Kaspersky Security Center 10

Praktyczne zastosowanie aplikacji

Wersja aplikacji: 10 Service Pack 2

Drogi Użytkowniku,

dziękujemy za wybranie naszego produktu. Mamy nadzieję, że ten podręcznik będzie pomocny podczas pracy i odpowie na większość pytań.

Dokument może zostać zmieniony bez wcześniejszego informowania. Najnowsza wersja podręcznika jest zawsze dostępna na stronie http://www.kaspersky.pl.

Data korekty dokumentu: 14.01.2016

http://www.kaspersky.pl
https://help.kaspersky.com/pl/
http://support.kaspersky.com/pl/

Spis treści

Informacje o tym dokumencie

Podręcznik administratora dla Kaspersky Security Center 10 (zwanego dalej "Kaspersky Security Center") jest przeznaczony dla profesjonalistów, którzy instalują i zarządzają Kaspersky Security Center, a także dla tych, którzy zapewniają wsparcie techniczne firmom korzystającym z programu Kaspersky Security Center.

Podręcznik zawiera instrukcje dotyczące konfiguracji i korzystania z Kaspersky Security Center.

W podręczniku znajduje się także lista alternatywnych źródeł informacji o aplikacji i sposobów uzyskania pomocy technicznej.

W tej sekcji:

W tym dokumencie

Dokument Praktyczne zastosowanie aplikacji Kaspersky Security Center zawiera zalecenia dotyczące instalacji, konfiguracji i korzystania z aplikacji, a także opisuje sposoby rozwiązywania typowych problemów występujących podczas działania aplikacji.

Planowanie instalacji Kaspersky Security Center (patrz strona 12)

Ta sekcja zawiera informacje dotyczące sposobu wybierania systemu zarządzania bazą danych (DBMS) dla Serwera administracyjnego, zapewnienia Serwerowi administracyjnemu dostępu do internetu, a także zarządzania standardową konfiguracją Kaspersky Security Center. Można tu znaleźć informacje o roli Agentów aktualizacji oraz o znaczeniu hierarchii Serwerów administracyjnych. Dodatkowo, opisano tu sposób zarządzania wirtualnymi Serwerami administracyjnymi, instalacji obrazów systemu operacyjnego oraz zarządzania urządzeniami mobilnymi i Network Access Control (NAC).

Instalowanie i wstępne konfigurowanie komponentów i aplikacji (patrz strona 35)

W tym miejscu można znaleźć opis instalacji Serwera administracyjnego, Agenta sieciowego i programu antywirusowego oraz wstępnej konfiguracji Kaspersky Security Center. Ponadto zawarto tu informacje dotyczące tworzenia kopii zapasowej i przywracania ustawień Serwera administracyjnego, obsługi profili użytkownika mobilnego, a także konfiguracji i korzystania z NAC.

Wykonywanie podstawowych zadań (patrz strona 124)

Z tej sekcji można się dowiedzieć o podstawowych zadaniach, które można wykonać, korzystając z aplikacji. Zadania te obejmują zdalny dostęp do komputerów, zarządzanie urządzeniami mobilnymi oraz stosowanie standardowych scenariuszy NAC do monitorowania aktywności urządzeń sieciowych.

Kontakt z działem pomocy technicznej (patrz strona 161)

Sekcja zawiera informacje o sposobach uzyskania pomocy technicznej i warunkach, które należy spełnić, aby tę pomoc uzyskać.

AO Kaspersky Lab (patrz strona 164)

Sekcja zawiera informacje o firmie AO Kaspersky Lab.

Informacje o znakach towarowych (patrz strona 166)

Ta sekcja zawiera nazwy stanowiące zastrzeżone znaki towarowe.

Oznaczenia stosowane w dokumencie

W niniejszym dokumencie używane są następujące oznaczenia (patrz tabela poniżej).

Tabela 1. Oznaczenia stosowane w dokumencie

Przykładowy tekst	Opis oznaczeń stosowanych w dokumencie
Pamiętaj, że...	Ostrzeżenia są wyróżnione kolorem czerwonym i znajdują się w ramkach. Ostrzeżenia zawierają informacje o działaniach, które mogą doprowadzić do niechcianych sytuacji.

Przykładowy tekst	Opis oznaczeń stosowanych w dokumencie
Zalecamy korzystać z...	Uwagi znajdują się w ramkach. Notatki zawierają dodatkowe informacje.
Przykład:	Przykłady znajdują się na niebieskim tle pod nagłówkiem "Przykład".
Aktualizacja to... Występuje zdarzenie *Bazy danych są nieaktualne*.	Następujące elementy oznaczone są kursywą: • Nowe pojęcia. • Nazwy stanów aplikacji i zdarzeń.
Wciśnij **ENTER**. Wciśnij **ALT**+**F4**.	Nazwy klawiszy oznaczone są pogrubioną czcionką i wielkimi literami. Nazwa klawiszy z umieszczonym pomiędzy nimi symbolem "+" oznacza użycie kombinacji klawiszy. Klawisze te należy wciskać jednocześnie.
Kliknij przycisk **Włącz**.	Nazwy elementów interfejsu aplikacji (pola do wprowadzania danych, elementy menu i przyciski) oznaczone są pogrubioną czcionką.
► *W celu skonfigurowania terminarza zadania:*	Frazy wprowadzające do instrukcji oznaczone są kursywą i towarzyszy im znak strzałki.
Wprowadź `help` w wierszu poleceń Pojawi się następująca wiadomość: `Określ datę w formacie dd:mm:rr.`	Następujące typy tekstu są wyróżnione specjalną czcionką: • tekst wiersza poleceń; • treść wiadomości wyświetlanej na ekranie przez aplikację; • dane, które użytkownik powinien wprowadzić z klawiatury.
<Nazwa użytkownika>	Zmienne znajdują się w nawiasach ostrych. Zamiast zmiennej należy wpisywać odpowiadającą jej wartość, pomijając nawiasy.

Planowanie instalacji Kaspersky Security Center

Podczas planowania instalacji komponentów Kaspersky Security Center w sieci firmowej należy uwzględnić rozmiar i obszar projektu, a zwłaszcza poniższe czynniki:

- Całkowitą liczbę hostów.
- Jednostki (biura lokalne, oddziały), które są oddalone geograficznie lub pod względem organizacyjnym.
- Oddalone od siebie sieci połączone wąskimi kanałami.
- Konieczność dostępu do Serwera administracyjnego z poziomu internetu (sekcja "Umożliwianie Serwerowi administracyjnemu uzyskanie dostępu do internetu" na stronie 14).

Jeden Serwer administracyjny może obsługiwać maksymalnie 50 000 komputerów. Jeśli całkowita liczba komputerów w sieci firmowej przekroczy 50 000, wówczas w tej sieci należy zainstalować kilka Serwerów administracyjnych i połączyć je w hierarchię w celu uproszczenia scentralizowanego zarządzania.

Jeśli firma zawiera znaczną liczbę zdalnych biur lokalnych (oddziałów), z których każdy posiada swojego administratora, znacznym ułatwieniem będzie zainstalowanie Serwera administracyjnego w każdym z tych biur. W przeciwnym razie, biura te należy postrzegać jako oddalone od siebie sieci połączone wąskimi kanałami.

Zapoznaj się z sekcją "Standardowa konfiguracja: Duże oddziały posiadające swoich administratorów " (strona 19).

Podczas korzystania z oddalonych od siebie sieci połączonych wąskimi kanałami, ruch sieciowy można zmniejszyć, wskazując kilku Agentów sieciowych jako Agentów aktualizacji (jeden Agent aktualizacji na 100-200 hostów). W tym przypadku wszystkie komputery w oddalonej sieci będą pobierać uaktualnienia z tych lokalnych centrów aktualizacji. Te Agenty aktualizacji mogą pobierać uaktualnienia z Serwera administracyjnego (domyślna opcja) lub z serwerów Kaspersky Lab dostępnych w internecie.

Zapoznaj się z sekcją "Standardowa konfiguracja: Małe zdalne biura" (strona 20).

Sekcja "Standardowa konfiguracja Kaspersky Security Center" (strona 18) zawiera szczegółowy opis standardowej konfiguracji Kaspersky Security Center. Podczas planowania instalacji wybierz najodpowiedniejszą konfigurację, mając na uwadze strukturę firmy.

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

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

Zapoznaj się z sekcją "Określanie certyfikatu Serwera administracyjnego" (strona 41).

W tej sekcji:

Wybieranie systemu zarządzania bazą danych (DBMS) dla Serwera administracyjnego

Podczas wybierania systemu zarządzania bazą danych (DBMS), który zostanie użyty przez Serwer administracyjny, należy brać pod uwagę liczbę komputerów podlegających Serwerowi administracyjnemu. Na przykład, system zarządzania bazą danych Microsoft® SQL Server® 2008 R2 Express Edition, który jest dostarczany wraz z Kaspersky Security Center, obsługuje tylko jeden procesor i maksymalnie 1 GB pamięci RAM. Rozmiar bazy danych jest ograniczony do 10 GB. Nie można używać systemu zarządzania bazą danych SQL Server Express edition, jeśli Serwer administracyjny obejmuje ponad 10 000 hostów. Jeśli Serwer administracyjny obsługuje ponad 10 000 komputerów, należy użyć wersji serwera SQL posiadającej mniej ograniczeń: SQL Server® Workgroup Edition, SQL Server® Web Edition, SQL Server® Standard Edition lub SQL Server® Enterprise Edition.

Jeśli Serwer administracyjny obsługuje 10 000 lub mniej komputerów, jako systemu zarządzania bazą danych można użyć także MySQL 5.0.

Zobacz również:

Wymagania sprzętowe dla systemu zarządzania bazą danych i Serwera administracyjnego.. 138

Wybieranie systemu zarządzania bazą danych..... 37

Umożliwianie uzyskania dostępu do Serwera administracyjnego przez internet

Wykonanie następujących czynności wymaga dostępu do Serwera administracyjnego przez internet:

- Zarządzanie komputerami (laptopami) użytkowników mobilnych

- Zarządzanie komputerami w zdalnych biurach
- Komunikowanie się z nadrzędnymi lub podrzędnymi Serwerami administracyjnymi w zdalnych biurach
- Zarządzanie urządzeniami mobilnymi

Ta sekcja opisuje podstawowe sposoby zapewnienia dostępu do Serwera administracyjnego poprzez internet. Każdy przypadek skupiający się na zapewnieniu dostępu do Serwera administracyjnego przez internet może wymagać dedykowanego certyfikatu dla Serwera administracyjnego (sekcja “Określanie certyfikatu Serwera administracyjnego“ na stronie 41).

W tej sekcji:

Dostęp do internetu: Serwer administracyjny w sieci lokalnej

Jeśli Serwer administracyjny znajduje się w wewnętrznej sieci firmy, port TCP o numerze 13000 Serwera administracyjnego stanie się dostępny z zewnątrz za pomocą przekierowania portów. Jeśli wymagane jest zarządzanie urządzeniami mobilnymi, port TCP o numerze 13292 stanie się dostępny.

Dostęp do internetu: Serwer administracyjny w strefie zdemilitaryzowanej (DMZ)

Jeśli Serwer administracyjny znajduje się w DMZ sieci firmowej, nie ma on dostępu do wewnętrznej sieci firmy. Dlatego też występują następujące ograniczenia:

- Serwer administracyjny nie może wykryć nowych komputerów.
- Serwer administracyjny nie może wykonać wstępnej instalacji Agenta sieciowego przy użyciu wymuszonej instalacji na komputerach w wewnętrznej sieci firmy.

Dotyczy to tylko wstępnej instalacji Agenta sieciowego. Jednakże jakiekolwiek późniejsze uaktualnienia Agenta sieciowego lub instalacja Kaspersky Anti-Virus mogą zostać wykonane przez Serwer administracyjny. Jednocześnie, wstępna instalacja Agentów sieciowych może odbyć się, na przykład, poprzez zasady grupy Microsoft® Active Directory®.

- Serwer administracyjny nie może wysyłać powiadomień na zarządzane komputery poprzez port UDP o numerze 15000, co nie jest krytyczne dla działania Kaspersky Security Center.
- Serwer administracyjny nie może przeszukiwać Active Directory. Jednakże w większości scenariuszy wyniki przeszukiwania Active Directory nie są wymagane.

Jeśli powyższe ograniczenia są postrzegane jako krytyczne, można je znieść przy pomocy Agentów aktualizacji znajdujących się wewnątrz sieci firmowej:

- Aby przeprowadzić wstępną instalację na komputerach bez Agenta sieciowego, w pierwszej kolejności zainstaluj Agenta sieciowego na jednym z komputerów, a następnie przypisz mu stan Agenta aktualizacji. W rezultacie, wstępna instalacja Agenta sieciowego na pozostałych komputerach zostanie przeprowadzona przez Serwer administracyjny poprzez tego Agenta aktualizacji.
- Aby wykrywać nowe komputery w wewnętrznej sieci firmy i przeszukiwać Active Directory, w jednym z Agentów aktualizacji musisz włączyć odpowiednie metody przeszukiwania sieci.
- Aby zapewnić pomyślne wysyłanie powiadomień poprzez port UDP o numerze 15000 na zarządzane komputery znajdujące się w wewnętrznej sieci firmy, musisz wypełnić całą swoją sieć Agentami aktualizacji, gdzie na jednego Agenta aktualizacji będzie przypadać od 100 do 200 komputerów. We właściwościach przydzielonych Agentów aktualizacji zaznacz pole **Nie odłączaj Serwera administracyjnego**. Serwer administracyjny nawiąże stale połączenie z Agentami aktualizacji, które będą mogły wysyłać powiadomienia poprzez port UDP o numerze 15000 na komputery w wewnętrznej sieci firmy (sekcja "Informacje o Agentach aktualizacji" na stronie 21).

Dostęp do internetu: Agent sieciowy w trybie bramy w strefie zdemilitaryzowanej (DMZ)

Tryb dostępu opisany poniżej jest stosowany do Kaspersky Security Center 10 Service Pack 1 i nowszych wersji.

Serwer administracyjny może znajdować się w wewnętrznej sieci firmy, w strefie zdemilitaryzowanej (DMZ), gdzie może być komputer z Agentem sieciowym działającym w trybie bramy z odwróconym połączeniem (Serwer administracyjny nawiązuje połączenie z Agentem sieciowym). W tym przypadku, w celu zapewnienia dostępu do internetu muszą zostać spełnione następujące warunki:

- Agent sieciowy musi być zainstalowany na komputerze znajdującym się w DMZ. Podczas instalacji Agenta sieciowego, w kroku **Brama połączenia** w Kreatorze instalacji wybierz **Użyj jako bramy połączenia**.
- Na Serwerze administracyjnym należy utworzyć dedykowaną grupę administracyjną, w której właściwościach należy przydzielić komputerowi DMZ stan bramy połączenia według adresu. Nie można dodawać do tej grupy administracyjnej żadnych komputerów.
- Dla Agentów sieciowych, które próbują uzyskać dostęp do Serwera administracyjnego poprzez internet, użyj opcji **Połącz z Serwerem administracyjnym przy użyciu bramy połączenia**, aby podczas instalacji określić nowo utworzoną bramę.

Dla bramy połączenia w strefie DMZ Serwer administracyjny tworzy certyfikat podpisany przez certyfikat Serwera administracyjnego. Jeśli administrator zdecyduje przydzielić Serwerowi administracyjnemu certyfikat niestandardowy, musi to zrobić przed utworzeniem bramy połączenia w strefie DMZ.

Jeśli niektórzy pracownicy korzystają z laptopów, które mogą łączyć się z Serwerem administracyjnym z sieci lokalnej lub poprzez internet, przydatne będzie utworzenie w profilu Agenta sieciowego reguły przełączania dla Agenta sieciowego.

Standardowa konfiguracja Kaspersky Security Center

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

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

W tej sekcji:

Standardowa konfiguracja: Jedno biuro

W sieci firmowej można zainstalować jeden lub kilka Serwerów administracyjnych. Liczbę Serwerów administracyjnych można określić na podstawie szczegółów dostępnego sprzętu (sekcja “Wymagania sprzętowe dla systemu zarządzania bazą danych i Serwera administracyjnego“ na stronie 138) lub całkowitej liczby hostów.

