga wskazująca, że aplikacja używa usług dostępności);

- informacje o wszystkich potencjalnie złośliwych obiektach i działaniach (fragment zawartości przetwarzanego obiektu); data i godzina wygaśnięcia certyfikatu; data i godzina wydania certyfikatu; identyfikator klucza z magazynu kluczy, użytego do szyfrowania; protokół użyty do wymiany danych z KSN; kolejność fragmentu w przetwarzanym obiekcie; dane wewnętrznego raportu, wygenerowanego przez moduł Oprogramowania antywirusowego dla przetwarzanego obiektu; nazwa wydawcy certyfikatu; klucz publiczny certyfikatu; algorytm obliczenia klucza publicznego certyfikatu; numer seryjny certyfikatu; data i godzina podpisania obiektu; ustawienia i nazwa właściciela certyfikatu; odcisk palca certyfikatu cyfrowego przeskanowanego obiektu i algorytm funkcji skrótu; data i godzina ostatniej modyfikacji przetwarzanego obiektu; data i godzina utworzenia przetwarzanego obiektu; przetwarzane obiekty lub ich części; opis przetwarzanego obiektu w sposób zdefiniowany we właściwościach obiektu; format przetwarzanego obiektu; typ sumy kontrolnej przetwarzanego obiektu; suma kontrolna (MD5) przetwarzanego obiektu; nazwa przetwarzanego obiektu; sumę kontrolną (SHA256) przetwarzanego obiektu; rozmiar przetwarzanego obiektu; nazwa producenta Oprogramowania; decyzja Oprogramowania odnośnie przetwarzanego obiektu; wersja przetwarzanego obiektu; źródło decyzji podjętej w stosunku do przetwarzanego obiektu; suma kontrolna przetwarzanego obiektu; nazwa aplikacji nadrzędnej; ścieżka do przetwarzanego obiektu; informacje o wyniku sprawdzania podpisu pliku; klucz sesji logowania; algorytm szyfrowania klucza sesji logowania; czas przechowywania przetwarzanego obiektu; algorytm wyliczania odcisku palca certyfikatu cyfrowego);

- typ kompilacji, na przykład, "user" lub "eng"; pełna nazwa produktu; producent produktu/sprzętu; czy dozwolona jest instalacja aplikacji spoza Google Play; stan usługi chmury w celu weryfikacji aplikacji Google; stan usługi chmury w celu weryfikacji aplikacji Google instalowanych za pośrednictwem standardu ADB; bieżąca nazwa kodowa lub "REL" opracowywania dla kompilacji produkcyjnej; numer kompilacji przyrostowej; ciąg znaków wersji widoczny dla użytkownika; nazwa urządzenia użytkownika; identyfikator kompilacji Oprogramowania widoczny dla użytkownika; odcisk cyfrowy oprogramowania układowego; identyfikator oprogramowania układowego; flaga wskazująca, czy urządzenie było rootowane; system operacyjny; nazwa oprogramowania; typ użytej licencji dla Oprogramowania;

- informacje o jakości usług KSN (protokół używany do wymiany danych z KSN; ID usługi KSN, do której dostęp uzyskało Oprogramowanie; data i godzina zaprzestania otrzymywania statystyk; liczba połączeń z KSN wzięta z pamięci podręcznej; liczba żądań, dla których odpowiedź znaleziono w lokalnej bazie żądań; liczba nieudanych połączeń z KSN; liczba nieudanych transakcji KSN; tymczasowa dystrybucja anulowanych żądań wysłanych do KSN; tymczasowa dystrybucja nieudanych połączeń z KSN; tymczasowa dystrybucja nieudanych transakcji KSN; tymczasowa dystrybucja pomyślnych połączeń z KSN; tymczasowa dystrybucja pomyślnych transakcji KSN; tymczasowa dystrybucja pomyślnych żądań wysłanych do KSN; tymczasowa dystrybucja żądań wysłanych do KSN, które przekroczyły limit czasu oczekiwania; liczba nowych połączeń z KSN; liczba niepomyślnych żądań wysłanych do KSN spowodowanych przez błędy routingu; liczba niepomyślnych żądań spowodowanych przez wyłączenie usługi KSN w ustawieniach Oprogramowania; liczba niepomyślnych żądań wysłanych do KSN spowodowanych przez problemy z siecią; liczba pomyślnych połączeń z KSN; liczba udanych transakcji KSN; całkowita liczba żądań wysłanych do KSN; data i godzina rozpoczęcia otrzymywania statystyk);

- ID urządzenia; pełna wersja Oprogramowania; ID aktualizacji Oprogramowania; ID instalacji Oprogramowania (PCID); typ zainstalowanego Oprogramowania;

- wysokość ekranu urządzenia; szerokość ekranu urządzenia; informacje o aplikacji wykorzystującej funkcję nakładki ekranowej: suma kontrolna MD5 pliku APK; informacje o aplikacji wykorzystującej funkcję nakładki ekranowej: suma kontrolna MD5 pliku classes.dex; informacje o aplikacji wykorzystującej funkcję nakładki ekranowej: nazwa pliku APK; informacje o aplikacji wykorzystującej funkcję nakładki ekranowej: ścieżka do pliku APK bez nazwy pliku; wysokość nakładki; informacje o nakładającym się Oprogramowaniu: suma kontrolna MD5 pliku APK; nakładające się informacje o aplikacji: suma kontrolna MD5 pliku classes.dex; nakładające się informacje o aplikacji: nazwa pliku APK; nakładające się informacje o aplikacji: ścieżka do pliku APK bez nazwy pliku; nakładające się informacje o aplikacji: nazwa pakietu aplikacji (dla nakładającego się aplikacja: jeśli reklama jest wyświetlana na pustym pulpicie, wartością powinien być ciąg "launcher"); data i godzina nałożenia; informacje o aplikacji wykorzystującej funkcję nakładki ekranowej: nazwa pakietu aplikacji; szerokość nakładki;

- ustawienia używanego punktu dostępowego Wi-Fi (typ wykrytego urządzenia; ustawienia DHCP (sumy kontrolne lokalnego adresu bramki: IPv6, DHCP IPv6, DNS1 IPv6, DNS2 IPv6; suma kontrolna długości prefiksu sieci; suma kontrolna adresu lokalnego IPv6); ustawienia DHCP (sumy kontrolne lokalnego adresu IP bramki, adresu IP DHCP, adresu IP DNS1, adresu IP DNS2 i maski podsieci); flaga wskazująca, czy domena DNS istnieje; suma kontrolna przypisanego lokalnego adresu IPv6; suma kontrolna przypisanego lokalnego adresu IPv4; flaga wskazująca, czy urządzenie jest podłączone; typ uwierzytelniania sieci Wi-Fi; lista dostępnych sieci Wi-Fi i ich ustawień; suma kontrolna (MD5 z solą) adresu MAC punktu dostępowego; suma kontrolna (SHA256 z solą) adresu MAC punktu dostępowego; typy połączeń wspomagane przez punkty dostępowe Wi-Fi; typ szyfrowania sieci Wi-Fi; czas lokalny rozpoczęcia i zakończenia połączenia z siecią Wi-Fi; identyfikator sieci Wi-Fi oparty na adresie MAC punktu dostępowego; identyfikator sieci Wi-Fi oparty na nazwie sieci Wi-Fi; identyfikator sieci Wi-Fi oparty na nazwie sieci Wi-Fi i adresie MAC punktu dostępowego; siła sygnału Wi-Fi; nazwę sieci bezprzewodowej (Wi-Fi); zbiór protokołów uwierzytelniania wspomaganych przez tę konfigurację; protokół uwierzytelniania stosowany dla połączenia WPA-EAP; wewnętrzny protokół uwierzytelniania; zbiór grupy szyfrów wspomaganych przez tę konfigurację; zbiór protokołów zarządzania kluczami wspomaganych przez tę konfigurację; ostatnia kategoria prywatności sieci w Oprogramowaniu; ostatnia kategoria bezpieczeństwa sieci w Oprogramowaniu; zestaw szyfrów blokowych dla WPA wspomaganych przez tę konfigurację; zestaw protokołów bezpieczeństwa wspomaganych przez tę konfigurację);

- data i godzina instalacji Oprogramowania; data aktywacji oprogramowania; identyfikator organizacji partnera, za pośrednictwem której złożono zamówienie na licencję dla Oprogramowania; identyfikator Oprogramowania pochodzący z licencji; numer seryjny klucza licencyjnego Oprogramowania; wersja językowa Oprogramowania; flaga wskazująca, czy uczestnictwo w KSN jest włączone; identyfikator licencjonowanego Oprogramowania; identyfikator licencji Oprogramowania; identyfikator systemu operacyjnego; wersję systemu operacyjnego.

Co więcej, w celu realizacji deklarowanego celu, tj. zwiększania efektywności ochrony zapewnianej przez Oprogramowanie, Posiadacz praw może otrzymywać obiekty, które mogą być wykorzystane przez niepowołane osoby do poczynienia szkód na Komputerze i stworzenia zagrożeń dla bezpieczeństwa informacji.

Udostępnianie powyższych informacji KSN jest dobrowolne. Możesz zakończyć uczestnictwo w Kaspersky Security Network w dowolnym momencie

Dostarczenia danych zgodnie z Oświadczeniem dotyczącym przetwarzania danych na potrzeby modułu Ochrona WWW

Zgodnie z Oświadczeniem dotyczącym modułu Ochrona WWW Posiadacz praw przetwarza dane w celu zapewnienia działania modułu Ochrona WWW. Określony cel obejmuje wykrywanie zagrożeń internetowych i określanie kategorii odwiedzanych stron internetowych przy użyciu usługi chmury Kaspersky Security Network (KSN).

Za zgodą Użytkownika następujące dane będą automatycznie i regularnie wysyłane do Posiadacza praw zgodnie z Oświadczeniem dotyczącym modułu Ochrona WWW:

- Wersja produktu; Unikatowy identyfikator urządzenia; ID instalacji; Typ produktu.
- Adres URL strony, numer portu, protokół URL, adres URL, który odsyła do żądanych informacji.

Dostarczenia danych zgodnie z Oświadczeniem dotyczącym przetwarzania danych w celach marketingowych.

Do przetwarzania danych Posiadacz praw używa systemów informacyjnych stron trzecich. Przetwarzanie danych przez strony trzecie podlega zapisom oświadczeń o ochronie prywatności dotyczących takich systemów informacyjnych stron trzecich. Poniżej wskazano usługi używane przez Posiadacza praw oraz przetwarzane w nich dane:

Google Analytics dla Firebase

Podczas korzystania z Oprogramowania następujące dane są automatycznie i regularnie wysyłane do usługi Google Analytics dla Firebase w celu spełnienia zadeklarowanego celu:

- informacje o aplikacji (wersja aplikacji, identyfikator aplikacji i identyfikator aplikacji w usłudze Firebase, identyfikator instancji w usłudze Firebase, nazwa sklepu, w którym zakupiono aplikację, znacznik czasowy pierwszego uruchomienia Oprogramowania)
- ID instalacji aplikacji na urządzeniu i metody instalacji na urządzeniu
- informacja o regionie i wersji językowej
- informacja o rozdzielczości ekranu urządzenia
- informacja o uzyskaniu przez użytkownika dostępu do konta root
- informacje diagnostyczne dotyczące urządzenia, pochodzące z usługi SafetyNet Attestation
- informacja o ustawieniu aplikacji Kaspersky Endpoint Security for Android jako funkcji ułatwień dostępu.
- informacje o przejściach między ekranami aplikacji, czasie trwania sesji, rozpoczęciu i zakończeniu sesji na ekranie, nazwie ekranu
- protokoł używany do przesyłania danych do usługi Firebase, jego wersja oraz ID używanej metody przesyłania danych
- szczegółowe informacje o typie i parametrach zgłaszanego zdarzenia
- informacje o licencji na aplikację, jej dostępności i liczbie urządzeń
- informacje o częstotliwości aktualizacji antywirusowej bazy danych i synchronizacji z Serwerem administracyjnym
- informacje o Konsoli administracyjnej (Kaspersky Security Center lub zewnętrzne systemy EMM)
- Android ID
- identyfikator treści reklamowych.
- informacje dotyczące Użytkownika: kategoria wiekowa i płeć, identyfikator kraju zamieszkania oraz lista zainteresowań