Jeden Serwer administracyjny może obsługiwać maksymalnie 50 000 komputerów. Należy rozważyć możliwość zwiększenia liczby zarządzanych komputerów w najbliższej przyszłości: wygodniejsze może być podłączenie do jednego Serwera administracyjnego mniejszej liczby komputerów.

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

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

Jeśli Serwer administracyjny obsługuje ponad 5 000 hostów, przydatne może być przypisanie stanu Agenta aktualizacji do komputerów w różnych segmentach sieci z liczbą od 100 do 200 zarządzanych komputerów dla jednego Agenta aktualizacji. Zmniejszy to obciążenie sieci i Serwera administracyjnego.

Zobacz również:

Określanie przestrzeni dyskowej dla Agenta aktualizacji 140

Ocenianie ilości ruchu między Agentem sieciowym a Serwerem administracyjnym 143

Informacje o Agentach aktualizacji 21

Hierarchia Serwerów administracyjnych 22

Standardowa konfiguracja: Duże oddziały posiadające swoich administratorów

Jeśli istnieje kilka oddziałów firmy, które są oddalone geograficznie od siebie, należy rozważyć opcję instalacji Serwera administracyjnego w każdym z tych biur - jeden lub kilka Serwerów na jedno biuro - w zależności od liczby komputerów klienckich i dostępnego sprzętu. W tym przypadku, dla każdego z biur można przeprowadzić "Standardową konfigurację: Jedno biuro". W celu ułatwienia zarządzania, wszystkie Serwery administracyjne powinny zostać połączone w hierarchię (najlepiej w wielopoziomową).

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

Zobacz również:

Standardowa konfiguracja: Małe zdalne biura

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

W głównej siedzibie należy zainstalować Serwer administracyjny, natomiast we wszystkich pozostałych biurach należy przydzielić jednego lub kilku Agentów aktualizacji. Jeśli biura są połączone przez internet, przydatne może być utworzenie zadania przekazania aktualizacji dla Agentów aktualizacji, aby mogły one pobierać uaktualnienia bezpośrednio z serwerów Kaspersky Lab, a nie z Serwera administracyjnego.

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

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

Serwer administracyjny nie będzie mógł wysyłać powiadomień poprzez port UDP o numerze 15000 na zarządzane komputery znajdujące się poza NAT w zdalnym biurze. Aby rozwiązać ten problem, we właściwościach komputerów pełniących rolę Agentów aktualizacji należy włączyć tryb

stałego połączenia z Serwerem administracyjnym (pole **Nie odłączaj Serwera administracyjnego**). Ten tryb jest dostępny, jeśli całkowita liczba Agentów aktualizacji nie przekracza 200.

Zobacz również:

Informacje o Agentach aktualizacji

Agent sieciowy może być używany jako Agent aktualizacji. W tym trybie Agent sieciowy może wykonywać następujące funkcje:

- Rozsyłać uaktualnienia (mogą być one pobierane z Serwera administracyjnego lub z serwerów Kaspersky Lab). Jeśli uaktualnienia są pobierane z serwerów Kaspersky Lab, zadanie przekazania aktualizacji musi zostać utworzone dla komputera, który pełni rolę Agenta aktualizacji.
- Instalować oprogramowanie (włączając w to wstępną instalację Agentów sieciowych) na pozostałych komputerach.
- Skanować sieć w celu odnalezienia nowych komputerów i zaktualizowania informacji o tych istniejących. Agent aktualizacji może stosować te same metody skanowania sieci co Serwer administracyjny.

Instalacja Agentów sieciowych w sieci firmowej realizuje następujące cele:

- Zmniejsza obciążenie na Serwerze administracyjnym.
- Optymalizuje ruch sieciowy.
- Zapewnia Serwerowi administracyjnemu dostęp do komputerów w ciężko dostępnych miejscach sieci firmowej. Dostępność Agenta aktualizacji w sieci poza NAT (w powiązaniu z Serwerem administracyjnym) umożliwia Serwerowi administracyjnemu wykonywanie następujących działań:

- Wysyłanie powiadomień na komputery poprzez protokół UDP.
- Skanowanie sieci.
- Przeprowadzanie wstępnej konfiguracji.

Agent aktualizacji jest przydzielony do grupy administracyjnej. W tym przypadku zakres działania Agenta aktualizacji obejmuje wszystkie komputery w grupie administracyjnej i jej podgrupach. Jednakże komputer pełniący funkcję Agenta aktualizacji może nie znajdować się w grupie administracyjnej, do której został przydzielony.

Agent aktualizacji może zostać wskazany jako brama połączenia. W tym przypadku komputery objęte zakresem działania Agenta aktualizacji będą łączyły się z Serwerem administracyjnym poprzez bramę, a nie bezpośrednio. Ten tryb może być przydatny w scenariuszach, które nie zezwalają na nawiązywanie bezpośredniego połączenia między komputerami a Agentem sieciowym i Serwerem administracyjnym.

Zobacz również:

Dostęp do internetu: Agent sieciowy w trybie bramy w strefie zdemilitaryzowanej (DMZ)..... 17

Standardowa konfiguracja: Małe zdalne biura 20

Tworzenie struktury grup administracyjnych i przydzielanie Agentów aktualizacji 50

Hierarchia Serwerów administracyjnych

W firmie może działać kilka Serwerów administracyjnych. Niewygodne może być zarządzanie kilkoma oddzielnymi Serwerami administracyjnymi, dlatego dobrym wyjściem jest utworzenie hierarchii. Zastosowanie konfiguracji nadrzędny-podrzędny dla dwóch Serwerów administracyjnych oferuje następujące możliwości:

- Podrzędny Serwer administracyjny dziedziczy profile i zadania od nadrzędnego Serwera administracyjnego, zapobiegając dzięki temu powielaniu ustawień.
- Zbiory wybranych komputerów na nadrzędnym Serwerze administracyjnym mogą zawierać komputery z podrzędnych Serwerów administracyjnych.

- Raporty na nadrzędnym Serwerze administracyjnym mogą zawierać dane (w tym szczegółowe informacje) z podrzędnych Serwerów administracyjnych.

Wirtualne Serwery administracyjne

W oparciu o fizyczny Serwer administracyjny można utworzyć kilka wirtualnych Serwerów administracyjnych, które będą podobne do podrzędnych Serwerów administracyjnych.
W przeciwieństwie do trybu poufnego dostępu, który jest oparty na listach kontroli dostępu (ACL), tryb wirtualnego Serwera administracyjnego jest bardziej funkcjonalny i zapewnia większy stopień izolacji. Oprócz dedykowanej struktury grup administracyjnych dla przypisanych komputerów z profilami i zadaniami, każdy wirtualny Serwer administracyjny posiada swoją własną grupę nieprzypisanych komputerów, swój własny zbiór raportów, wybranych komputerów i zdarzeń, pakietów instalacyjnych, reguł przenoszenia itd. Zasięg działania wirtualnego Serwera administracyjnego może być wykorzystany przez dostawców usług (xSP) do zwiększenia izolacji klientów, a także przez organizacje działające na szeroką skalę z zaawansowanym przepływem pracy i dużą liczbą administratorów.

Wirtualne Serwery administracyjne są bardzo podobne do podrzędnych Serwerów administracyjnych, jednakże posiadają pewne różnice:

- Wirtualny Serwer administracyjny nie posiada większości ustawień globalnych i swoich własnych portów TCP.
- Wirtualny Serwer administracyjny nie posiada podrzędnych Serwerów administracyjnych.
- Wirtualny Serwer administracyjny nie posiada innych wirtualnych Serwerów administracyjnych.
- Fizyczny Serwer administracyjny wyświetla komputery, grupy, zdarzenia i obiekty na zarządzanych komputerach (elementy w Kwarantannie, rejestrze aplikacji itd.) ze wszystkich swoich wirtualnych Serwerów administracyjnych.
- Wirtualny Serwer administracyjny może skanować sieć wyłącznie przy podłączonych Agentach aktualizacji.

Instalowanie obrazów systemów operacyjnych

Kaspersky Security Center umożliwia instalację obrazów WIM pulpitu i serwerowych systemów operacyjnych Windows® na komputerach w sieci firmowej.

W celu uzyskania obrazu systemu operacyjnego, który będzie mógł zostać zainstalowany przy użyciu narzędzi Kaspersky Security Center:

- Zaimportuj obraz z pliku install.wim znajdującego się w pakiecie dystrybucyjnym systemu Windows
- Przechwyć obraz z komputera odniesienia.

Dla instalacji obrazów systemu operacyjnego są obsługiwane dwa scenariusze:

- Instalacja na "czystym" komputerze, na którym nie ma zainstalowanego systemu operacyjnego.
- Instalacja na komputerze działającym pod kontrolą systemu Windows.

Serwer administracyjny zawiera obraz środowiska preinstalacyjnego systemu Windows (Windows PE), który jest zawsze używany do przechwytywania obrazów systemu operacyjnego oraz do ich instalowania. Wszystkie sterowniki niezbędne do właściwego funkcjonowania wszystkich komputerów docelowych muszą zostać dodane do obrazu WinPE. Zazwyczaj też należy dodać sterowniki mikroukładu, aby interfejs sieci Ethernet działał poprawnie.

W celu zaimplementowania scenariuszy przechwytywania i instalacji obrazu muszą być spełnione następujące warunki:

- Na Serwerze administracyjnym musi być zainstalowany Zestaw zautomatyzowanej instalacji systemu Windows (Windows WAIK) w wersji 2.0 (lub nowszej) bądź Zestaw do oceny i wdrażania systemu Windows (Windows WADK). Jeśli scenariusz przewiduje instalowanie i przechwytywanie obrazów na systemie Windows XP, należy zainstalować Windows WAIK.
- W sieci, w której znajduje się komputer docelowy, musi być dostępny serwer DHCP.

- Folder współdzielony Serwera administracyjnego musi być otwarty do odczytu z poziomu sieci, w której znajduje się komputer docelowy. Jeśli folder współdzielony znajduje się na Serwerze administracyjnym, należy nadać kontu KlPxeUser uprawnienia dostępu. Jeśli folder współdzielony znajduje się poza Serwerem administracyjnym, uprawnienie dostępu musi zostać nadane każdemu.

Podczas wybierania instalowanego obrazu systemu operacyjnego administrator musi wyraźnie określić architekturę procesora komputera docelowego: x86 lub x86-64.

Zarządzanie urządzeniami mobilnymi

W tej sekcji:

Serwer urządzeń mobilnych Exchange ActiveSync

Serwer urządzeń mobilnych Exchange ActiveSync® umożliwia zarządzanie urządzeniami mobilnymi, które są połączone z Serwerem administracyjnym za pomocą protokołu Exchange ActiveSync (urządzenia EAS).

W tej sekcji:

Instalowanie serwera urządzeń mobilnych Exchange ActiveSync

Jeśli w organizacji zainstalowano kilka serwerów Microsoft Exchange z obrębu macierzy serwera dostępu klienta, na każdym serwerze w tej macierzy należy zainstalować serwer urządzeń mobilnych Exchange ActiveSync. W kreatorze instalacji serwera urządzeń mobilnych Exchange ActiveSync włącz opcję **Cluster mode**. W tym przypadku zestaw serwerów urządzeń mobilnych Exchange ActiveSync zainstalowanych na serwerach w macierzy będzie określany jako klaster serwerów urządzeń mobilnych Exchange ActiveSync.

Jeśli w organizacji nie zainstalowano żadnej macierzy serwera dostępu klienta Microsoft Exchange Servers, serwer urządzeń mobilnych Exchange ActiveSync musi zostać zainstalowany na serwerze Microsoft Exchange Server, na którym jest dostęp klienta. W tym przypadku, w kreatorze instalacji serwera urządzeń mobilnych Exchange ActiveSync włącz opcję **Standard mode**.

Wraz z serwerem urządzeń mobilnych Exchange ActiveSync należy zainstalować Agenta sieciowego, gdyż pomoże to zintegrować serwer urządzeń mobilnych Exchange ActiveSync z Kaspersky Security Center.

Domyślnym obszarem skanowania serwera urządzeń mobilnych Exchange ActiveSync jest bieżąca domena Active Directory, w której został zainstalowany. Instalowanie serwera urządzeń mobilnych Exchange ActiveSync na serwerze z zainstalowanym serwerem Microsoft Exchange Server (wersje 2010, 2013) umożliwia rozszerzenie obszaru skanowania w celu uwzględnienia całego lasu domen na serwerze urządzeń mobilnych Exchange ActiveSync (sekcja "Konfigurowanie obszaru skanowania" na stronie 129). Podczas skanowania wymagane są informacje o kontach użytkowników serwera Microsoft Exchange, profilach Exchange ActiveSync

oraz urządzeniach mobilnych użytkowników podłączonych do serwera Microsoft Exchange Server poprzez protokół Exchange ActiveSync.

W jednej domenie nie można zainstalować kilku serwerów urządzeń mobilnych Exchange ActiveSync, jeśli działają w **trybie standardowym** i są zarządzane przez jeden Serwer administracyjny.

W obrębie jednego lasu domeny Active Directory nie można zainstalować kilku serwerów urządzeń mobilnych Exchange ActiveSync (lub kilku klastrów serwerów urządzeń mobilnych Exchange ActiveSync), jeśli działają w **trybie standardowym** z rozszerzonym obszarem skanowania, który zawiera cały las domen, i jeśli są połączone z jednym Serwerem administracyjnym.

Zobacz również:

Instalowanie serwera urządzeń mobilnych Exchange ActiveSync 102

Konfigurowanie obszaru skanowania 129

Uprawnienia wymagane do zainstalowania serwera urządzeń mobilnych Exchange ActiveSync

Instalacja serwera urządzeń mobilnych Exchange ActiveSync na serwerze Microsoft Exchange Server (2010, 2013) wymaga uprawnień administratora domeny i roli Zarządzanie organizacją. Instalacja serwera urządzeń mobilnych Exchange ActiveSync na serwerze Microsoft Exchange Server (2007) wymaga uprawnień administratora domeny i członkostwa w grupie zabezpieczeń Administratorzy organizacji programu Exchange.

Konto dla usługi Exchange ActiveSync

Po zainstalowaniu serwera urządzeń mobilnych Exchange ActiveSync, w Active Directory automatycznie tworzone jest konto:

- Na serwerze Microsoft Exchange Server (2010, 2013): Konto KLMDM4ExchAdmin***** z rolą KLMDM Role Group
- Na serwerze Microsoft Exchange Server (2007): Konto KLMDM4ExchAdmin***** należące do grupy zabezpieczeń KLMDM Secure Group.

Usługa serwera urządzeń mobilnych Exchange ActiveSync jest uruchamiana z poziomu tego konta.

Jeśli chcesz anulować automatyczne tworzenie konta, musisz utworzyć niestandardowe konto z następującymi uprawnieniami:

- Podczas korzystania z serwera Microsoft Exchange Server (2010, 2013) do konta musi zostać przypisana rola, która może wykonywać następujące polecenia cmdlet:
  - Get-CASMailbox
  - Set-CASMailbox
  - Remove-ActiveSyncDevice
  - Clear-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Get-AcceptedDomain
  - Set-AdServerSettings
  - Get-ActiveSyncMailboxPolicy
  - New-ActiveSyncMailboxPolicy
  - Set-ActiveSyncMailboxPolicy
  - Remove-ActiveSyncMailboxPolicy
- Podczas korzystania z serwera Microsoft Exchange Server (2007) konto musi posiadać uprawnienia dostępu do obiektów Active Directory (patrz poniższa tabela).