- informacje dotyczące komputera Użytkownika, na którym Oprogramowanie jest zainstalowane: nazwa producenta komputera, typ komputera, model, wersja i wersja językowa systemu operacyjnego, informacje o aplikacji pierwszy raz otwartej w ciągu ostatnich 7 dni oraz o aplikacji pierwszy raz otwartej ponad 7 dni temu

  Do usługi Firebase dane są przekazywane za pośrednictwem bezpiecznego połączenia. Informacje dotyczące sposobu przetwarzania danych w usłudze Firebase są dostępne na stronie internetowej https://firebase.google.com/support/privacy.

Usługa zaświadczania SafetyNet Attestation

Podczas korzystania z Oprogramowania następujące dane będą regularnie przesyłane automatycznie do usługi SafetyNet Attestation w celu realizacji deklarowanego celu:

- Czas kontroli urządzenia
- Informacja o oprogramowaniu, nazwy i dane certyfikatów oprogramowania
- Wyniki kontroli urządzenia
- Losowe kontrole ID w celu weryfikacji wyników kontroli urządzenia

  Do usługi SafetyNet Attestation dane są przekazywane za pośrednictwem bezpiecznego kanału. Informacje dotyczące sposobu przetwarzania danych w usłudze SafetyNet Attestation są dostępne na stronie internetowej: https://policies.google.com/privacy.

Firebase Performance Monitoring

Podczas korzystania z Oprogramowania następujące dane będą regularnie przesyłane automatycznie do usługi Firebase Performance Monitoring w celu realizacji deklarowanego celu:

- unikatowy identyfikator instalacji;
- nazwa pakietu aplikacji;
- wersję zainstalowanego Oprogramowania;
- poziom baterii i stan naładowania baterii;
- operator;
- stan aplikacji na pierwszym planie lub w tle;
- geografia;
- Adres IP
- kod języka urządzenia;
- informacje o połączeniu sieciowym/radiowym;
- pseudonimowy identyfikator instancji Oprogramowania;
- rozmiar dysku i pamięci RAM;
- flaga wskazująca, czy usunięto zabezpieczenia producenta w urządzeniu lub czy urządzenie było rootowane;
- siła sygnału;
- czas trwania automatycznego śledzenia;

- sieć, a także następujące odpowiednie informacje: kod odpowiedzi, rozmiar ładunku w bajtach, czas odpowiedzi
- opis urządzenia.

  Do usługi Firebase Performance Monitoring dane są przekazywane za pośrednictwem bezpiecznego połączenia. Informacje dotyczące sposobu przetwarzania danych w usłudze Firebase Performance Monitoring są dostępne na stronie internetowej: https://firebase.google.com/support/privacy.

Crashlytics

Podczas korzystania z Oprogramowania następujące dane będą regularnie przesyłane automatycznie do usługi Crashlytics w celu realizacji deklarowanego celu:

- ID oprogramowania;
- wersję zainstalowanego Oprogramowania;
- flaga wskazująca, czy Oprogramowanie było uruchomione w tle;
- architektura procesora;
- unikatowy identyfikator zdarzenia;
- data i godzina zdarzenia;
- modelu urządzenia;
- całkowity rozmiar dysku oraz przestrzeń aktualnie używana;
- nazwa i wersja systemu operacyjnego;
- całkowity rozmiar pamięci RAM oraz rozmiar aktualnie używany;
- flaga wskazująca, czy urządzenie było rootowane;
- orientacja ekranu w momencie wystąpienia zdarzenia;
- producent produktu/sprzętu;
- unikatowy identyfikator instalacji;
- wersja przesyłanych statystyk;
- typ wyjątku Oprogramowania;
- treść komunikatu o błędzie;
- flaga wskazująca, czy wyjątek Oprogramowania był spowodowany przez zagnieżdżony wyjątek;
- ID wątku;
- flaga wskazująca, czy ramka była przyczyną błędu Oprogramowania;
- flaga wskazująca, czy wątek spowodował niespodziewane zakończenie działania Oprogramowania;
- informacje o sygnale, który spowodował niespodziewane zakończenie działania Oprogramowania: nazwa sygnału, kod sygnału, adres sygnału

- dla każdej ramki skojarzonej z wątkiem, wyjątkiem lub błędem: nazwa pliku ramki, numer wiersza pliku ramki, symbole debugowania, adres i przesunięcie w obrazie binarnym, nazwa wyświetlana biblioteki z ramką, typ ramki, flaga wskazująca, czy ramka była przyczyną błędu
- identyfikator systemu operacyjnego;
- ID problemu skojarzonego ze zdarzeniem;
- informacje o zdarzeniach, które wystąpiły przed niespodziewanym zakończeniem działania Oprogramowania: identyfikator zdarzenia, data i godzina zdarzenia, typ i wartość zdarzenia
- wartości rejestru procesora;
- typ zdarzenia oraz wartość.

  Dane są przekazywane do usługi Crashlytics za pośrednictwem bezpiecznego kanału. Informacje na temat sposobu przetwarzania danych w usłudze Crashlytics są dostępne pod adresem: https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

Podanie powyższych informacji na potrzeby przetwarzania w celach marketingowych nie jest obowiązkowe.

Zapewnianie danych w Kaspersky Security for iOS

Produkt Kaspersky Security for Mobile jest zgodny z wymaganiami Rozporządzenia o Ochronie Danych Osobowych (GDPR - General Data Protection Regulation).

Aby zainstalować aplikację, użytkownik urządzenia musi przeczytać i zaakceptować następujące oświadczenia dotyczące przetwarzania jego danych osobowych:

- Umowa licencyjna
- Polityka prywatności dla Produktów i Usług

Opcjonalnie użytkownik może przeczytać i zaakceptować warunki następującego oświadczenia:

- Oświadczenie Kaspersky Security Network

Użytkownik może wyświetlić warunki z niniejszych dokumentów w dowolnym czasie w sekcji **Informacje o aplikacji** → **Umowy i oświadczenia** w ustawieniach Kaspersky Security for iOS. W tej sekcji użytkownik może także zaakceptować lub odrzucić warunki Oświadczenia KSN.

Wymiana informacji z Kaspersky Security Network

W celu udoskonalenia ochrony w czasie rzeczywistym, Kaspersky Security for iOS wykorzystuje usługę chmury Kaspersky Security Network podczas działania komponentu **Ochrona WWW**. Aplikacja wykorzystuje dane pobrane z KSN do skanowania zasobów internetowych przed ich otwarciem.

Informacje dotyczące typu danych wysyłanych do Kaspersky podczas korzystania z KSN w trakcie działania Ochrony WWW są dostępne w Umowie licencyjnej użytkownika końcowego. Akceptując warunki i postanowienia Umowy licencyjnej, wyrażasz zgodę na wysyłanie tych informacji.

Informacje dotyczące typu danych statystycznych wysyłanych do Kaspersky podczas korzystania z KSN w trakcie działania aplikacji mobilnej Kaspersky Security for iOS są dostępne w Oświadczeniu Kaspersky Security Network. Akceptując warunki i postanowienia Oświadczenia, wyrażasz zgodę na wysyłanie tych informacji.

Dostarczanie danych zgodnie z Umową licencyjną

Jeżeli do aktywacji Oprogramowania jest używany Kod aktywacyjny, w celu weryfikacji uprawnionego wykorzystania Oprogramowania, Użytkownik końcowy wyraża zgodę na okresowe przekazywanie Posiadaczowi praw następujących informacji:

- Format danych w żądaniu wysłanym do infrastruktury Posiadacza praw; adres iPv4 usługi sieciowej, do którego uzyskiwano dostęp; rozmiar zawartości żądania wysłanego do infrastruktury Posiadacza praw; ID protokołu; kod aktywacyjny oprogramowania; typ kompresji danych; ID oprogramowania; zestaw identyfikatorów Oprogramowania, które może być aktywowane na urządzeniu użytkownika; wersja językowa Oprogramowania; pełna wersja Oprogramowania; unikatowy identyfikator urządzenia; data i godzina na urządzeniu użytkownika; ID instalacji Oprogramowania (PCID); aktualnie używany kod aktywacyjny dla Oprogramowania; wersję systemu operacyjnego, numer wersji systemu operacyjnego, numer aktualizacji systemu operacyjnego, wydanie systemu operacyjnego, rozszerzone informacje o wydaniu systemu operacyjnego; model urządzenia; kod operatora sieci komórkowej; rodzinę systemu operacyjnego; identyfikator Oprogramowania pochodzący z licencji; lista umów przedstawionych użytkownikowi przez Oprogramowanie; typ umowy prawnej zaakceptowanej przez użytkownika podczas korzystania z Oprogramowania; wersja umowy prawnej zaakceptowanej przez użytkownika podczas korzystania z Oprogramowania; flaga wskazująca, czy użytkownik zaakceptował warunki umowy prawnej podczas korzystania z Oprogramowania; typ sumy kontrolnej przetwarzanego obiektu; nagłówek licencji Oprogramowania; ID regionalnego centrum aktywacji; dat i godzina utworzenia klucza licencyjnego Oprogramowania; identyfikator licencji Oprogramowania; ID modelu informacji użytego do dostarczenia licencji dla Oprogramowania; data i godzina wygaśnięcia licencji dla Oprogramowania; bieżący stan klucza licencyjnego Oprogramowania; typ użytej licencji dla Oprogramowania; typ licencji użytej do aktywowania Oprogramowania; identyfikator Oprogramowania pochodzący z licencji;

Posiadacz praw może wykorzystywać takie informacje również do gromadzenia informacji statystycznych dotyczących dystrybucji i użytkowania Oprogramowania Posiadacza praw.

W celu ochrony Komputera przed zagrożeniami dla bezpieczeństwa informacji Użytkownik końcowy zobowiązuje się do okresowego dostarczania Posiadaczowi praw następujących informacji:

- Format danych w żądaniu wysłanym do infrastruktury Posiadacza praw; ostatnio używany adres usługi sieciowej (URL, IP); numer portu; adres internetowy źródła żądania usługi sieciowej (odnośnik).

- pełna wersja Oprogramowania; ID aktualizacji Oprogramowania; typ zainstalowanego Oprogramowania; ID oprogramowania; identyfikator konfiguracji; wynik działania Oprogramowania; kod błędu.

- Przetwarzany adres internetowy; adres iPv4 usługi sieciowej, do którego uzyskiwano dostęp; odcisk palca certyfikatu cyfrowego przeskanowanego obiektu i algorytm funkcji skrótu; typ certyfikatu; treści przetwarzanego podpisu cyfrowego.

Dostarczenia danych zgodnie z Oświadczeniem Kaspersky Security Network

Po zaakceptowaniu Oświadczenia KSN Posiadacz praw automatycznie otrzymuje i przetwarza następujące dane:

- Informacje o jakości usług KSN (protokół używany do wymiany danych z KSN; ID usługi KSN, do której dostęp uzyskało Oprogramowanie; data i godzina zaprzestania otrzymywania statystyk; liczba połączeń z KSN wzięta z pamięci podręcznej; liczba żądań, dla których odpowiedź znaleziono w lokalnej bazie żądań; liczba nieudanych połączeń z KSN; liczba nieudanych transakcji KSN; tymczasowa dystrybucja anulowanych żądań wysłanych do KSN; tymczasowa dystrybucja nieudanych połączeń z KSN; tymczasowa dystrybucja nieudanych transakcji KSN; tymczasowa dystrybucja pomyślnych połączeń z KSN; tymczasowa dystrybucja pomyślnych transakcji KSN; tymczasowa dystrybucja pomyślnych żądań wysłanych do KSN; tymczasowa dystrybucja żądań wysłanych do

KSN, które przekroczyły limit czasu oczekiwania; liczba nowych połączeń z KSN; liczba niepomyślnych żądań wysłanych do KSN spowodowanych przez błędy routingu; liczba niepomyślnych żądań spowodowanych przez wyłączenie usługi KSN w ustawieniach Oprogramowania; liczba niepomyślnych żądań wysłanych do KSN spowodowanych przez problemy z siecią; liczba pomyślnych połączeń z KSN; liczba udanych transakcji KSN; całkowita liczba żądań wysłanych do KSN; data i godzina rozpoczęcia otrzymywania statystyk).