Tabela 2. Uprawnienia dostępu do obiektów Active Directory

Dostęp	Obiekt	Cmdlet
Pełny	Thread "CN=Mobile Mailbox Policies,CN=<Nazwa organizacji>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nazwa domeny>"	`Add-ADPermission -User <Nazwa grupy lub użytkownika> -Identity "CN=Mobile Mailbox Policies,CN=<Nazwa organizacji>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nazwa domeny>" -InheritanceType All -AccessRight GenericAll`
Odczyt	Thread "CN=<Nazwa organizacji>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nazwa domeny>"	`Add-ADPermission -User <Nazwa domeny> -Identity "CN=<Nazwa organizacji>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nazwa domeny>" -InheritanceType All -AccessRight GenericRead`
Odczyt/ zapis	Właściwości msExchMobileMailboxPolicyLink i msExchOmaAdminWirelessEnable dla obiektów w Active Directory	`Add-ADPermission -User <Nazwa grupy lub użytkownika> -Identity "DC=<Nazwa domeny>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable`

Dostęp	Obiekt	Cmdlet
Rozszerzone uprawnienia ms-Exch-Store-Active	Mailbox repositories of Exchange server, thread "CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<Nazwa organizacji>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nazwa domeny>"	`Get-MailboxDatabase | Add-ADPermission -User <Nazwa użytkownika lub grupy> -ExtendedRights ms-Exch-Store-Admin`

Serwer urządzeń mobilnych iOS MDM

Serwer urządzeń mobilnych iOS MDM umożliwia zarządzanie urządzeniami iOS poprzez zainstalowane na nich profile iOS MDM. Obsługiwane są następujące funkcje:

- Blokowanie urządzenia
- Resetowanie hasła
- Usuwanie danych
- Instalowanie i dezinstalowanie aplikacji
- Użycie profilu iOS MDM z ustawieniami zaawansowanymi (np. ustawienia VPN, ustawienia e-mail, ustawienia Wi-Fi, ustawienia aparatu, certyfikaty itd.).

Serwer urządzeń mobilnych iOS MDM jest usługą sieciową odbierającą połączenia przychodzące z urządzeń mobilnych poprzez swój protokół TLS (domyślne jest to port 443), która jest zarządzana poprzez Kaspersky Security Center przy użyciu Agenta sieciowego. Agent sieciowy jest instalowany lokalnie, na komputerze z zainstalowanym serwerem urządzeń mobilnych iOS MDM.

Podczas instalacji serwera urządzeń mobilnych iOS MDM administrator musi wykonać następujące czynności:

- Zapewnić Agentowi sieciowemu dostęp do Serwera administracyjnego

- Zapewnić urządzeniom mobilnym dostęp do portu TCP serwera urządzeń mobilnych iOS MDM.

Ta sekcja przedstawia dwie standardowe konfiguracje serwera urządzeń mobilnych iOS MDM.

W tej sekcji:

Standardowa konfiguracja: Kaspersky Mobile Device Management w strefie DMZ

Serwer urządzeń mobilnych iOS MDM znajduje się w strefie zdemilitaryzowanej (DMZ) sieci lokalnej firmy z dostępem do internetu. Specjalną funkcją tej konfiguracji jest brak jakichkolwiek problemów podczas uzyskiwania dostępu do usługi sieciowej iOS MDM z poziomu urządzeń, przez internet.

Ponieważ zarządzanie serwerem urządzeń mobilnych iOS MDM wymaga zainstalowania Agenta sieciowego lokalnie, należy zapewnić interakcję Agenta sieciowego z Serwerem administracyjnym. Można to zrobić przy użyciu jednej z następujących metod:

- Przenieś Serwer administracyjny do strefy DMZ.
- Użyj bramy połączenia (sekcja "Dostęp do internetu: Agent sieciowy w trybie bramy w strefie zdemilitaryzowanej (DMZ)" na stronie 17):

    a. Na komputerze z zainstalowanym serwerem urządzeń mobilnych iOS MDM połącz Agenta sieciowego z Serwerem administracyjnym poprzez bramę połączenia.

    b. Na komputerze z zainstalowanym serwerem urządzeń mobilnych iOS MDM wskaż Agenta sieciowego jako bramę połączenia.

Zobacz również:

Uproszczony schemat instalacji 105

Standardowa konfiguracja: serwer urządzeń mobilnych iOS MDM w sieci lokalnej firmy

Serwer urządzeń mobilnych iOS MDM znajduje się w wewnętrznej sieci firmy. Aby umożliwić dostęp z zewnątrz, należy włączyć port 443 (domyślny port). Można to zrobić, na przykład, publikując usługę sieciową iOS MDM na Microsoft Forefront® Threat Management Gateway (zwany dalej TMG) (sekcja "Schemat łączenia urządzeń KES z Serwerem wykorzystujący delegowanie protokołu Kerberos (KCD)" na stronie 111).

Każda standardowa konfiguracja wymaga dla serwera urządzeń mobilnych iOS MDM dostępu do usług sieciowych Apple (zakres 17.0.0.0/8) poprzez port TCP 2195. Ten port jest używany do powiadamiania urządzeń o nowych poleceniach przy użyciu dedykowanej usługi o nazwie APN (sekcja “Konfigurowanie dostępu do usługi Apple Push Notification“ na stronie 108).

Zarządzanie urządzeniami mobilnymi z zainstalowanym programem Kaspersky Endpoint Security for Android

Urządzenia mobilne z zainstalowanym programem Kaspersky Endpoint Security for Android™ (zwane dalej "urządzenia KES") są zarządzane przy użyciu Serwera administracyjnego. Kaspersky Security Center 10 Service Pack 1 (SP1) obsługuje następujące funkcje zarządzania urządzeniami KES:

- Zarządzanie urządzeniami mobilnymi jak komputerami klienckimi:
  - Członkostwo w grupach administracyjnych
  - Stany, zdarzenia, raporty itd.

    - Modyfikowanie ustawień lokalnych i przydzielanie profili dla Kaspersky Endpoint Security for Android
- Wysyłanie poleceń w sposób scentralizowany
- Zdalne instalowanie pakietów aplikacji mobilnych.

Urządzenia KES są zarządzane przez Serwer administracyjny poprzez port TLS, TCP 13292.

Zobacz również:

Umożliwianie uzyskania dostępu do Serwera administracyjnego przez internet 14

Określanie certyfikatu Serwera administracyjnego 41

Informacje o Network Access Control (NAC)

Domyślnie Network Access Control (NAC) został zaprojektowany do gromadzenia i zarządzania informacjami o dostępie do sieci Ethernet, który został nadany urządzeniom. Korzystając z NAC, możesz pobrać kilka podstawowych ustawień sieciowych urządzeń, na przykład ich adresy MAC, adresy IP, nazwy NetBIOS i pewne ustawienia zaawansowane, zdefiniowane podczas aktywnego skanowania: wersję systemu operacyjnego, typ urządzenia, listę otwartych portów sieciowych itd.

Utworzenie profili przydzielających prawa dostępu umożliwia zdefiniowanie kryteriów i reguł, które zostaną użyte do nadania urządzeniu pełnego lub częściowego dostępu do zasobów sieciowych lub do nie nadania żadnego dostępu. Zestaw kryteriów użytych do opisania jednego lub kilku urządzeń nosi nazwę *obiekt sieciowy*. Kryteria obiektu sieciowego obejmują podstawowe ustawienia sieci, a także ustawienia zaawansowane, zdefiniowane podczas aktywnego skanowania. Natomiast reguły określają typ dostępu do zasobów sieciowych, który zostanie udzielony urządzeniom (jeśli spełniają odpowiednie kryteria).

Agenty sieciowe sprawdzają dostęp urządzeń do sieci i stosują profile. Agent sieciowy z włączoną funkcją NAC jest nazywany *Agentem NAC*. Do poprawnego działania NAC wymagany jest jeden aktywny Agent NAC w każdej domenie rozgłoszeniowej znajdującej się w sieci. Na przykład, jeśli

sieć 50 000 urządzeń zawiera 50 domen rozgłoszeniowych, z których każda wymaga jednego aktywnego Agenta NAC, co daje w sumie 50 aktywnych Agentów NAC. *Agent NAC jest aktywny, jeśli działa w trybie głównym*. Jeśli aktywny Agent NAC nie może działać poprawnie (na przykład, gdy komputer jest uruchamiany ponownie), zapasowy Agent NAC (który zazwyczaj działa w trybie Rezerwacja) może przejąć funkcje aktywnego Agenta NAC. Zapasowy Agent NAC (jeśli jest dostępny) musi działać w tej samej domenie rozgłoszeniowej co główny Agent.

Agenty NAC używają technologii monitorowania aktywnego portu zwanej Nmap i dlatego, jeśli najbardziej popularne porty są zamknięte na urządzeniu, wyniki skanowania mogą nie być dokładne lub w ogóle może ich nie być.

Bieżąca implementacja obejmuje funkcję NAC uwzględnioną w programie Kaspersky Security Center i jest oparta na technologiach analizy i manipulacji ruchem po protokole ARP. Jeśli NAC działa w trybie "Symulacja", tylko analiza ruchu po protokole ARP jest używana (nie jest stosowana manipulacja ruchem po protokole ARP).

Z powodu ograniczeń nałożonych przez protokół ARP, wszelkie działania Agenta NAC nie wyjdą poza domenę rozgłoszeniową. Z reguły domena ta jest ograniczona przez ruter. Korzystanie z NAC wymaga odłączenia ochrony przed atakami ARP spoofing skierowanymi na rutery.

Aktualnie sieci IEEE 802.11 (Wi-Fi) nie są obsługiwane.

Zobacz również:

Konfigurowanie i korzystanie z NAC 118

NAC: Zdarzenia i standardowe scenariusze 133

Problemy związane z Network Access Control (NAC) 158

Instalacja i wstępna konfiguracja

Kaspersky Security Center zawiera następujące aplikacje:

- Serwer administracyjny—główny komponent, zaprojektowany do zarządzania komputerami w firmie i przechowywania danych w DBMS.
- Konsola administracyjna—podstawowe narzędzie administratora. Konsola administracyjna jest dostarczana wraz z Serwerem administracyjnym, ale można ją także zainstalować oddzielnie na jednym lub kilku komputerach administratora.
- Agent sieciowy—zaprojektowany do zarządzania aplikacją antywirusową zainstalowaną na komputerze, a także do zbierania informacji o tym komputerze. Agenty sieciowe są instalowane na komputerach w firmie.

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

- Instalacja Serwera administracyjnego
- Instalacja niestandardowa Konsoli administracyjnej na komputerze administratora
- Instalacja Agenta sieciowego i aplikacji antywirusowej na komputerach w firmie.

W tej sekcji:

Instalowanie Serwera administracyjnego

Ta sekcja zawiera zalecenia dotyczące instalacji Serwera administracyjnego na komputerze. Opisane są tu także scenariusze korzystania z folderu współdzielonego na komputerze z Serwerem administracyjnym w celu zainstalowania Agenta sieciowego na komputerach klienckich.

W tej sekcji:

Tworzenie kont dla usług Serwera administracyjnego

Domyślnie instalator automatycznie tworzy konta bez uprawnień dla usług Serwera administracyjnego. To zachowanie jest najbardziej praktyczne podczas instalacji Serwera administracyjnego na zwykłym komputerze.

Jednakże instalacja Serwera administracyjnego na kontrolerze domeny lub klastrze typu failover wymaga innego scenariusza:

1. W Active Directory utwórz globalne grupy domeny o nazwach: KLAdmins i KLOperators.
2. Dla usług Serwera administracyjnego utwórz konta domenowe bez uprawnień i przydziel je do globalnej grupy zabezpieczeń w domenie o nazwie KLAdmins.
3. W instalatorze Serwera administracyjnego określ utworzone konta domenowe.

Wybieranie systemu zarządzania bazą danych

Podczas instalacji Serwera administracyjnego można wybrać system zarządzania bazą danych, którego będzie używał Serwer administracyjny. Możesz zainstalować SQL Server Express Edition znajdujący się w pakiecie dystrybucyjnym lub wybrać istniejący system zarządzania bazą danych DBMS. Poniższa tabela wyświetla listę prawidłowych opcji systemu DBMS, a także ograniczeń dotyczących ich użycia.

Tabela 3. Ograniczenia dotyczące systemu DBMS

DBMS	Ograniczenia
SQL Server Express Edition znajdujący się w pakiecie dystrybucyjnym Kaspersky Security Center	Zalecane jest unikanie przydzielania 10 000 komputerów do jednego Serwera administracyjnego.
Lokalny serwer SQL Server inny niż Express	Brak ograniczeń.

DBMS	Ograniczenia
Zdalny serwer SQL Server inny niż Express	Działa, jeśli oba komputery są w tej samej domenie Windows. Jeśli domeny są inne, należy nawiązać między nimi obustronną relację zaufania.
Lokalny lub zdalny MySQL 5.0	Serwer administracyjny może obsługiwać maksymalnie 10 000 komputerów.

Jednoczesne korzystanie z systemu DBMS serwera SQL Server Express Edition przez Serwer administracyjny i inną aplikację jest surowo zabronione.

Zobacz również:

Wybieranie systemu zarządzania bazą danych (DBMS) dla Serwera administracyjnego 14

Określanie folderu współdzielonego

Podczas instalacji Serwera administracyjnego możesz określić lokalizację folderu współdzielonego. Określenie lokalizacji folderu współdzielonego jest także możliwe po instalacji, we właściwościach Serwera administracyjnego. Domyślnie folder współdzielony zostanie utworzony na komputerze z zainstalowanym Serwerem administracyjnym (z uprawnieniami do odczytu dla podgrupy **Wszyscy**). Jednakże w niektórych przypadkach (duże obciążenie sieci, konieczność uzyskania dostępu z odizolowanej sieci itd.) przydatne może być umiejscowienie folderu współdzielonego w dedykowanym zasobie plików.

Folder współdzielony jest sporadycznie używany podczas instalacji Agenta sieciowego.

W tej sekcji:

Zdalna instalacja przy użyciu narzędzi Serwera administracyjnego poprzez profile grupy Active Directory

Jeśli komputery docelowe znajdują się w domenie systemu Windows (bez grup roboczych), wstępna instalacja (instalacja Agenta sieciowego i aplikacji antywirusowej na komputerach, które nie są jeszcze zarządzane) musi zostać przeprowadzona poprzez profile grupy Active Directory. Instalacja odbywa się przy użyciu standardowego zadania zdalnej instalacji z programu Kaspersky Security Center. W przypadku sieci dużej skali, dobrym rozwiązaniem jest umieszczenie folderu współdzielonego w dedykowanym zasobie plików w celu zmniejszenia obciążenia podsystemu dyskowego komputera z Serwerem administracyjnym.

Zdalna instalacja poprzez dostarczenie ścieżki UNC do pakietu autonomicznego

Jeśli użytkownicy komputerów w sieci firmowej posiadają uprawnienia administratora lokalnego, stosowana jest inna metoda wstępnej instalacji - poprzez utworzenie autonomicznego pakietu Agenta sieciowego (lub nawet pakietu Agenta sieciowego połączonego z aplikacją antywirusową). Po utworzeniu pakietu autonomicznego należy wysłać do użytkowników odsyłacz do tego pakietu, który jest przechowywany w folderze współdzielonym. Instalacja rozpocznie się w momencie, gdy użytkownik kliknie odsyłacz.

Aktualizowanie z folderu współdzielonego Serwera administracyjnego

W zadaniu aktualizacji aplikacji antywirusowej możesz skonfigurować aktualizację z folderu współdzielonego Serwera administracyjnego. Jeśli zadanie zostało przypisane do dużej liczby komputerów, dobrym rozwiązaniem będzie umieszczenie folderu współdzielonego w dedykowanym zasobie plików.

Instalowanie obrazów systemów operacyjnych

Instalacja obrazów systemów operacyjnych zawsze odbywa się poprzez folder współdzielony Serwera administracyjnego: komputery docelowe pobierają obrazy systemów operacyjnych z tego folderu. Jeśli instalacja obrazów została zaplanowana na dużej liczbie komputerów firmowych, dobrym rozwiązaniem będzie umieszczenie folderu współdzielonego w dedykowanym zasobie plików.

Zobacz również:

Instalowanie Agenta sieciowego i aplikacji antywirusowej 63

Określanie adresu Serwera administracyjnego

Podczas instalacji Serwera administracyjnego możesz określić adres komputera, na którym znajduje się Serwer administracyjny. Podczas tworzenia pakietów instalacyjnych Agenta sieciowego ten adres będzie używany jako domyślny. Domyślnie używana jest nazwa NetBIOS komputera z Serwerem administracyjnym. Jeśli serwer DNS (Domain Name System) w sieci firmowej został skonfigurowany i działa poprawnie, należy określić w DNS nazwę FQDN komputera z Serwerem administracyjnym. Jeśli Serwer administracyjny jest zainstalowany w strefie DMZ, pomocne może się okazać określenie zewnętrznego adresu komputera z Serwerem administracyjnym. Wówczas możliwa będzie zmiana adresu komputera z Serwerem administracyjnym przy użyciu narzędzi Konsoli administracyjnej; adres nie zostanie zmieniony automatycznie w już utworzonych pakietach instalacyjnych Agenta sieciowego.