- ID urządzenia; pełna wersja Oprogramowania; ID aktualizacji Oprogramowania; ID instalacji Oprogramowania (PCID); typ zainstalowanego Oprogramowania.

- Data i godzina instalacji Oprogramowania; data aktywacji oprogramowania; wersja językowa Oprogramowania; flaga wskazująca, czy uczestnictwo w KSN jest włączone; identyfikator licencjonowanego Oprogramowania; identyfikator licencji Oprogramowania; identyfikator systemu operacyjnego; wersja systemu operacyjnego zainstalowanego na komputerze użytkownika; wersję systemu operacyjnego.

Udostępnianie powyższych informacji KSN jest dobrowolne. Możesz zakończyć uczestnictwo w Kaspersky Security Network w dowolnym momencie

Kontakt z pomocą techniczną

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 Kaspersky Security for Mobile lub w jednym z dodatkowych źródeł informacji o Kaspersky Security for Mobile, skontaktuj się z działem pomocy technicznej. Eksperci z działu pomocy technicznej odpowiedzą na wszystkie Twoje pytania związane z instalacją i użytkowaniem Kaspersky Security for Mobile.

Kaspersky zapewnia wsparcie dla aplikacji Kaspersky Security for Mobile w trakcie jej cyklu życia (zobacz stronę czasu trwania wsparcia technicznego). Przed skontaktowaniem się z działem pomocy technicznej przeczytaj zasady korzystania z pomocy technicznej.

Możesz skontaktować się z działem pomocy technicznej na jeden z następujących sposobów:

- Odwiedzając stronę pomocy technicznej
- Wysyłając zgłoszenie do pomocy technicznej poprzez portal Kaspersky CompanyAccount

Pomoc techniczna poprzez Kaspersky CompanyAccount

Kaspersky CompanyAccount to portal dla firm, które korzystają z aplikacji Kaspersky. Portal Kaspersky CompanyAccount został zaprojektowany w celu ułatwienia interakcji między użytkownikami a specjalistami z Kaspersky poprzez zgłoszenia online. Możesz użyć Kaspersky CompanyAccount do śledzenia stanu swoich zgłoszeń online oraz do przechowywania ich historii.

Możesz zarejestrować wszystkich pracowników firmy pod jednym kontem na portalu Kaspersky 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:

- angielskim
- hiszpańskim
- włoskim
- niemieckim
- polskim
- portugalskim
- rosyjskim

- francuskim
- japońskim

Więcej informacji o portalu Kaspersky CompanyAccount można znaleźć na stronie działu pomocy technicznej.

Źródła informacji o aplikacji

Strona programu Kaspersky Security for Mobile na witrynie Kaspersky

Na stronie Kaspersky Security for Mobile możesz znaleźć ogólne informacje o aplikacji, jej funkcjach i parametrach działania.

Strona internetowa Kaspersky Security for Mobile zawiera odnośnik do sklepu internetowego. Możesz w nim kupić lub odnowić licencję dla aplikacji.

Strona programu Kaspersky Security for Mobile w Bazie wiedzy

Baza wiedzy to sekcja na stronie działu pomocy technicznej.

Na stronie internetowej Kaspersky Security for Mobile w Bazie wiedzy znajdziesz artykuły zawierające przydatne informacje, zalecenia i odpowiedzi na najczęściej zadawane pytania dotyczące zakupu, instalacji i korzystania z aplikacji.

Artykuły z Bazy wiedzy mogą zawierać odpowiedzi na pytania spoza zakresu programu Kaspersky Security for Mobile, związane z innymi aplikacjami Kaspersky. Artykuły z Bazy wiedzy mogą także zawierać nowości z działu pomocy technicznej.

Pomoc elektroniczna

Pomoc elektroniczna aplikacji zawiera pliki pomocy.

Pomoc kontekstowa wtyczek zarządzających dla Kaspersky Security for Mobile zawiera informacje o oknach Kaspersky Security Center: opis ustawień Kaspersky Security for Mobile i odnośniki do opisów zadań, które wykorzystują te ustawienia.

Pełna pomoc aplikacji Kaspersky Endpoint Security for Android i Kaspersky Security for iOS zawiera informacje na temat konfigurowania i korzystania z aplikacji mobilnych.

Forum internetowe firmy Kaspersky z dyskusjami na temat aplikacji Kaspersky

Jeżeli zapytanie nie wymaga natychmiastowej odpowiedzi, można przedyskutować je ze specjalistami z firmy Kaspersky lub innymi użytkownikami jej oprogramowania na naszym Forum.

Na Forum możesz przeglądać istniejące tematy, pozostawiać swoje komentarze i tworzyć nowe tematy.

Słownik

Administrator Kaspersky Security Center

Osoba zarządzająca działaniami aplikacji za pośrednictwem systemu zdalnego zarządzania Kaspersky Security Center.

Administrator urządzenia

Zestaw uprawnień aplikacji na urządzeniu z systemem Android, który umożliwia aplikacji użycie zasad zarządzania urządzeniami. Jest on konieczny do zaimplementowania w pełni funkcjonalnej wersji programu Kaspersky Endpoint Security na urządzeniach z systemem Android.

Aktywowanie aplikacji

Przełączanie aplikacji do trybu pełnej funkcjonalności. Aktywacja aplikacji jest przeprowadzana przez użytkownika podczas lub po instalacji aplikacji. Aby aktywować aplikację, należy posiadać kod aktywacyjny lub plik klucza.

Antywirusowe bazy danych

Bazy danych zawierające informacje o zagrożeniach ochrony komputera znane specjalistom z Kaspersky w momencie opublikowania antywirusowych baz danych. Wpisy w antywirusowych bazach danych umożliwiają wykrywanie szkodliwego kodu w skanowanych obiektach. Antywirusowe bazy danych są tworzone przez specjalistów z Kaspersky i aktualizowane co godzinę.

Autonomiczny pakiet instalacyjny

Plik instalacyjny Kaspersky Endpoint Security dla systemu operacyjnego Android, który zawiera ustawienia połączenia aplikacji z Serwerem administracyjnym. Jest on tworzony na podstawie pakietu instalacyjnego tej aplikacji i jest szczególnym elementem pakietu aplikacji mobilnej.

Certyfikat Apple Push Notification service (APNs)

Certyfikat podpisany przez Apple, który umożliwia korzystanie z Apple Push Notification. Za pośrednictwem Apple Push Notification serwer iOS MDM Server może zarządzać urządzeniami iOS.

Grupa administracyjna

Zestaw zarządzanych urządzeń, takich jak urządzenia mobilne pogrupowane według wykonywanych funkcji, a także zestaw aplikacji zainstalowanych na tych urządzeniach. Zarządzane urządzenia są pogrupowane tak, aby możliwe było zarządzanie nimi jako jednostką. Na przykład, urządzenia mobilne działające na tym samym systemie operacyjnym mogą zostać połączone w grupy administracyjne. Grupa może zawierać w sobie inne grupy administracyjne. Dla urządzeń w grupie możliwe jest utworzenie zasad grupy i zadań grupowych.

IMAP

Protokół umożliwiający dostęp do poczty. W przeciwieństwie do protokołu POP3, IMAP zapewnia więcej możliwości pracy ze skrzynkami pocztowymi, na przykład zarządzanie folderami oraz wiadomościami bez kopiowania ich zawartości z serwera pocztowego. Protokół IMAP korzysta z portu 134.

Kaspersky Private Security Network (Private KSN)

Kaspersky Private Security Network to rozwiązanie, które zapewnia użytkownikom urządzeń z zainstalowanymi aplikacjami Kaspersky dostęp do baz danych reputacji Kaspersky Security Network i innych danych statystycznych - bez wysyłania danych z ich urządzeń do Kaspersky Security Network. Kaspersky Private Security Network jest przeznaczony dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z jednego z następujących powodów:

- Urządzenia użytkownika nie są połączone z internetem.
- Przesyłanie jakichkolwiek danych poza kraj lub korporacyjną sieć LAN jest zabronione przez prawo lub korporacyjne zasady bezpieczeństwa.

Kaspersky Security Center Web Server

Składnik Kaspersky Security Center, który jest instalowany wraz z Serwerem administracyjnym. Serwer sieciowy został zaprojektowany do przesyłania poprzez sieć autonomicznych pakietów instalacyjnych, profili iOS MDM oraz plików z folderu współdzielonego.

Kaspersky Security Network (KSN)

Usługa chmury oferująca dostęp do bazy danych firmy Kaspersky, zawierającej ciągle aktualizowane informacje o reputacji plików, zasobów sieciowych oraz oprogramowania. Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji Kaspersky na zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów.

Kategorie Kaspersky

Predefiniowane kategorie danych, stworzone przez ekspertów z Kaspersky. Kategorie mogą być aktualizowane podczas aktualizacji baz danych aplikacji. Administrator ds. bezpieczeństwa nie może modyfikować ani usuwać predefiniowanych kategorii.

Kod aktywacyjny

Kod, który otrzymasz po zakupie licencji dla Kaspersky Endpoint Security. Ten kod jest wymagany do aktywacji aplikacji.

Kod aktywacyjny jest unikatową sekwencją dwudziestu liter i cyfr w formacie xxxxx-xxxxx-xxxxx-xxxxx.

Kod odblokowujący

Kod, który możesz uzyskać w Kaspersky Security Center. Jest on potrzebny do odblokowania urządzenia po wykonaniu poleceń **Blokada oraz Lokalizacja**, **Alarm** lub **Zrób zdjęcie (mugshot)** i gdy wyzwolona zostaje Autoochrona.

Kontrola zgodności

Sprawdzanie, czy ustawienia urządzenia mobilnego i Kaspersky Endpoint Security for Android odpowiadają firmowym wymaganiom bezpieczeństwa. Firmowe wymagania bezpieczeństwa regulują korzystanie z urządzenia. Na przykład, ochrona w czasie rzeczywistym musi być włączona na urządzeniu, antywirusowe bazy danych muszą być aktualne, a hasło do urządzenia musi być wystarczająco silne. Kontrola zgodności opiera się na liście reguł. Reguła zgodności obejmuje następujące komponenty:

- Kryterium sprawdzania urządzenia (na przykład, brak zabronionych aplikacji na urządzeniu)
- Czas, jaki użytkownik ma na wyeliminowanie niezgodności (na przykład 24 godziny)
- Działanie, jakie zostanie podjęte na urządzeniu, jeśli użytkownik nie wyeliminuje niezgodności w określonym przedziale czasu (na przykład, zablokowanie urządzenia)

Kwarantanna

Folder, do którego aplikacja Kaspersky przenosi wykryte prawdopodobnie zainfekowane obiekty. Obiekty są przechowywane w Kwarantannie w postaci zaszyfrowanej w celu uniknięcia jakiegokolwiek wpływu na komputer.

Licencja

Czasowo ograniczone prawo do korzystania z aplikacji nadane zgodnie z Umową licencyjną.

Okres ważności licencji

Okres, w którym masz dostęp do funkcji aplikacji i posiadasz uprawnienia do korzystania z dodatkowych usług. Usługi, z których możesz korzystać, zależą od typu licencji.