Zobacz również:

Dostęp do internetu: Serwer administracyjny w strefie zdemilitaryzowanej (DMZ)..... 15

Określanie certyfikatu Serwera administracyjnego

Jeśli jest to konieczne, możesz przypisać specjalny certyfikat do Serwera administracyjnego, korzystając z narzędzia wiersza polecenia klsetsrvcert.

Podczas zamiany certyfikatu, wszystkie Agenty sieciowe, które wcześniej były połączone z Serwerem administracyjnym za pomocą protokołu SSL, utracą połączenie i zwrócą "Błąd autoryzacji Serwera administracyjnego".

Należy zauważyć, że certyfikat Serwera administracyjnego jest często dodawany do pakietów Agenta sieciowego podczas ich tworzenia. W takim przypadku, zastąpienie certyfikatu Serwera administracyjnego przy użyciu narzędzia klsetsrvcert nie spowoduje zamiany certyfikatu Serwera administracyjnego w istniejących pakietach Agenta sieciowego.

Dobrym rozwiązaniem jest zastąpienie certyfikatu natychmiast po zainstalowaniu Serwera administracyjnego, a przed zakończeniem działania Kreatora wstępnej konfiguracji.

Więcej informacji o warunkach, które wymagają zastąpienia certyfikatu można znaleźć w sekcji "Planowanie instalacji z uwzględnieniem struktury organizacyjnej firmy i topologii sieci (sekcja "Planowanie instalacji Kaspersky Security Center" na stronie 12).

Aby zamienić certyfikat, należy utworzyć nowy (na przykład przy użyciu klucza publicznego firmy) w formacie PKCS#12 i przekazać narzędziu klsetsrvcert (zapoznaj się z poniższą tabelą w celu sprawdzenia wartości ustawień narzędzia).

Składnia wiersza poleceń narzędzia:

klsetsrvcert [-l PLIKRAPORTU] -t TYP [-p HASŁO] -i PLIK

Tabela 4. Wartości ustawień narzędzia klsetsrvcert

Ustawienie	Wartość
-t TYP	Typ zastępowanego certyfikatu. Możliwe wartości ustawienia TYP: • C – podmienia certyfikat dla portów 13000 i 13291; • CR – podmienia rezerwowy certyfikat dla portów 13000 i 13291; • M – podmienia certyfikat dla urządzeń mobilnych na porcie 13292.
-i PLIK	Kontener z certyfikatem w formacie PKCS#12 (plik z rozszerzeniem .p12 lub .pfx).
-p HASŁO	Hasło używane do ochrony kontenera .p12 z certyfikatem.
-l PLIKRAPORTU	Zapisuje dane wynikowe. Domyślnie dane wynikowe są przekierowywane do standardowego strumienia wyjściowego.

Wstępna konfiguracja

Po zakończeniu instalacji Serwera administracyjnego, zostaje uruchomiona Konsola administracyjna, która oferuje przeprowadzenie wstępnej konfiguracji przy użyciu odpowiedniego kreatora. Jeśli Kreator wstępnej konfiguracji jest uruchomiony, w głównej grupie administracyjnej tworzone są następujące profile i zadania:

- Profil Kaspersky Endpoint Security
- Grupowe zadanie aktualizacji Kaspersky Endpoint Security
- Grupowe zadanie skanowania komputera z zainstalowanym programem Kaspersky Endpoint Security
- Profil Agenta sieciowego
- Zadanie wykrywania luk (zadanie Agenta sieciowego)

- Zadanie instalacji uaktualnień i naprawy luk (zadanie Agenta sieciowego).

Profile i zadania są tworzone z domyślnymi ustawieniami, które mogą okazać się nieoptymalne lub nawet niedopuszczalne dla organizacji. Dlatego też należy sprawdzić właściwości utworzonych obiektów i zmodyfikować je ręcznie (jeśli zajdzie taka konieczność).

Ta sekcja zawiera informacje dotyczące wstępnej konfiguracji profili, zadań i innych parametrów Serwera administracyjnego.

W tej sekcji:

Ręczna konfiguracja profilu Kaspersky Endpoint Security

W tej sekcji można znaleźć zalecenia dotyczące konfiguracji profilu Kaspersky Endpoint Security, który jest tworzony przez Kreator wstępnej konfiguracji programu Kaspersky Security Center. Konfiguracja jest przeprowadzana w oknie właściwości profilu.

Podczas modyfikowania ustawień należy pamiętać o kliknięciu ikony blokady nad odpowiednim ustawieniem, aby umożliwić jego użycie na stacji roboczej.

W tej sekcji:

Konfigurowanie profilu w sekcji Ochrona antywirusowa

Poniżej opisano dodatkowe działania, które zalecamy wykonać w oknie właściwości profilu programu Kaspersky Endpoint Security, w sekcji **Ochrona antywirusowa**.

Sekcja Ochrona antywirusowa, podsekcja Zapora sieciowa

Sprawdź listę sieci we właściwościach profilu. Lista może nie zawierać wszystkich sieci.

► *W celu sprawdzenia listy sieci:*

1. W oknie właściwości profilu odszukaj sekcję **Ochrona antywirusowa** i wybierz podsekcję **Zapora sieciowa**.
2. W sekcji **Dostępne sieci** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno **Zapora sieciowa**. W tym oknie, na zakładce **Sieci** wyświetlana jest lista sieci.

Sekcja Ochrona antywirusowa, podsekcja Ochrona plików

Włączenie skanowania dysków sieciowych może spowodować znaczne obciążenie dysków sieciowych. Praktyczniejsze jest wykonywanie bezpośredniego skanowania na serwerach plików.

► *W celu wyłączenia skanowania dysków sieciowych:*

1. W oknie właściwości profilu odszukaj sekcję **Ochrona antywirusowa** i wybierz podsekcję **Ochrona plików**.

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

3. W otwartym oknie **Ochrona plików**, na zakładce **Ogólne** odznacz pole **Wszystkie dyski sieciowe**.

Konfigurowanie profilu w sekcji Ustawienia zaawansowane

Poniżej opisano zaawansowane działania, które zalecamy wykonać w oknie właściwości profilu programu Kaspersky Endpoint Security, w sekcji **Ustawienia zaawansowane**.

Sekcja Ustawienia zaawansowane, podsekcja Raporty i powiadomienia

W sekcji **Informuj Serwer administracyjny** zwróć uwagę na następujące ustawienia:

- Pole **Informacje o wykrytych lukach**: To ustawienie jest wymagane przede wszystkim do zapewnienia wstecznej kompatybilności z Kaspersky Security Center 9. Wykrywanie luk jest zintegrowane z Kaspersky Security Center, począwszy od wersji 10. Dlatego, jeśli korzystasz z Serwera administracyjnego i Agentów sieciowych w wersji 10 lub nowszej, upewnij się, że to pole jest odznaczone.

- Pole **Informacje o uruchomionych aplikacjach**: Jeśli to pole jest zaznaczone, bazy danych Serwera administracyjnego zapisują informacje o wszystkich wersjach wszystkich modułów aplikacji na komputerach w sieci firmowej. Informacje mogą wymagać znaczącej ilości miejsca na dysku dla bazy danych Kaspersky Security Center (kilkadziesiąt gigabajtów). Dlatego, jeśli pole **Informacje o uruchomionych aplikacjach** jest cały czas zaznaczone w profilu o najwyższym poziomie, musi ono zostać odznaczone.

Sekcja Ustawienia zaawansowane, podsekcja Interfejs

Jeśli ochrona antywirusowa w sieci firmowej musi być zarządzana w sposób scentralizowany poprzez Konsolę administracyjną, musisz wyłączyć wyświetlanie interfejsu Kaspersky Endpoint Security na stacjach roboczych (odznaczając pole **Wyświetl interfejs aplikacji** w sekcji **Interakcja**

z użytkownikiem) oraz włączyć ochronę hasłem (zaznaczając pole **Włącz ochronę hasłem** w sekcji **Ochrona hasłem**).

Sekcja Ustawienia zaawansowane, podsekcja Ustawienia KSN

Należy włączyć korzystanie z KSN Proxy (zaznaczając pole **Użyj serwera KSN Proxy**), gdyż w znacznym stopniu zwiększy to niezawodność wykrywania złośliwych programów.

Konfigurowanie profilu w sekcji Zdarzenia

W sekcji **Zdarzenia** należy wyłączyć zapisywanie wszelkich zdarzeń na Serwerze administracyjnym, za wyjątkiem następujących zdarzeń:

- Na zakładce **Informacje**:
  - Wyleczony obiekt
  - Usunięty obiekt
  - Zablokowane uruchomienie aplikacji w trybie testowym
  - Obiekt przeniesiony do Kwarantanny
  - Obiekt przywrócony z Kwarantanny
  - Utworzona kopia zapasowa obiektu.
- Na zakładce **Ostrzeżenie**:
  - Autoochrona jest wyłączona
  - Składniki ochrony są wyłączone
  - Niepoprawny zapasowy kod aktywacyjny
  - Użytkownik zrezygnował z profilu szyfrowania
  - Zażalenie dotyczące zablokowania uruchomienia aplikacji
  - Zażalenie dotyczące blokady dostępu do urządzenia

- Zażalenie dotyczące blokady dostępu do zawartości strony internetowej
- Wykryto aplikację, która może zostać użyta przez cyberprzestępców.

- Na zakładce **Błąd funkcjonalny**:
  - Błąd ustawień zadania Ustawienia nie zostały zastosowane
- Na zakładce **Zdarzenie krytyczne**:
  - Automatyczne uruchamianie aplikacji jest wyłączone
  - Dostęp został zablokowany
  - Zablokowane
  - Zablokowano uruchomienie aplikacji
  - Leczenie nie jest możliwe
  - Naruszono warunki Umowy licencyjnej
  - Nie można załadować modułu szyfrującego
  - Nie można uruchomić dwóch zadań jednocześnie
  - Wykryto prawdopodobnie zainfekowany obiekt
  - Wykryto szkodliwy obiekt
  - Wykryto aktywne zagrożenie Należy uruchomić zaawansowane leczenie
  - Wykryto wcześniej otwarty odnośnik phishingowy
  - Wykryto wcześniej otwarty szkodliwy odnośnik
  - Wykryto atak sieciowy
  - Nie wszystkie komponenty zostały zaktualizowane
  - Operacja na urządzeniu została zablokowana
  - Błąd aktywacji

- Błąd włączenia trybu przenośnego
- Błąd interakcji z Kaspersky Security Center
- Błąd wyłączenia trybu przenośnego
- Błąd modyfikacji zawartości aplikacji
- Błąd zastosowania szyfrowania / deszyfrowania pliku
- Nie można zastosować profilu
- Proces został przerwany
- Zablokowano aktywność sieciową
- Błąd aktualizacji sieci.

Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security

> Informacje zawarte w tej podsekcji odnoszą się tylko do Kaspersky Security Center 10 MR1 i nowszych wersji programu.

Optymalną i zalecaną opcją terminarza dla Kaspersky Endpoint Security w wersji 10 i / lub 10 SP1 jest **Po pobraniu nowych uaktualnień do repozytorium**, gdy zaznaczone jest pole **Automatycznie określ opóźnione uruchamianie zadania**.

Dla grupowego zadania aktualizacji w Kaspersky Endpoint Security w wersji 8 należy wyraźnie określić opóźnienie uruchamiania (1 godzina lub dłużej) oraz zaznaczyć pole **Automatycznie określ opóźnione uruchamianie zadania**.

Ręczna konfiguracja grupowego zadania skanowania komputerów z zainstalowanym programem Kaspersky Endpoint Security

Kreator wstępnej konfiguracji tworzy grupowe zadanie skanowania komputera. Domyślnie skonfigurowano terminarz **uruchamiania zadania w piątki o godzinie 19:00** z automatyczną randomizacją i odznaczonym polem **Uruchom pominięte zadania**.

Oznacza to, że jeśli komputery w organizacji są wyłączone w piątki, na przykład o godzinie 18:30, zadanie skanowania komputerów nigdy nie zostanie uruchomione. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Ręczna konfiguracja terminarza zadania wykrywania luk

Kreator wstępnej konfiguracji tworzy dla Agenta sieciowego grupowe zadanie wykrywania luk. Domyślnie skonfigurowano terminarz **uruchamiania zadania we wtorki o godzinie 19:00** z automatyczną randomizacją i zaznaczonym polem **Uruchom pominięte zadania**.

Jeśli zasady obowiązujące w organizacji nakazują wyłączenie komputerów w tym czasie, zadanie wykrywania luk zostanie uruchomione, gdy komputery znowu zostaną włączone, czyli w środę rano. Takie działanie nie jest wskazane, ponieważ wykrywanie luk może zwiększać zużycie procesora i obciążenie podsystemu dyskowego. Terminarz dla zadania wykrywania luk należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Ręczna konfiguracja grupowego zadania instalacji uaktualnień i naprawy luk

Kreator wstępnej konfiguracji tworzy dla Agenta sieciowego grupowe zadanie instalacji uaktualnień i naprawy luk. Domyślnie skonfigurowano terminarz uruchamiania zadania codziennie o godzinie 01:00 z automatyczną randomizacją i odznaczonym polem **Uruchom pominięte zadania**.

Jeśli reguły obowiązujące w organizacji nakazują wyłączanie komputerów na noc, zadanie instalacji uaktualnień nigdy nie zostanie uruchomione. Terminarz dla zadania wykrywania luk

należy skonfigurować w oparciu o zasady obowiązujące w organizacji. Należy pamiętać, że zadanie instalacji uaktualnień może wymagać ponownego uruchomienia komputera.

Tworzenie struktury grup administracyjnych i przydzielanie Agentów aktualizacji

Struktura grup administracyjnych w Kaspersky Security Center pełni następujące funkcje:

- Tworzy zakres profili.

  Istnieje alternatywny sposób stosowania odpowiedniego zestawu ustawień na komputerach przy użyciu *profili zasad*. W tym przypadku zakres profili jest tworzony ze znacznikami, lokalizacjami komputerów w jednostkach organizacyjnych Active Directory, członkostwem w grupach zabezpieczeń Active Directory itd. (sekcja “Hierarchia profili i korzystanie z profili“ na stronie 53).

- Tworzy zakres zadań grupowych.

  Istnieje sposób określania zakresu zadań grupowych, który nie jest oparty na hierarchii grup administracyjnych: korzystanie z zadań dla wyboru komputerów oraz z zadań dla wskazanych komputerów.

- Nadaje komputerom, wirtualnym Serwerom administracyjnym oraz podrzędnym Serwerom administracyjnym uprawnienia dostępu.

- Przydziela Agenty aktualizacji.

Podczas tworzenia struktury grup administracyjnych należy wziąć pod uwagę topologię sieci firmowej dla optymalnego przydzielenia Agentów aktualizacji. Optymalne przydzielenie Agentów aktualizacji pozwala na zmniejszenie ruchu w sieci firmowej.

W zależności od struktury organizacyjnej firmy oraz topologii sieci, w strukturze grup administracyjnych można zastosować następujące standardowe konfiguracje:

- Jedno biuro

- Wiele małych, oddzielonych od siebie biur

W tej sekcji:

Standardowa konfiguracja: Jedno biuro

W standardowej konfiguracji "jedno biuro" wszystkie komputery znajdują się w obrębie sieci firmowej i są dla siebie widoczne. Sieć firmowa może zawierać kilka oddzielnych części (sieci lub fragmentów sieci) połączonych ze sobą wąskimi kanałami.

Dostępne są następujące metody tworzenia struktury grup administracyjnych:

- Tworzenie struktury grup administracyjnych z uwzględnieniem topologii sieci. Struktura grup administracyjnych nie musi odzwierciedlać topologii sieci z absolutną dokładnością. Wystarczy dopasowanie oddzielnych części sieci i pewnych grup administracyjnych. Możesz skorzystać z automatycznego przydzielenia Agentów aktualizacji lub zrobić to ręcznie.