Pakiet instalacyjny

Zestaw plików utworzonych dla zdalnej instalacji aplikacji Kaspersky przy pomocy systemu zdalnego zarządzania. Pakiet instalacyjny jest tworzony na podstawie dedykowanych plików znajdujących się w pakiecie dystrybucyjnym aplikacji. Pakiet instalacyjny zawiera szereg ustawień potrzebnych do zainstalowania aplikacji i uruchomienia od razu po instalacji. Wartości ustawień w pakiecie dystrybucyjnym odpowiadają domyślnym wartościom ustawień aplikacji.

Phishing

Rodzaj oszustwa internetowego, którego celem jest uzyskanie nieautoryzowanego dostępu do poufnych danych użytkownika.

Plik klucza

Plik w formacie xxxxxxxx.key, który umożliwia korzystanie z aplikacji firmy Kaspersky na warunkach licencji testowej lub komercyjnej. Aplikacja generuje plik klucza w oparciu o kod aktywacyjny. Możesz użyć aplikacji tylko wtedy, gdy posiadasz plik klucza.

Plik manifestu

Plik w formacie PLIST zawierający odnośnik do pliku aplikacji (plik ipa) znajdującego się na serwerze sieciowym. Jest on używany przez urządzenia z systemem iOS do lokalizacji, pobierania i instalowania aplikacji z serwera sieciowego.

POP3

Protokół sieciowy używany przez klienta poczty do odbierania wiadomości z serwera pocztowego.

Profil informacyjny

Zbiór ustawień niezbędny do działania aplikacji na urządzeniach mobilnych iOS. Profil informacyjny zawiera informacje o licencji; jest połączony z określoną aplikacją.

Profil iOS MDM

Profil zawierający zbiór ustawień do podłączenia urządzeń mobilnych iOS do Serwera administracyjnego. Profil iOS MDM umożliwia wysyłanie profili konfiguracyjnych iOS w tle poprzez serwer iOS MDM, a także pobranie rozszerzonych informacji diagnostycznych dotyczących urządzeń mobilnych. Odsyłacz do profilu iOS MDM powinien zostać wysłany do użytkownika w celu umożliwienia serwerowi iOS MDM wykrycie i podłączenie urządzenia mobilnego użytkownika z systemem iOS.

Profil roboczy Android

Bezpieczne środowisko na urządzeniu użytkownika, w którym administrator może zarządzać aplikacjami i kontami użytkowników bez ograniczenia korzystania z danych osobowych przez użytkownika. Po utworzeniu profilu roboczego na urządzeniu mobilnym użytkownika, automatycznie instalowane są w profilu roboczym następujące aplikacje: Sklep Google Play, Google Chrome, Pobrane, Kaspersky Endpoint Security for Android i inne. Aplikacje firmowe zainstalowane w profilu roboczym oraz powiadomienia tych aplikacji oznaczone są ikoną czerwonej teczki. Dla aplikacji Google Play należy utworzyć oddzielne konto firmowe Google. Aplikacje zainstalowane w profilu roboczym pojawią się na ogólnej liście aplikacji.

Serwer administracyjny

Moduł aplikacji Kaspersky Security Center realizujący funkcje scentralizowanego przechowywania informacji na temat wszystkich aplikacji firmy Kaspersky zainstalowanych w sieci korporacyjnej. Może być używany do zarządzania tymi aplikacjami.

Serwer iOS MDM

Składnik Kaspersky Endpoint Security zainstalowany na urządzeniu klienckim pozwalający na połączenie urządzeń mobilnych iOS z Serwerem administracyjnym i zarządzanie urządzeniami mobilnymi iOS za pośrednictwem usługi Apple Push Notifications (APNs).

Serwer proxy

Usługa sieci komputerowej, która umożliwia użytkownikom wysyłanie bezpośrednich żądań do innych usług sieciowych. Użytkownik łączy się z serwerem proxy i żąda określonego zasobu (na przykład, pliku), znajdującego się na innym serwerze. Następnie serwer proxy łączy się z określonym serwerem i uzyskuje z niego zasób lub zwraca zasób ze swojej pamięci podręcznej (jeśli proxy posiada swoją pamięć podręczną). W niektórych przypadkach żądanie użytkownika lub odpowiedź serwera może być zmodyfikowana przez serwer proxy dla określonych celów.

Serwer urządzeń mobilnych Exchange

Komponent programu Kaspersky Endpoint Security, który umożliwia podłączenie urządzeń mobilnych Exchange ActiveSync do Serwera administracyjnego.

Serwery aktualizacji Kaspersky

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

SSL

Protokół szyfrowania danych używany w internecie i sieciach lokalnych. Protokół Secure Sockets Layer (SSL) jest używany w aplikacjach internetowych do tworzenia bezpiecznego połączenia między klientem a serwerem.

Stacja robocza administratora

Komputer, na którym została wdrożona Konsola administracyjna Kaspersky Security Center. Jeśli wtyczka zarządzająca aplikacją jest zainstalowana na stacji roboczej administratora, administrator może zarządzać aplikacjami mobilnymi Kaspersky Endpoint Security, które są zainstalowane na urządzeniach użytkownika.

Subskrypcja

Umożliwia korzystanie z aplikacji z wybranymi parametrami (data wygaśnięcia i liczba urządzeń). Możesz wstrzymać lub wznowić subskrypcję, odnowić ją automatycznie lub anulować ją.

Umowa licencyjna

Wiążąca umowa prawna zawierana pomiędzy Tobą a firmą AO Kaspersky Lab, która określa zasady korzystania z zakupionej aplikacji.

Urządzenie EAS

Urządzenie mobilne podłączone do Serwera administracyjnego za pośrednictwem protokołu Exchange ActiveSync.

Urządzenie iOS MDM

Urządzenie mobilne iOS, kontrolowane przez serwer iOS MDM.