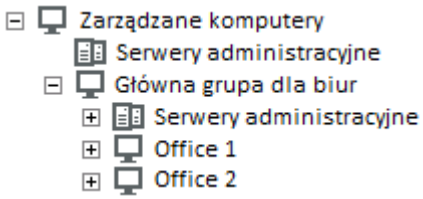
- Tworzenie struktury grup administracyjnych bez uwzględnienia topologii sieci. W tym przypadku należy wyłączyć automatyczne przydzielanie Agentów aktualizacji, a następnie wskazać jeden lub kilka komputerów jako Agenty aktualizacji dla głównej grupy administracyjnej w każdej z oddzielnych części sieci, na przykład dla grupy **Zarządzane komputery**. Wszystkie Agenty aktualizacji będą na tym samym poziomie i będą obejmować ten sam obszar, uwzględniając wszystkie komputery w sieci firmowej. W tym przypadku każdy Agent sieciowy w wersji 10 SP1 lub nowszej nawiąże połączenie z Agentem aktualizacji, który ma najkrótszą drogę. Trasę do Agenta aktualizacji można ustalić za pomocą narzędzia tracert.

Podczas ręcznego przypisywania Agentów aktualizacji, do jednego Agenta aktualizacji należy przypisać od 100 do 200 zarządzanych komputerów. Agentami aktualizacji powinny być mocne komputery z wystarczającą ilością wolnego miejsca na dysku (sekcja “Określanie przestrzeni dyskowej dla Agenta aktualizacji“ na stronie 140). Agenty aktualizacji nie mogą być zbyt często wyłączane oraz powinny mieć wyłączony tryb uśpienia.

Standardowa konfiguracja: Wiele małych, odizolowanych biur

Ta standardowa konfiguracja została utworzona z myślą o małych zdalnych biurach, które mogą kontaktować się z główną siedzibą za pośrednictwem internetu. Każde zdalne biuro znajduje się poza NAT, czyli połączenie jednego zdalnego biura z innym jest niemożliwe, gdyż biura są od siebie odizolowane.

Konfiguracja musi być odzwierciedlona w strukturze grup administracyjnych: dla każdego zdalnego biura musi zostać utworzona oddzielna grupa administracyjna (grupy **Office 1** i **Office 2** na rysunku poniżej).



Rysunek 1. Zdalne biura uwzględnione w strukturze grupy administracyjnej

Do każdej grupy administracyjnej odpowiadającej biuru należy przydzielić jednego lub kilku Agentów aktualizacji. Agentami aktualizacji muszą być komputery ze zdalnego biura, które posiadają wystarczającą ilość wolnego miejsca na dysku (sekcja “Określanie przestrzeni dyskowej dla Agenta aktualizacji“ na stronie 140). Komputery z grupy **Office 1** będą, na przykład, łączyć się z Agentami aktualizacji przydzielonymi do grupy administracyjnej **Office 1**.

Jeśli niektórzy użytkownicy poruszają się między biurami ze swoimi laptopami, w każdym zdalnym biurze, dla grupy administracyjnej najwyższego poziomu (**Główna grupa dla biur** na rysunku) należy wskazać dwa lub więcej komputerów jako Agentów aktualizacji (oprócz już istniejących Agentów aktualizacji) .

Przykład: Laptop znajduje się w grupie administracyjnej **Office 1**, a następnie zostaje fizycznie przeniesiony do biura, które odpowiada grupie administracyjnej **Office 2**. Po przeniesieniu laptopa, Agent sieciowy spróbuje połączyć się z Agentami aktualizacji przypisanymi do grupy **Office 1**, ale te Agenty aktualizacji są niedostępne. Następnie Agent sieciowy próbuje połączyć się z Agentami aktualizacji, które zostały przypisane do **Głównej grupy dla biur**. Ponieważ zdalne biura są odizolowane od siebie, próby nawiązania połączenia z Agentami aktualizacji przypisanymi do grupy administracyjnej **Główna grupa dla biur** zakończą się pomyślnie tylko wtedy, gdy Agent sieciowy spróbuje połączyć się z Agentami aktualizacji w grupie **Office 2**. Oznacza to, że laptop

pozostanie w grupie administracyjnej, która odpowiada pierwszemu biuru, ale będzie korzystał z Agenta aktualizacji biura, w którym aktualnie się znajduje.

Hierarchia profili i korzystanie z profili

W tej sekcji można znaleźć informacje dotyczące stosowania profili do komputerów w grupach administracyjnych. Znaleźć tu można także informacje o profilach zasad obsługiwanych przez Kaspersky Security Center, począwszy od wersji 10 SP1.

W tej sekcji:

Hierarchia profili

W Kaspersky Security Center profile są używane do określenia jednego zestawu ustawień dla kilku komputerów. Na przykład, obszar profilu produktu P zdefiniowanego dla grupy administracyjnej G zawiera zarządzane komputery z zainstalowanym produktem P, które zostały dodane do grupy G i wszystkich jej podgrup, za wyjątkiem tych podgrup, we właściwościach których odznaczono opcję **Dziedzicz od grupy nadrzędnej**.

Profil można odróżnić od lokalnego ustawienia po ikonach "kłódki" obok jego ustawień. Jeśli ustawienie (lub grupa ustawień) jest "zablokowane" we właściwościach profilu, w pierwszej kolejności należy użyć tego ustawienia (lub grupy ustawień) podczas tworzenia obowiązującego ustawienia, a następnie należy zapisać ustawienie (lub grupę ustawień) do profilu podrzędnego.

Tworzenie obowiązujących ustawień można opisać w następujący sposób: wartości wszystkich ustawień, które nie zostały "zablokowane", są kopiowane z profilu, a następnie są nadpisywane przez wartości ustawień lokalnych, a w kolejnym etapie wartości wynikowe są nadpisywane przez "zablokowane" ustawienia pobrane z profilu.

Profile tego samego produktu wpływają na siebie poprzez hierarchię grup administracyjnych: "Zablokowane" ustawienia z profilu nadrzędnego nadpisują te same ustawienia z profilu podrzędnego.

Dla użytkowników mobilnych istnieje specjalny profil. Ten profil jest aktywowany na komputerze, gdy ten przełącza się do trybu użytkownika mobilnego. Profile dla użytkowników mobilnych nie oddziałują na inne profile poprzez hierarchię grup administracyjnych.

> Profil dla użytkowników mobilnych nie będzie obsługiwany w kolejnych wersjach Kaspersky Security Center. W kolejnych wersjach, zamiast profili dla użytkowników mobilnych będą używane profile zasad.

Profile zasad

Stosowanie profili na komputerach poprzez hierarchię grup administracyjnych może być niewygodne tylko w kilku przypadkach. Konieczne może być utworzenie kilku instancji jednego profilu, które różnią się jednym lub dwoma ustawieniami dla różnych grup administracyjnych, oraz zsynchronizowanie zawartości tych profili w przyszłości.

Aby uniknąć takich problemów, Kaspersky Security Center (począwszy od wersji 10 SP1) obsługuje *profile zasad*. Profil zasad jest to inaczej podzbiór ustawień profilu. Ten podzbiór jest stosowany na komputerach docelowych wraz z profilem i uzupełnia go zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od "podstawowego" profilu, który jest aktywny na urządzeniu klienckim (komputerze lub urządzeniu mobilnym). Aktywacja profilu zmodyfikuje ustawienia zasad, które były aktywne na urządzeniu przed aktywacją profilu. Te ustawienia przyjmują wartości określone w profilu.

Aktualnie na profile zasad nałożone są następujące ograniczenia:

- Profil może zawierać maksymalnie 100 profili.
- Profil zasad nie może zawierać innych profili.
- Profil zasad nie może zawierać ustawień powiadamiania.

Zawartość profilu

Profil zasad zawiera następujące elementy:

- Nazwa. Profile z takimi samymi nazwami wpływają na siebie poprzez hierarchię grup administracyjnych ze wspólnymi regułami.
- Podzbiór ustawień profilu. Profil zawiera tylko aktualnie wymagane ustawienia (ustawienia "zablokowane").
- Warunek aktywacji jest wyrażeniem logicznym z właściwościami komputera — profil jest aktywny (uzupełnia profil) tylko wtedy, gdy warunek aktywacji profilu jest prawdziwy. We wszystkich pozostałych przypadkach profil jest nieaktywny i jest ignorowany. W wyrażeniu logicznym mogą być uwzględnione następujące właściwości komputera:
  - Stan trybu użytkownika mobilnego.
  - Właściwości środowiska sieci – nazwa aktywnej reguły dla połączenia Agenta Sieciowego (sekcja “Konfigurowanie profili połączenia dla użytkowników mobilnych“ na stronie 100).
  - Obecność lub brak określonych znaczników na komputerze.
  - Przydzielenie komputera do jednostki organizacyjnej Active Directory (OU): jawne (komputer znajduje się w określonej jednostce OU) lub niejawne (komputer jest w jednostce OU, która znajduje się w określonej jednostce OU na dowolnym poziomie zagnieżdżenia).
  - Członkostwo komputera w grupie zabezpieczeń Active Directory (jawne lub niejawne).
  - Członkostwo użytkownika komputera w grupie zabezpieczeń Active Directory (jawne lub niejawne).
- Pole wyłączające profil. Wyłączone profile są zawsze ignorowane, a ich odpowiednie warunki aktywacji nie są sprawdzane.
- Priorytet profilu. Warunki aktywacji różnych profili są niezależne, a więc można aktywować kilka profili jednocześnie. Jeśli aktywne profile zawierają nienakładające się na siebie zbiory ustawień, nie pojawi się żaden problem. Jednakże dwa aktywne profile zawierające różne wartości tego samego ustawienia spowodują niejednoznaczność. Tę niejednoznaczność

można wyeliminować poprzez priorytety profilu: Wartość niejednoznacznej zmiennej zostanie pobrana z profilu, który ma wyższy priorytet (ten, który znajduje się wyżej na liście profili).

Zachowanie profili, gdy zasady oddziałują na siebie poprzez hierarchię

Profile o tych samych nazwach zostają scalone zgodnie z regułami scalania profilu. Profile zasady nadrzędnej mają wyższy priorytet niż zasady podrzędnej. Jeśli modyfikowanie ustawień jest zabronione w zasadzie nadrzędnej (są "zablokowane"), zasada podrzędna używa warunków aktywacji profilu z zasady nadrzędnej. Jeśli modyfikowanie ustawień jest dozwolone w zasadzie nadrzędnej, używane są warunki aktywacji profilu z zasady podrzędnej.

Ponieważ w swoim warunku aktywacji profil zasad może zawierać opcję **Komputer w trybie użytkownika mobilnego**, profile całkowicie zastępują funkcję profili dla użytkowników mobilnych, które nie będą już obsługiwane.

Profil dla użytkowników mobilnych może zawierać profile, ale te profile mogą zostać aktywowane dopiero po przełączeniu komputera w tryb użytkownika mobilnego.

Zadania

W Kaspersky Security Center dostępne są następujące typy zadań podzielone ze względu na obszar:

- Zadania lokalne—utworzone bezpośrednio na zarządzanych komputerach. Zadania lokalne mogą zostać zmodyfikowane przez administratora po stronie Kaspersky Security Center przy użyciu narzędzi Konsoli administracyjnej, a także przez użytkownika zdalnego komputera (na przykład, z poziomu interfejsu aplikacji antywirusowej). Jeśli zadanie lokalne zostało zmodyfikowane jednocześnie przez administratora i użytkownika zarządzanego komputera, zostaną zastosowane zmiany wprowadzone przez administratora, gdyż mają wyższy priorytet.

- Zadania grupowe—wpływają na grupę administracyjną i jej wszystkie podgrupy. Zadania grupowe mogą też wpływać (opcjonalnie) na komputery, które zostały przyłączone do podrzędnych i wirtualnych Serwerów administracyjnych zainstalowanych w tej grupie lub w jej dowolnej podgrupie.

- Zadania dla wskazanych komputerów—wpływają na ograniczony zbiór komputerów, który został określony podczas tworzenia zadania.

- Zadania dla wyborów komputerów—wpływają na komputery, które znajdują się w określonym wyborze. Obszar zadania zmienia się, gdy zmienia się zbiór komputerów zawartych w wyborze. Wybór komputerów można utworzyć w oparciu o atrybuty komputerów, włączając w to oprogramowanie zainstalowane na komputerach, a także w oparciu o znaczniki przydzielone do komputerów. Wybór to najbardziej elastyczny sposób definiowania obszaru zadania.

  > Zadania dla wyborów komputerów są zawsze uruchamiane przez Serwer administracyjny zgodnie z terminarzem. Zadania dla wyborów komputerów nie mogą być uruchamiane na komputerach, które nie mają połączenia z Serwerem administracyjnym. Zadania nie są uruchamiane zgodnie z czasem lokalnym komputera docelowego tylko z czasem lokalnym Serwera administracyjnego.

- Zadania klastra (zadania macierzy serwera)—wpływają na węzły określonego klastra lub macierzy serwera.

Reguły przenoszenia komputerów

Zalecane jest skonfigurowanie automatycznego przenoszenia komputerów do grup administracyjnych. Można to zrobić, stosując *reguły przenoszenia komputerów*. Reguła przenoszenia komputerów składa się z trzech głównych części: nazwy, warunku wykonania (wyrażenie logiczne z atrybutami komputera) oraz docelowej grupy administracyjnej. Reguła przenosi komputer do docelowej grupy administracyjnej, jeśli atrybuty komputera spełniają warunek wykonania reguły.

Reguły przenoszenia komputerów posiadają priorytet. Serwer administracyjny sprawdza, czy atrybuty komputera spełniają warunek wykonania każdej reguły, w rosnącej kolejności priorytetów. Jeśli atrybuty komputera spełniają warunek wykonania reguły, komputer zostaje przeniesiony do grupy docelowej, a przetwarzanie reguły zostanie zakończone dla tego komputera. Jeśli atrybuty komputera spełniają warunki kilku reguł, komputer zostanie przeniesiony do grupy docelowej reguły z najwyższym priorytetem (czyli tej, która znajduje się najwyżej na liście).

Reguły przenoszenia komputerów mogą być tworzone pośrednio. Na przykład, we właściwościach zdalnego pakietu instalacyjnego lub zadania możesz określić grupę administracyjną, do której komputer musi zostać przeniesiony po zainstalowaniu na nim Agenta sieciowego. Reguły przenoszenia komputerów mogą być tworzone także bezpośrednio przez administratora Kaspersky Security Center na liście reguł przenoszenia. Lista ta znajduje się w Konsoli administracyjnej, we właściwościach grupy **Nieprzypisane**.

Domyślnie reguła przenoszenia komputerów jest przeznaczona do jednorazowego, wstępnego przydzielenia komputerów do grup administracyjnych. Reguła przenosi komputery z grupy **Nieprzypisane** tylko raz. Jeśli komputer był już raz przeniesiony przy użyciu tej reguły, reguła ta nie przeniesie go już nawet wtedy, gdy ręcznie przeniesiesz komputer z powrotem do grupy **Nieprzypisane**. Jest to zalecany sposób stosowania reguł przenoszenia.

Możesz przenieść komputery, które już zostały przydzielone do grup administracyjnych. W tym celu, we właściwościach reguły odznacz pole **Przenieś tylko komputery, które nie są dodane do grup administracyjnych**.

Stosowanie reguł przenoszenia do komputerów, które już zostały przydzielone do grup administracyjnych, znacząco zwiększa obciążenie na Serwerze administracyjnym.

Możesz utworzyć regułę przenoszenia, która będzie nieprzerwanie oddziaływać na jeden komputer.

Szczególnie zalecane jest unikanie ciągłego przenoszenia komputera z jednej grupy do drugiej (na przykład, w celu zastosowania specjalnego profilu do tego komputera, uruchomienia specjalnego zadania grupowego lub zaktualizowania komputera poprzez Agenta aktualizacji).

Takie scenariusze nie są obsługiwane, ponieważ w bardzo dużym stopniu zwiększają obciążenie na Serwerze administracyjnym oraz ruch sieciowy. Te scenariusze doprowadzają też do konfliktu z zasadami działania Kaspersky Security Center (szczególnie w obszarze uprawnień dostępu, zdarzeń i raportów). W tej sytuacji można skorzystać z dostępnego rozwiązana uwzględniającego użycie profili zasad (strona 54), zadań dla wyborów komputerów (sekcja “Zadania“ na stronie 56), poprzez przydzielenie Agentów sieciowych zgodnie ze standardowym scenariuszem (sekcja “Tworzenie struktury grup administracyjnych i przydzielanie Agentów aktualizacji“ na stronie 50) itd.

Kategoryzacja oprogramowania

Głównym narzędziem do monitorowania uruchomień aplikacji są kategorie Kaspersky Lab (zwane dalej "kategorie KL"). Kategorie KL umożliwiają administratorowi Kaspersky Security Center uproszczenie obsługi kategoryzacji oprogramowania i zminimalizowanie ruchu sieciowego skierowanego do zarządzanych komputerów.

Kategorie użytkownika powinny być tworzone tylko dla aplikacji, których nie można zaklasyfikować do żadnej z istniejących kategorii KL (na przykład, dla oprogramowania wykonanego na zamówienie użytkownika). Kategorie użytkownika są tworzone na podstawie pakietu instalacyjnego produktu (MSI) lub folderu z pakietami instalacyjnymi.

Jeśli dostępna jest duża ilość programów, które nie zostały skategoryzowane poprzez kategorie KL, można utworzyć automatycznie aktualizowaną kategorię. Sumy kontrolne plików wykonywalnych będą automatycznie dodawane do tej kategorii po każdej modyfikacji folderu zawierającego pakiety dystrybucyjne.

Automatycznie aktualizowanych kategorii oprogramowania nie można tworzyć na podstawie folderów Moje dokumenty, %windir% oraz %ProgramFiles%. Pula plików w tych folderach podlega częstym zmianom, co prowadzi do zwiększonego obciążenia na Serwerze administracyjnym i zwiększonego ruchu sieciowego. Należy utworzyć dedykowany folder ze zbiorem oprogramowania i okresowo dodawać do niego nowe elementy.

Tworzenie kopii zapasowej i przywracanie ustawień Serwera administracyjnego

Tworzenie kopii zapasowej ustawień Serwera administracyjnego i jego baz danych odbywa się przy użyciu zadania tworzenia kopii zapasowej oraz narzędzia klbackup. Kopia zapasowa zawiera wszystkie główne ustawienia i obiekty dotyczące Serwera administracyjnego, takie jak: Certyfikaty Serwera administracyjnego, klucze główne do szyfrowania dysków na zarządzanych komputerach, klucze dla różnych licencji, strukturę grup administracyjnych z całą jej zawartością, zadania, profile itd. Przy użyciu kopii zapasowej możesz szybko przywrócić działanie Serwera administracyjnego.

Nigdy nie rezygnuj z regularnego wykonywania kopii zapasowej Serwera administracyjnego przy użyciu standardowego zadania tworzenia kopii zapasowej.

Jeśli nie ma dostępnej kopii zapasowej, błąd może doprowadzić do bezpowrotnej utraty certyfikatów i wszystkich ustawień Serwera administracyjnego. Będzie to wymagało przeprowadzenia konfiguracji Kaspersky Security Center od początku oraz ponownego zainstalowania Agenta sieciowego w sieci firmowej. Wszystkie klucze główne do szyfrowania dysków na zarządzanych komputerach zostaną utracone, co spowoduje ryzyko utraty zaszyfrowanych danych na komputerach z zainstalowanym programem Kaspersky Endpoint Security.

Kreator wstępnej konfiguracji tworzy zadanie wykonywania kopii zapasowej dla ustawień Serwera administracyjnego, które będzie uruchamiane codziennie o 3:00. Domyślnie kopie zapasowe są zapisywane w folderze %ALLUSERSPROFILE%\Application Data\KasperskySC.

Jeśli serwer Microsoft SQL Server, zainstalowany na innym komputerze, jest używany jako DBMS, należy zmodyfikować zadanie tworzenia kopii zapasowej, określając jako folder do przechowywania kopii zapasowych ścieżkę UNC, która jest używana do zapisywania usługi Serwera administracyjnego oraz usługi SQL Server. To wymaganie, które nie jest oczywiste, wynika ze specyfiki specjalnej funkcji kopii zapasowej w systemie DBMS serwera Microsoft SQL Server.

Jeśli jako system DBMS używana jest lokalna instancja serwera Microsoft SQL Server, przydatne będzie zapisanie kopii zapasowych na dedykowanym nośniku w celu zabezpieczenia ich przed uszkodzeniem.

Ponieważ kopia zapasowa zawiera ważne dane, zadanie tworzenia kopii zapasowej oraz narzędzie klbackup oferują ochronę kopii zapasowej przy użyciu hasła. Domyślnie zadanie tworzenia kopii zapasowej wykonuje kopię zapasową z pustym hasłem. Hasło należy ustawić we właściwościach zadania tworzenia kopii zapasowej. Pominięcie tego wymagania doprowadza do sytuacji, w której wszystkie klucze certyfikatów Serwera administracyjnego, klucze dla licencji oraz klucze główne dla szyfrowania dysków na zarządzanych komputerów pozostaną niezaszyfrowane.

Oprócz regularnych kopii zapasowych, kopie zapasowe należy tworzyć także przed każdą znaczącą zmianą, w tym instalacją aktualizacji i łat Serwera administracyjnego.

Aby zmniejszyć rozmiar kopii zapasowych, w ustawieniach serwera SQL Server zaznacz pole **Kompresuj kopie zapasowe** (**Kompresuj kopię zapasową**).

Przywracanie kopii zapasowej odbywa się przy użyciu narzędzia klbackup na działającej instancji Serwera administracyjnego, który został właśnie zainstalowany i posiada tę samą wersję (lub nowszą), dla której kopia zapasowa została utworzona.

Instancja Serwera administracyjnego, na którym kopia zapasowa ma zostać przywrócona, musi korzystać z systemu DBMS tego samego typu (ten sam SQL Server lub MySQL) i tej samej (lub nowszej) wersji. Wersja Serwera administracyjnego może być taka sama (z tą samą lub późniejszą łatą) lub nowsza.

Sekcja opisuje standardowe scenariusze przywracania ustawień i obiektów Serwera administracyjnego.

W tej sekcji:

Komputer z zainstalowanym Serwerem administracyjnym nie działa

Jeśli komputer, na którym jest zainstalowany Serwer administracyjny, nie działa z powodu błędu, zalecane jest wykonanie następujących działań:

- Nowy Serwer administracyjny musi posiadać ten sam adres: nazwę NetBIOS, nazwę FQDN lub statyczny adres IP (w zależności od tego, co zostało ustawione podczas instalacji Agentów sieciowych).
- Zainstaluj Serwer administracyjny, używając systemu DBMS tego samego typu i w tej samej wersji. Możesz zainstalować tę samą wersję Serwera z tą samą (lub późniejszą) łatą

lub nowszą wersję Serwera. Po instalacji nie przeprowadzaj wstępnej konfiguracji przy użyciu Kreatora.

- Z poziomu menu **Start** uruchom narzędzie klbackup i przywróć kopię zapasową.

Ustawienia Serwera administracyjnego lub bazy danych są uszkodzone

Jeżeli Serwer administracyjny nie działa ze względu na uszkodzone ustawienia lub bazę danych (na przykład, w wyniku przepięcia), zalecane jest użycie następujących scenariuszy:

1. Przeskanuj system plików na uszkodzonym komputerze.
2. Odinstaluj niedziałającą wersję Systemu operacyjnego.
3. Zainstaluj ponownie Serwer administracyjny, używając systemu DBMS tego samego typu i w tej samej (lub nowszej) wersji. Możesz zainstalować tę samą wersję Serwera z tą samą (lub późniejszą) łatą bądź nowszą wersję Serwera. Po instalacji nie przeprowadzaj wstępnej konfiguracji przy użyciu Kreatora.
4. Z poziomu menu **Start** uruchom narzędzie klbackup i przywróć kopię zapasową.

Surowo zabronione jest przywracanie Serwera administracyjnego w sposób inny niż przy użyciu narzędzia klbackup.

Wszelkie próby przywrócenia Serwera administracyjnego przy użyciu oprogramowania firm trzecich doprowadzą do desynchronizacji danych na węzłach aplikacji Kaspersky Security Center i w konsekwencji - do niepoprawnego działania produktu.

Instalowanie Agenta sieciowego i aplikacji antywirusowej

Aby zarządzać komputerami w firmie, na każdym z nich należy zainstalować Agenta sieciowego. Zdalna instalacja aplikacji Kaspersky Security Center na komputerach w firmie zazwyczaj rozpoczyna się od zainstalowania na nich Agenta sieciowego.

W tej sekcji:

Wstępna zdalna instalacja

Jeśli Agent sieciowy został już zainstalowany na komputerze, zdalna instalacja aplikacji na tym komputerze odbywa się poprzez Agenta sieciowego. Pakiet dystrybucyjny aplikacji, która ma

zostać zainstalowana, jest przesyłany za pośrednictwem kanałów komunikacji pomiędzy Agentami sieciowymi i Serwerem administracyjnym wraz z ustawieniami instalacji, zdefiniowanymi przez administratora. Aby przesłać pakiet dystrybucyjny, możesz użyć węzłów pośredniczących, na przykład, Agentów sieciowych, dostarczania multiemisyjnego itd. Więcej informacji dotyczących instalacji aplikacji na zarządzanych komputerach, na których jest już zainstalowany Agent sieciowy, można znaleźć poniżej.

Możesz przeprowadzić wstępną instalację Agenta sieciowego na komputerach działających pod kontrolą systemu Windows, korzystając z jednej z następujących metod:

- Używając narzędzi firm trzecich do zdalnej instalacji aplikacji.
- Klonując obraz dysku twardego administratora z systemem operacyjnym i Agentem sieciowym: przy pomocy narzędzi do zarządzania obrazami dysku, dostępnych w Kaspersky Security Center, lub przy użyciu narzędzi firm trzecich.
- Korzystając z zasad grupy w systemie Windows: używając standardowych narzędzi do zarządzania systemu Windows dla zasad grupy lub w trybie automatycznym, poprzez odpowiednią, dedykowaną opcję w zadaniu zdalnej instalacji programu Kaspersky Security Center.
- W trybie wymuszonym, korzystając ze specjalnych opcji w zadaniu zdalnej instalacji programu Kaspersky Security Center.
- Wysyłając do użytkowników komputerów odnośniki do pakietów autonomicznych wygenerowanych przez Kaspersky Security Center. Pakiety autonomiczne to moduły wykonywalne, które zawierają pakiety dystrybucyjne wybranych aplikacji wraz ze zdefiniowanymi ustawieniami.
- Ręcznie, uruchamiając instalatory produktów na komputerach docelowych.

Na platformach innych niż Windows wstępna instalacja Agenta sieciowego na zarządzanych komputerach musi zostać wykonana z użyciem dostępnych narzędzi firm trzecich. Na platformach innych niż Windows możesz uaktualnić Agenta sieciowego do nowej wersji lub zainstalować inne aplikacje firmy Kaspersky Lab, korzystając z Agenta sieciowego (już zainstalowanego na komputerach) przeznaczonego do wykonywania zadań zdalnej instalacji. W tym przypadku instalacja przebiega identycznie jak instalacja na komputerach z zainstalowanym systemem Windows.

Podczas wybierania metody i strategii zdalnej instalacji produktów w zarządzanej sieci należy mieć na uwadze kilka czynników (częściowa lista):

- Konfigurację sieci firmowej (sekcja "Standardowa konfiguracja Kaspersky Security Center" na stronie 18)
- Całkowitą liczbę hostów
- Obecność w sieci firmowej komputerów, które nie należą do żadnej domeny Active Directory, oraz obecność jednakowych kont z uprawnieniami administratora na tych komputerach
- Pojemność kanału pomiędzy Serwerem administracyjnym a komputerami docelowymi
- Rodzaj komunikacji pomiędzy Serwerem administracyjnym a zdalnymi podsieciami oraz pojemność kanałów sieciowych w tych podsieciach
- Ustawienia zabezpieczeń zastosowane na zdalnych komputerach w momencie uruchomienia zdalnej instalacji (na przykład, użycie UAC lub Prostego udostępniania plików).

Konfigurowanie instalatorów

Przed uruchomieniem zdalnej instalacji aplikacji Kaspersky Lab w sieci, należy określić ustawienia instalacji (ustawienia definiowane podczas instalacji aplikacji). Podczas instalacji Agenta sieciowego należy określić przynajmniej adres połączenia z Serwerem administracyjnym; niektóre ustawienia zaawansowane też mogą być wymagane. W zależności od wybranej metody instalacji, ustawienia można zdefiniować w różny sposób. W najprostszym przypadku (ręczna instalacja interaktywna na wybranym komputerze) wszystkie odpowiednie ustawienia można skonfigurować z poziomu interfejsu instalatora.

Ta metoda definiowania ustawień jest nieodpowiednia w nieinteraktywnej instalacji (cichej) aplikacji w grupach komputerów. Na ogół administrator musi określić wartości dla ustawień w sposób scentralizowany; te wartości mogą być następnie użyte w instalacji nieinteraktywnej na wybranych komputerach w sieci.

Pakiety instalacyjne

Pierwsza i główna metoda definiowania ustawień instalacji aplikacji jest uniwersalna i tym samym jest odpowiednia dla wszystkich metod instalacji: przy użyciu narzędzi Kaspersky Security Center oraz większości narzędzi firm trzecich. Ta metoda obejmuje utworzenie pakietów instalacyjnych aplikacji w Kaspersky Security Center.

Pakiety instalacyjne są generowane przy użyciu następujących metod:

- Automatycznie, z określonych pakietów dystrybucyjnych, na podstawie załączonych *deskryptorów* (pliki z rozszerzeniem .kud, które zawierają reguły dla instalacji, wyniki analizy oraz inne informacje)

- Z plików wykonywalnych instalatorów lub z instalatorów w formacie Microsoft Windows Installer (*.msi), które są dla standardowych lub obsługiwanych aplikacji.

Wygenerowane pakiety instalacyjne są zorganizowane hierarchicznie jako foldery z zagnieżdżonymi podfolderami i plikami. Oprócz oryginalnego pakietu dystrybucyjnego, pakiet instalacyjny zawiera ustawienia dostępne do modyfikacji (w tym ustawienia instalatora oraz reguły przetwarzania dla takich sytuacji, jak konieczność ponownego uruchomienia systemu operacyjnego w celu zakończenia instalacji), a także drobne moduły pomocnicze.

Wartości ustawień instalacji, które są charakterystyczne dla pojedynczej obsługiwanej aplikacji, można zdefiniować w interfejsie Konsoli administracyjnej podczas tworzenia pakietu instalacyjnego. Podczas zdalnej instalacji aplikacji przy użyciu narzędzi Kaspersky Security Center pakiety instalacyjne są dostarczane na komputery docelowe, dzięki czemu uruchomienie instalatora aplikacji udostępni dla tej aplikacji wszystkie ustawienia zdefiniowane przez administratora. Jeśli do zainstalowania aplikacji firmy Kaspersky Lab używasz narzędzi firm trzecich, musisz zapewnić dostępność całego pakietu instalacyjnego, czyli pakietu dystrybucyjnego i jego ustawień. Pakiety instalacyjne są tworzone i przechowywane przez Kaspersky Security Center w dedykowanym podfolderze, znajdującym się w folderze współdzielonym (sekcja "Określanie folderu współdzielonego" na stronie 38).

Więcej informacji dotyczących korzystania z tej metody definiowania ustawień dla aplikacji Kaspersky Lab przed ich zainstalowaniem przy użyciu narzędzi firm trzecich można znaleźć w sekcji "Zdalna instalacja przy użyciu zasad grupy Microsoft Windows" (sekcja "Zdalna instalacja przy użyciu zasad grupy Microsoft Windows" na stronie 71).

Natychmiast po zainstalowaniu programu Kaspersky Security Center, automatycznie zostaje wygenerowanych kilka pakietów instalacyjnych. Pakiety te są gotowe do zainstalowania i zawierają pakiety Agenta sieciowego oraz pakiety aplikacji antywirusowych dla platformy Microsoft Windows.

> Klucz dla aplikacji można ustawić we właściwościach pakietu instalacyjnego, jednakże zalecane jest unikanie tej metody dystrybucji licencji, gdyż w łatwy sposób można uzyskać dostęp do pakietów instalacyjnych. Dla kluczy należy używać zadań automatycznego rozsyłania kluczy lub instalacji produktu.

Właściwości MSI i pliki transformacji

Innym sposobem skonfigurowania instalacji na platformie Windows jest zdefiniowanie właściwości MSI i plików transformacji. Ta metoda może być stosowana w następujących przypadkach:

- Podczas instalacji poprzez zasady grupy systemu Windows, korzystając ze standardowych narzędzi Microsoft lub innych narzędzi firm trzecich do zarządzania zasadami grupy systemu Windows
- Podczas instalacji aplikacji przy użyciu narzędzi firm trzecich przeznaczonych do zarządzania instalatorami w formacie Microsoft Installer (sekcja "Konfigurowanie instalatorów" na stronie 84).