Urządzenie nadzorowane

Urządzenie iOS, którego ustawienia są monitorowane przez Apple Configurator, program do konfiguracji grupowej urządzeń iOS. Urządzenie nadzorowane posiada stan *supervised* (nadzorowane) w Apple Configurator. Za każdym razem, gdy urządzenie nadzorowane nawiązuje połączenie z komputerem, Apple Configurator porównuje konfigurację urządzenia z określonymi ustawieniami referencyjnymi, a następnie ponownie je definiuje (jeśli jest to konieczne). Urządzenie nadzorowane nie może zostać zsynchronizowane z aplikacją Apple Configurator, zainstalowaną na innym komputerze.

Każde urządzenie nadzorowane oferuje więcej ustawień do ponownego zdefiniowania za pośrednictwem zasady Kaspersky Device Management for iOS niż urządzenie nienadozrowane. Na przykład, możesz skonfigurować serwer proxy HTTP do monitorowania ruchu internetowego na urządzeniu w obrębie sieci firmowej. Domyślnie, wszystkie urządzenia mobilne są nienadzorowane.

Wirus

Program, który infekuje inne programy poprzez dodanie do nich swojego kodu w celu uzyskania kontroli, gdy uruchamiane są zainfekowane pliki. Ta prosta definicja umożliwia identyfikowanie głównej akcji, wykonanej przez dowolnego wirusa: infekcji.

Wtyczka do zarządzania aplikacją

Dedykowany moduł, który zawiera interfejs zarządzania aplikacjami firmy Kaspersky poprzez Konsolę administracyjną. Każda aplikacja, która może być zarządzana za pomocą Kaspersky Security Center SPE posiada swoją własną wtyczkę do zarządzania aplikacją. Wtyczka do zarządzania aplikacją jest zawarta we wszystkich aplikacjach Kaspersky, które mogą być zarządzane za pomocą Kaspersky Security Center.

Zadanie grupowe

Zadanie przeznaczone dla grupy administracyjnej i wykonywane na zarządzanych urządzeniach tej grupy.

Żądanie podpisania certyfikatu

Plik z ustawieniami Serwera administracyjnego, który jest zatwierdzony przez Kaspersky, a następnie zostaje wysłany do Apple w celu uzyskania certyfikatu APNs.

Zasada

Zestaw ustawień aplikacji i aplikacji mobilnych Kaspersky Endpoint Security stosowany na urządzeniach w grupach administracyjnych bądź na pojedynczych urządzeniach. Różne zasady mogą być stosowane dla różnych grup administracyjnych. Zasada zawiera skonfigurowane ustawienia wszystkich funkcji aplikacji mobilnych Kaspersky Endpoint Security.

Informacje o kodzie firm trzecich

Możesz pobrać i przeczytać informacje o kodzie stron trzecich w następujących plikach:

- legal_notices_Android.txt (dla aplikacji Kaspersky Endpoint Security for Android)
- legal_notices_iOS.txt (dla aplikacji Kaspersky Security for iOS)

Na urządzeniach mobilnych informacje o kodzie stron trzecich są dostępne w sekcji **Informacje o aplikacji** w aplikacjach mobilnych.

Informacje o znakach towarowych

Zastrzeżone znaki towarowe i usługowe stanowią odpowiednio własność ich właścicieli.

PostScript jest zastrzeżonym znakiem towarowym bądź znakiem towarowym firmy Adobe zarejestrowanym w Stanach Zjednoczonych i/lub innych krajach.

AirDrop i AirPrint są zastrzeżonymi znakami towarowymi firmy Apple Inc.

Apple, Apple Configurator, AirPlay, AirPort Express, App Store, Apple TV, Bonjour, Face ID, FaceTime, FileVault, iBooks, iCal, iCloud, iPad, iPadOS, iPhone, iTunes, OS X, Safari, Spotlight i Touch ID są zastrzeżonymi znakami towarowymi firmy Apple Inc., zarejestrowanymi w Stanach Zjednoczonych i innych krajach i regionach.

Aruba Networks jest zastrzeżonym znakiem towarowym firmy Aruba Networks, Inc. w Stanach Zjednoczonych i innych krajach.

Słowo, znak i logo Bluetooth są własnością Bluetooth SIG, Inc.

Cisco, Cisco AnyConnect i IOS są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Cisco Systems, Inc. i/lub jej oddziałów, zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

SecurID jest zastrzeżonym znakiem towarowym lub znakiem towarowym firmy EMC Corporation, zarejestrowanym w Stanach Zjednoczonych i/lub innych krajach.

Google, Android, Chrome, Chromebook, Chromium, Crashlytics, Firebase, Google Analytics, Google Chrome, Google Mail, Google Maps, Google Play, Nexus i SPDY są zastrzeżonymi znakami towarowymi firmy Google LLC.

HTC jest znakiem towarowym firmy HTC Corporation.

Huawei, HUAWEI i EMUI są zastrzeżonymi znakami towarowymi firmy Huawei Technologies Co., Ltd, zarejestrowanymi w Chinach i innych krajach.

IBM i Maas360 są znakami towarowymi firmy International Business Machines Corporation, zarejestrowanymi w wielu jurysdykcjach na świecie.

Juniper Networks, Juniper i JUNOS są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Juniper Networks, Inc., zastrzeżonymi w Stanach Zjednoczonych i innych krajach.

Microsoft, ActiveSync, Microsoft Intune, Tahoma, Windows, Windows Mobile i Windows Phone są znakami towarowymi grupy firm Microsoft.

MOTOROLA i Stylized M Logo to znaki towarowe lub zastrzeżone znaki towarowe firmy Motorola Trademark Holdings, LLC.

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

BlackBerry jest zastrzeżonym znakiem towarowym firmy Research In Motion Limited zarejestrowanym na terenie Stanów Zjednoczonych i jest w trakcie rejestrowania lub już jest zarejestrowany na terenie innych krajów.

Samsung to znak towarowy firmy SAMSUNG zarejestrowany w Stanach Zjednoczonych lub innych krajach.

SonicWALL, Aventail, and SonicWALL Mobile Connect są zastrzeżonymi znakami towarowymi firmy SonicWall, Inc.

SOTI i MobiControl są zastrzeżonymi znakami towarowymi firmy SOTI Inc., zarejestrowanymi w Stanach Zjednoczonych i innych jurysdykcjach.