Zdalna instalacja przy użyciu narzędzi firm trzecich

Jeśli w firmie dostępne są jakiekolwiek narzędzia do zdalnej instalacji aplikacji (na przykład, Microsoft System Center), wygodnym rozwiązaniem będzie przeprowadzenie wstępnej zdalnej instalacji przy użyciu tych narzędzi.

Należy wykonać następujące czynności:

- Wybierz metodę konfiguracji instalacji, która najbardziej odpowiada używanemu narzędziu do zdalnej instalacji.

- Zdefiniuj mechanizm synchronizacji pomiędzy modyfikacją ustawień pakietów instalacyjnych (poprzez interfejs Konsoli administracyjnej) a działaniem wybranych narzędzi firm trzecich, używanych do zdalnej instalacji aplikacji z pakietu instalacyjnego.
- Podczas instalacji z folderu współdzielonego upewnij się, że ten zasób plików posiada wystarczającą pojemność.

Zobacz również:

Określanie folderu współdzielonego 38

Konfigurowanie instalatorów 84

Informacje ogólne o zadaniach zdalnej instalacji w Kaspersky Security Center

Kaspersky Security Center oferuje różne mechanizmy zdalnej instalacji aplikacji, które są zaimplementowane pod postacią zadań zdalnej instalacji (instalacja wymuszona, instalacja poprzez skopiowanie obrazu dysku twardego, instalacja poprzez zasady grupy systemu Microsoft Windows). Możesz utworzyć zadanie zdalnej instalacji dla określonej grupy administracyjnej oraz dla wskazanych komputerów lub wyboru komputerów (takie zadania są wyświetlane w Konsoli administracyjnej, w folderze **Zadania dla wskazanych komputerów**). Podczas tworzenia zadania możesz wybrać pakiety instalacyjne (Agenta sieciowego i / lub innej aplikacji), które zostaną zainstalowane w obrębie tego zadania, a także określić pewne ustawienia, które definiują metodę zdalnej instalacji. Dodatkowo można użyć Kreatora zdalnej instalacji, którego działanie polega na utworzeniu zadania zdalnej instalacji i monitorowaniu wyników.

> Zadania dla grup administracyjnych dotyczą komputerów znajdujących się w określonej grupie oraz wszystkich komputerów we wszystkich podgrupach tej grupy administracyjnej. Zadanie obejmuje komputery podrzędnego Serwera administracyjnego znajdujące się w grupie lub jej dowolnych podgrupach, jeśli odpowiednie ustawienie zostało włączone w zadaniu.

Zadania dla wskazanych komputerów aktualizują listę komputerów klienckich przy każdym uruchomieniu zgodnie z zestawem wyborów w momencie uruchomienia zadania. Jeśli wybór

zawiera komputery, które zostały połączone z podrzędnym Serwerem administracyjnym, zadanie zostanie uruchomione także na tych komputerach. Szczegółowe informacje dotyczące tych ustawień i metod instalacji znajdują się poniżej.

> Aby zapewnić pomyślne działanie zadania zdalnej instalacji na komputerach połączonych z podrzędnym Serwerem administracyjnym, należy użyć zadania retranslacji do przekazania podrzędnemu Serwerowi administracyjnemu pakietów instalacyjnych używanych przez zadanie użytkownika.

Zdalna instalacja poprzez przechwycenie i skopiowanie obrazu dysku twardego komputera

Jeśli konieczne jest zainstalowanie Agenta sieciowego na komputerach, na których musi zostać (ponownie) zainstalowany system operacyjny i inne oprogramowanie, możesz wykorzystać mechanizm przechwytywania i kopiowania obrazu dysku twardego komputera.

Przechwytywanie i kopiowanie obrazu dysku twardego komputera odbywa się w następujący sposób:

1. Utwórz komputer referencyjny z zainstalowanym systemem operacyjnym i niezbędnym oprogramowaniem, włączając w to Agenta sieciowego i aplikację antywirusową.
2. Przechwyć obraz komputera referencyjnego i roześlij ten obraz na nowe komputery przy użyciu dedykowanego zadania z Kaspersky Security Center.

   Aby przechwytywać i instalować obrazy dysków, możesz skorzystać z narzędzi firm trzecich dostępnych w firmie lub z funkcji (na mocy licencji Zarządzania systemami) oferowanej przez Kaspersky Security Center (sekcja "Instalowanie obrazów systemów operacyjnych" na stronie 24).

Jeśli do zarządzania obrazami dysków używasz narzędzi firm trzecich, podczas zdalnej instalacji na komputerze docelowym z obrazu referencyjnego musisz usunąć informacje, których Kaspersky Security Center używa do identyfikowania zarządzanego komputera. W przeciwnym razie, Serwer administracyjny nie będzie mógł odróżnić komputerów, które zostały utworzone poprzez skopiowanie tego samego obrazu (patrz strona http://support.kaspersky.com/pl/9334).

Podczas przechwytywania obrazu dysku przy użyciu narzędzi Kaspersky Security Center ten problem jest rozwiązywany automatycznie.

Kopiowanie dysku przy użyciu narzędzi firm trzecich

Jeśli podczas przechwytywania obrazu komputera z zainstalowanym Agentem sieciowym stosujesz narzędzia firm trzecich, użyj jednej z następujących metod:

- Zalecana metoda. Podczas instalacji Agenta sieciowego na komputerze referencyjnym, wybierz opcję **Po zakończeniu instalacji nie uruchamiaj usługi** i przed pierwszym uruchomieniem usługi Agenta sieciowego przechwyć obraz komputera (ponieważ unikatowa informacja identyfikująca komputer jest tworzona przy pierwszym połączeniu Agenta sieciowego z Serwerem administracyjnym). Zalecane jest unikanie uruchamiania usługi Agenta sieciowego, aż do zakończenia operacji przechwytywania obrazu.

- Na komputerze referencyjnym zatrzymaj usługę Agenta sieciowego i uruchom narzędzie klmover z przełącznikiem -dupfix. Narzędzie klmover znajduje się w pakiecie instalacyjnym Agenta sieciowego. Unikaj kolejnych uruchomień usługi Agenta sieciowego, dopóki operacja przechwytywania obrazu nie zostanie zakończona.

- Upewnij się, że narzędzie klmover zostanie uruchomione z przełącznikiem -dupfix przed (wymaganie obowiązkowe) pierwszym uruchomieniem usługi Agenta sieciowego na komputerach docelowych, przy pierwszym uruchomieniu systemu operacyjnego po zainstalowaniu obrazu. Narzędzie klmover znajduje się w pakiecie instalacyjnym Agenta sieciowego.

Jeśli obraz dysku twardego został skopiowany niepoprawnie, przejdź do sekcji Niepoprawne skopiowanie obrazu dysku twardego (strona 147).

Dla zdalnej instalacji Agenta sieciowego na nowych komputerach możesz zastosować alternatywny scenariusz, korzystając z obrazów systemu operacyjnego:

- Przechwycony obraz nie zawiera zainstalowanego Agenta sieciowego
- Pakiet autonomiczny Agenta sieciowego, który znajduje się w folderze współdzielonym Kaspersky Security Center, został dodany do listy plików wykonywalnych uruchamianych po zakończeniu instalacji obrazu na komputerach docelowych.

Ten scenariusz instalacji dodaje element elastyczności: Możesz użyć jednego obrazu systemu operacyjnego z różnymi opcjami instalacji dla Agenta sieciowego i / lub produktu antywirusowego, włączając w to reguły przenoszenia komputerów dotyczące pakietu autonomicznego. To może trochę skomplikować proces zdalnej instalacji: Musisz umożliwić dostęp do folderu sieciowego z pakietami autonomicznymi z komputera docelowego (sekcja "Instalowanie obrazów systemów operacyjnych" na stronie 24).

Zdalna instalacja przy użyciu zasad grupy Microsoft Windows

Przeprowadzenie wstępnej instalacji Agentów sieciowych poprzez zasady grupy Microsoft Windows jest zalecane wtedy, gdy spełnione są następujące warunki:

- Komputery docelowe są członkami domeny Active Directory.
- Schemat zdalnej instalacji umożliwia zaczekanie na regularne ponowne uruchomienie komputerów docelowych przed rozpoczęciem zdalnej instalacji Agentów sieciowych na tych komputerach (lub można wymusić zastosowanie na tych komputerach zasady grupy systemu Windows).

Ten schemat instalacji charakteryzuje się następującymi cechami:

- Pakiet dystrybucyjny aplikacji w formacie Microsoft Installer (pakiet MSI) znajduje się w folderze współdzielonym (folder, w którym konta System lokalny komputerów docelowych mają uprawnienia do odczytu).
- W profilu grupy Active Directory, dla pakietu dystrybucyjnego tworzony jest obiekt instalacji.
- Obszar instalacji jest ustawiany poprzez określenie jednostki organizacyjnej (OU) i / lub grupy zabezpieczeń, która zawiera komputery docelowe.

- Następnym razem, gdy komputer docelowy zaloguje się do domeny (przed zalogowaniem się użytkowników do systemu), wszystkie zainstalowane aplikacje są sprawdzane pod kątem żądanej aplikacji. Jeśli żądana aplikacja nie zostanie odnaleziona, pakiet dystrybucyjny zostanie pobrany z zasobu określonego w profilu, a następnie zostanie zainstalowany.

Ten schemat zdalnej instalacji niesie za sobą korzyść, jaką jest instalowanie przypisanych aplikacji na komputerach docelowych podczas ładowania systemu operacyjnego, czyli przed zalogowaniem się użytkownika do systemu. Nawet jeśli użytkownik, który nie ma wystarczających uprawnień, usunie aplikację, zostanie ona ponownie zainstalowana przy kolejnym uruchomieniu systemu operacyjnego. Wadą tego schematu zdalnej instalacji jest fakt, że zmiany w profilu grupowym, które zostały wprowadzone przez administratora, nie zostaną zastosowane, aż do ponownego uruchomienia komputera (jeśli nie są używane narzędzia dodatkowe).

Profile grupy można użyć do zainstalowania Agenta sieciowego oraz innych aplikacji, jeśli ich instalatory są w formacie Windows Installer.

Podczas wybierania schematu zdalnej instalacji należy mieć na uwadze obciążenie zasobu plików, z którego pliki zostaną skopiowane na komputery docelowe po zastosowaniu zasad grupy systemu Windows.

Zarządzanie zasadami Microsoft Windows przy użyciu zadania zdalnej instalacji z programu Kaspersky Security Center

Najprostszym sposobem zainstalowania aplikacji poprzez zasady grupy systemu Microsoft Windows jest zaznaczenie opcji **Przypisz pakiet instalacyjny do profilu grupy Active Directory** we właściwościach zadania zdalnej instalacji z programu Kaspersky Security Center. W tym przypadku, podczas uruchamiania zadania Serwer administracyjny automatycznie wykonuje następujące działania:

- Tworzy wymagane obiekty w zasadach grupy systemu Microsoft Windows.
- Tworzy dedykowane grupy zabezpieczeń, umieszcza w nich komputery docelowe i przypisuje do nich instalację wybranych aplikacji. Zbiór grup zabezpieczeń zostanie zaktualizowany przy każdym uruchomieniu zadania, zgodnie z pulą komputerów docelowych w momencie uruchomienia.

Aby ta funkcja działała, we właściwościach zadania określ konto, które posiada uprawnienia do zapisu w profilach grupy Active Directory.

Jeśli chcesz zainstalować Agenta sieciowego i inną aplikację przy użyciu tego samego zadania, zaznaczenie opcji **Przypisz pakiet instalacyjny do profilu grupy Active Directory** spowoduje utworzenie obiektu instalacji w profilu Active Directory tylko dla Agenta sieciowego. Druga aplikacja wybrana w zadaniu zostanie zainstalowana przy użyciu narzędzi Agenta sieciowego od razu po jego zainstalowaniu na komputerze docelowym. Jeśli poprzez zasady grupy systemu Windows chcesz zainstalować aplikację inną niż Agent sieciowy, musisz utworzyć zadanie instalacji tylko dla tego pakietu instalacyjnego (bez pakietu Agenta sieciowego).

Jeśli żądane obiekty są tworzone w profilu grupy przy użyciu narzędzi Kaspersky Security Center, folder współdzielony Kaspersky Security Center zostanie użyty jako źródło pakietu instalacyjnego. Podczas planowania zdalnej instalacji należy zestawić prędkość odczytu tego folderu z liczbą komputerów docelowych i rozmiarem pakietu dystrybucyjnego przeznaczonego do zainstalowania. Przydatne może być umieszczenie folderu współdzielonego Kaspersky Security Center w dedykowanym repozytorium plików charakteryzującym się wysoką wydajnością (sekcja "Określanie folderu współdzielonego" na stronie 38).

Oprócz łatwości użycia, automatyczne tworzenie zasad grupy systemu Windows poprzez Kaspersky Security Center posiada następujące korzyści: podczas planowania instalacji Agenta sieciowego można w łatwy sposób określić grupę administracyjną Kaspersky Security Center, do której komputery będą automatycznie przenoszone po zakończeniu instalacji. Tę grupę można określić przy użyciu Kreatora tworzenia nowego zadania lub w oknie ustawień zadania zdalnej instalacji.

> Podczas zarządzania zasadami grupy systemu Windows poprzez Kaspersky Security Center możesz wskazać komputery docelowe dla obiektu zasad grupy, tworząc grupę zabezpieczeń. Kaspersky Security Center synchronizuje zawartość grupy zabezpieczeń z bieżącym zbiorem komputerów uwzględnionych w zadaniu. Jeśli do zarządzania zasadami grupy używasz innych narzędzi, możesz skojarzyć obiekty zasad grupy bezpośrednio z wybranymi jednostkami organizacyjnymi Active Directory.

Samodzielna instalacja aplikacji przy użyciu zasad Microsoft Windows

Administrator może tworzyć obiekty wymagane do zainstalowania w zasadach grupy systemu Windows w swoim imieniu. W tym przypadku administrator może udostępnić odnośniki do pakietów przechowywanych w folderze współdzielonym Kaspersky Security Center lub wysłać te pakiety na dedykowany serwer plików i udostępnić odnośniki do ich pobrania.

Dostępne są następujące scenariusze instalacji:

- Administrator tworzy pakiet instalacyjny i konfiguruje jego ustawienia w Konsoli administracyjnej. Obiekt zasad grupy zawiera odnośnik do pliku msi tego pakietu, który jest przechowywany w folderze współdzielonym Kaspersky Security Center.

- Administrator tworzy pakiet instalacyjny i konfiguruje jego ustawienia w Konsoli administracyjnej. Następnie administrator kopiuje cały podfolder EXEC tego pakietu z folderu współdzielonego Kaspersky Security Center do folderu w dedykowanym zasobie plików w firmie. Obiekt zasad grupy zawiera odnośnik do pliku msi tego pakietu, który jest przechowywany w podfolderze w dedykowanym zasobie plików w firmie.

- Administrator pobiera pakiet dystrybucyjny aplikacji (w tym pakiet Agenta sieciowego) z internetu i wysyła go do dedykowanego zasobu plików w firmie. Obiekt zasad grupy zawiera odnośnik do pliku msi tego pakietu, który jest przechowywany w podfolderze w dedykowanym zasobie plików w firmie. Ustawienia instalacji są definiowane poprzez konfigurowanie właściwości MSI lub poprzez konfigurowanie plików transformacji MST (sekcja "Konfigurowanie instalatorów" na stronie 84).

Wymuszona zdalna instalacja przy użyciu zadania zdalnej instalacji z Kaspersky Security Center

Jeśli musisz natychmiast rozpocząć instalację Agentów sieciowych lub innych aplikacji, nie czekając na zalogowanie w domenie kolejnych komputerów docelowych, lub jeśli są dostępne jakiekolwiek komputery docelowe, które nie znajdują się w domenie Active Directory, możesz użyć instalacji wymuszonej wybranych pakietów instalacyjnych poprzez zadanie zdalnej instalacji z Kaspersky Security Center.

W tej sytuacji możesz bezpośrednio wskazać komputery docelowe lub wybrać grupę administracyjną Kaspersky Security Center, do której należą, bądź też utworzyć wybór komputerów w oparciu o określone kryterium. Instalacja rozpoczyna się zgodnie z terminarzem zadania. Jeśli we właściwościach zadania włączone jest ustawienie **Uruchom pominięte zadania**, zadanie może zostać uruchomione albo natychmiast po włączeniu komputerów docelowych, albo po ich przeniesieniu do docelowej grupy administracyjnej.

Ten rodzaj instalacji obejmuje kopiowanie plików do zasobu administracyjnego (admin$) na

każdym komputerze docelowym oraz zdalną rejestrację usług pomocniczych na tych komputerach. W tym przypadku muszą być spełnione następujące warunki:

- Komputery docelowe muszą być dostępne dla połączenia albo po stronie Serwera administracyjnego, albo po stronie Agenta aktualizacji.
- Rozwiązywanie nazw komputerów docelowych musi działać poprawnie w sieci.
- Zasób administracyjny (admin$) musi pozostać włączony na komputerach docelowych.
- Na komputerach docelowych musi być uruchomiona usługa systemowa Serwer (domyślnie jest uruchomiona).
- W celu zezwolenia na zdalny dostęp przy użyciu narzędzi systemu Windows, na komputerach docelowych muszą być otwarte poniższe porty: TCP 139, TCP 445, UDP 137, UDP 138.
- Tryb Proste udostępnianie plików musi być wyłączony na komputerach docelowych.
- Na komputerach docelowych udostępnianie i model zabezpieczeń muszą być ustawione na *Klasyczny - uwierzytelnianie użytkowników lokalnych jako samych siebie*. W żadnym wypadku nie może być ustawione *Tylko gość - uwierzytelnianie użytkowników lokalnych jako gościa*.
- Komputery docelowe muszą być członkami domeny lub wcześniej należy utworzyć na komputerach docelowych jednakowe konta z uprawnieniami administratora.

Komputery w grupach roboczych mogą zostać przystosowane zgodnie z powyższymi wymaganiami przy użyciu narzędzia riprep.exe, którego opis znajduje się na stronie działu pomocy technicznej firmy Kaspersky Lab (http://support.kaspersky.com/pl/7434).

Podczas instalacji na nowych komputerach, które jeszcze nie zostały przydzielone do grup administracyjnych Kaspersky Security Center, możesz otworzyć właściwości zadania zdalnej instalacji i określić grupę administracyjną, do której komputery zostaną przeniesione po zakończeniu instalacji Agenta sieciowego.

> Podczas tworzenia zadania grupowego należy pamiętać, że każde zadanie grupowe ma wpływ na wszystkie komputery we wszystkich grupach zagnieżdżonych w wybranej grupie. Dlatego też należy unikać powielania zadań instalacji w podgrupach.

Automatyczna instalacja jest uproszczonym sposobem tworzenia zadań dla wymuszonej instalacji aplikacji. We właściwościach grupy administracyjnej należy otworzyć listę pakietów instalacyjnych i wybrać te, które muszą zostać zainstalowane na komputerach w tej grupie. W rezultacie, wybrane pakiety instalacyjne zostaną automatycznie zainstalowane na wszystkich komputerach w tej grupie i wszystkich jej podgrupach. Przedział czasu, w trakcie którego pakiety zostaną zainstalowane, zależy od przepustowości sieci i całkowitej liczby komputerów w sieci.

Instalacja wymuszona może być zastosowana także wtedy, gdy komputery docelowe nie są dostępne bezpośrednio dla Serwera administracyjnego, na przykład: komputery znajdują się w odizolowanych sieciach lub komputery są w sieci lokalnej, a Serwer administracyjny znajduje się w strefie DMZ. Aby umożliwić instalację wymuszoną, w każdej odizolowanej sieci należy umieścić Agenty aktualizacji.

Korzystanie z Agentów aktualizacji jako lokalnych centrów instalacji jest dobrym rozwiązaniem, gdy instalacja na komputerach w podsieciach komunikujących się z Serwerem administracyjnym odbywa się poprzez wąskie kanały, a pomiędzy komputerami w tej podsieci dostępny jest szeroki kanał. Jednakże należy zauważyć, że ta metoda instalacji powoduje duże obciążenie komputerów pełniących role Agentów aktualizacji. Dlatego też zalecane jest wybranie jako Agentów aktualizacji mocniejszych komputerów z jednostkami przechowywania danych o wysokim poziomie wydajności. Co więcej, wolna przestrzeń na dysku, na którym znajduje się folder *%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit*, musi przekraczać wielokrotnie całkowity rozmiar pakietów dystrybucyjnych zainstalowanych aplikacji (sekcja "Określanie przestrzeni dyskowej dla Agenta aktualizacji" na stronie 140).

Uruchamianie pakietów autonomicznych utworzonych przez Kaspersky Security Center

Powyżej opisane metody wstępnej zdalnej instalacji Agenta sieciowego i innych aplikacji nie zawsze będą mogły zostać zaimplementowane, gdyż nie jest możliwe spełnienie wszystkich wymaganych warunków. W takich przypadkach można utworzyć standardowy plik wykonywalny zwany *autonomicznym pakietem instalacyjnym* poprzez Kaspersky Security Center, korzystając z pakietów instalacyjnych z odpowiednimi ustawieniami instalacji, które zostały przygotowane przez administratora. Autonomiczny pakiet instalacyjny jest przechowywany w folderze współdzielonym Kaspersky Security Center.

Korzystając z Kaspersky Security Center, możesz wysłać do wybranych użytkowników wiadomość e-mail zawierającą odnośnik do tego pliku w folderze współdzielonym oraz prośbę o jego

uruchomienie (w trybie interaktywnym lub z przełącznikiem "-s" dla cichej instalacji). Do wiadomości e-mail możesz załączyć autonomiczny pakiet instalacyjny, a następnie wysłać ją do użytkowników komputerów, którzy nie mają dostępu do folderu współdzielonego Kaspersky Security Center. Administrator może skopiować pakiet autonomiczny na urządzenie zewnętrzne, dostarczyć go na odpowiedni komputer, a następnie uruchomić go.

Pakiet autonomiczny można utworzyć z pakietu Agenta sieciowego, pakietu innej aplikacji (na przykład, antywirusowej) lub z obu pakietów. Jeśli pakiet autonomiczny został utworzony z pakietu Agenta sieciowego i innej aplikacji, instalacja rozpocznie się z Agenta sieciowego.

Podczas tworzenia pakietu autonomicznego z pakietu Agenta sieciowego możesz określić grupę administracyjną, do której nowe komputery (te, które nie zostały przydzielone do żadnej grupy administracyjnej) zostaną automatycznie przeniesione po zakończeniu instalacji Agenta sieciowego na tych komputerach.

Pakiety autonomiczne mogą być uruchomione w trybie interaktywnym (opcja domyślna), wyświetlając wynik instalacji aplikacji, które zawierają, lub mogą być uruchomione w trybie cichym (z przełącznikiem "-s"). Tryb cichy może zostać użyty dla instalacji ze skryptów, na przykład, ze skryptów skonfigurowanych do uruchamiania po wdrożeniu obrazu systemu operacyjnego. Wynik instalacji w trybie cichym jest determinowany przez kod zwrotny procesu.

Opcje ręcznej instalacji aplikacji

Administratorzy lub doświadczeni użytkownicy mogą zainstalować aplikacje ręcznie w trybie interaktywnym. Mogą oni użyć oryginalnych pakietów dystrybucyjnych lub wygenerowanych z nich pakietów instalacyjnych, które są przechowywane w folderze współdzielonym Kaspersky Security Center. Domyślnie instalatory są uruchamiane w trybie interaktywnym i wyświetlają użytkownikom komunikaty z pytaniami o podanie wszystkich wymaganych wartości. Jednakże podczas uruchamiania procesu setup.exe z katalogu głównego pakietu instalacyjnego z przełącznikiem "-s", instalator zostanie uruchomiony w trybie cichym i z ustawieniami, które zostały określone podczas konfiguracji pakietu instalacyjnego.

> Podczas uruchamiania procesu setup.exe z katalogu głównego pakietu instalacyjnego, przechowywanego w folderze współdzielonym Kaspersky Security Center, pakiet zostanie najpierw skopiowany do tymczasowego folderu lokalnego, a następnie instalator aplikacji zostanie uruchomiony z folderu lokalnego.

Zdalna instalacja aplikacji na komputerach z zainstalowanym Agentem sieciowym

Jeśli na komputerze jest zainstalowany działający Agent sieciowy, połączony z nadrzędnym Serwerem administracyjnym (lub jednym z jego Serwerów podrzędnych), możesz uaktualnić Agenta sieciowego na tym komputerze do nowej wersji, a także zainstalować, uaktualnić lub usunąć z Agentem sieciowym dowolne obsługiwane aplikacje.

Tę opcję można włączyć, zaznaczając pole **Przy użyciu Agenta sieciowego** we właściwościach zadania zdalnej instalacji (sekcja "Informacje ogólne o zadaniach zdalnej instalacji aplikacji w Kaspersky Security Center" na stronie 68).

Jeśli to pole jest zaznaczone, pakiety instalacyjne z ustawieniami instalacji, zdefiniowanymi przez administratora, zostaną przesłane na komputery docelowe poprzez kanały komunikacyjne między Agentem sieciowym a Serwerem administracyjnym.

Aby zoptymalizować obciążenie na Serwerze administracyjnym oraz zminimalizować ruch pomiędzy Serwerem administracyjnym a komputerami docelowymi, należy wskazać Agenty aktualizacji w każdej sieci zdalnej lub domenie rozgłoszeniowej (sekcja "Informacje o Agentach aktualizacji" (na stronie 21) oraz sekcja Tworzenie struktury grup administracyjnych i przydzielanie Agentów aktualizacji (na stronie 50)). W tym przypadku pakiety instalacyjne oraz ustawienia instalatora są rozsyłane z Serwera administracyjnego na komputery docelowe poprzez Agenty aktualizacji.

Co więcej, możliwe jest użycie Agentów aktualizacji do transmisyjnego (multiemisja) dostarczania pakietów instalacyjnych, co pozwala znacząco zmniejszyć ruch sieciowy podczas zdalnej instalacji aplikacji.

Podczas wysyłania pakietów instalacyjnych na komputery docelowe poprzez kanały komunikacyjne między Agentami sieciowymi a Serwerem administracyjnym, wszystkie pakiety instalacyjne, które zostały przygotowane do wysłania, zostaną także zbuforowane w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Jeśli używanych jest kilka dużych pakietów instalacyjnych różnych typów oraz wykorzystywana jest duża liczba Agentów aktualizacji, rozmiar tego folderu może drastycznie się powiększyć.

Nie można ręcznie usunąć plików z folderu FTServer. Jeśli oryginalne pakiety instalacyjne zostaną usunięte, odpowiednie dane zostaną automatycznie usunięte z folderu FTServer.

Wszystkie dane otrzymane po stronie Agentów aktualizacji są zapisywane w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTClTmp.

Nie można ręcznie usunąć plików z folderu $FTClTmp. Po zakończeniu działania zadań korzystających z danych z tego folderu, jego zawartość zostanie automatycznie usunięta.

Ponieważ pakiety instalacyjne są rozsyłane poprzez kanały komunikacyjne między Serwerem administracyjnym a Agentami sieciowymi z repozytorium pośredniczącego w formacie zoptymalizowanym dla transferów sieciowych, nie można wprowadzać żadnych zmian w pakietach instalacyjnych, przechowywanych w oryginalnym folderze każdego pakietu instalacyjnego. Takie zmiany nie zostałyby automatycznie zarejestrowane przez Serwer administracyjny. Jeśli chcesz ręcznie zmodyfikować pliki pakietów instalacyjnych (chociaż zalecane jest unikanie takiego rozwiązania), należy zmodyfikować dowolne ustawienia pakietu instalacyjnego w Konsoli administracyjnej. Zmodyfikowanie ustawień pakietu instalacyjnego w Konsoli administracyjnej spowoduje, że Serwer administracyjny zaktualizuje obraz pakietu w pamięci podręcznej, który został przygotowany do przesłania na komputery docelowe.

Zarządzanie ponownym uruchamianiem komputerów docelowych w zadaniu zdalnej instalacji

Aby zakończyć zdalną instalację aplikacji, często wymagane jest ponowne uruchomienie komputerów (szczególnie w systemie Windows).

Jeśli korzystasz z zadania zdalnej instalacji z Kaspersky Security Center, w Kreatorze tworzenia nowego zadania lub w oknie właściwości zadania, które zostało utworzone (sekcja **Ponowne uruchomienie systemu operacyjnego**), możesz wybrać akcję, jaka zostanie wykonana, gdy wymagane będzie ponowne uruchomienie:

- **Nie uruchamiaj ponownie komputera**. W tym przypadku komputer nie zostanie automatycznie uruchomiony ponownie. Aby zakończyć instalację, należy uruchomić

komputer ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania komputerem). Informacje o przymusowym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie komputera. Opcja ta jest odpowiednia dla zadań instalacji na serwerach i innych komputerach, na których działanie ciągłe jest krytyczne.

- **Uruchom ponownie komputer**. W tym przypadku komputer jest zawsze automatycznie uruchamiany ponownie, jeśli jest to wymagane do zakończenia instalacji. Opcja jest przydatna, gdy zadania instalacji są uruchamiane na komputerach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**. W tym przypadku na komputerze klienckim wyświetlane jest przypomnienie o ponownym uruchomieniu komputera z prośbą o zrobienie tego ręcznie. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Opcja **Pytaj użytkownika o akcję** jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia komputera.

Aktualizowanie baz danych w pakiecie instalacyjnym aplikacji antywirusowej

Przed rozpoczęciem wdrażania ochrony antywirusowej należy pamiętać o możliwości aktualizacji antywirusowych baz danych (w tym modułów i łat), dostarczanych wraz z pakietem dystrybucyjnym aplikacji antywirusowej. Dobrym rozwiązaniem jest zaktualizowanie baz danych w pakiecie instalacyjnym aplikacji przed rozpoczęciem wdrożenia (na przykład przy użyciu odpowiedniego polecenia z menu kontekstowego wybranego pakietu instalacyjnego). Przedwdrożeniowa aktualizacja baz danych zmniejszy liczbę ponownych uruchomień komputera, niezbędnych do zakończenia wdrożenia ochrony antywirusowej na komputerach docelowych.

Wybieranie metody odinstalowania niekompatybilnych aplikacji podczas instalacji aplikacji antywirusowej firmy Kaspersky Lab

Instalacja aplikacji antywirusowej firmy Kaspersky Lab poprzez Kaspersky Security Center może wymagać usunięcia oprogramowania firmy trzeciej niekompatybilnego z instalowaną aplikacją. Istnieją dwa sposoby odinstalowania aplikacji innych firm.

Automatyczna dezinstalacja niekompatybilnych aplikacji przy użyciu instalatora

Ta opcja jest obsługiwana przez różne typy instalacji. Przed zainstalowaniem aplikacji antywirusowej wszystkie niekompatybilne aplikacje są usuwane automatycznie, jeśli w oknie właściwości pakietu instalacyjnego tej aplikacji antywirusowej (sekcja **Niekompatybilne aplikacje**) zaznaczono pole **Automatycznie dezinstaluj niekompatybilne aplikacje**.

Dezinstalowanie niekompatybilnych aplikacji przy użyciu dedykowanego zadania

Aby usunąć niekompatybilne aplikacje, użyj zadania **Zdalna dezinstalacja aplikacji**. Zadanie musi zostać uruchomione na komputerach docelowych zaraz przed uruchomieniem zadania instalacji aplikacji antywirusowej. Na przykład, w zadaniu instalacji możesz wybrać opcję terminarza **Po zakończeniu innego zadania**, gdzie inne zadanie to **Zdalna dezinstalacja aplikacji**.

Ta metoda dezinstalacji jest przydatna, gdy instalator aplikacji antywirusowej nie może poprawnie usunąć niekompatybilnego oprogramowania.

Korzystanie z narzędzi do zdalnej instalacji aplikacji z Kaspersky Security Center do uruchamiania odpowiednich plików wykonywalnych na zarządzanych komputerach

Korzystając z Kreatora tworzenia nowego pakietu, możesz wybrać dowolny plik wykonywalny i zdefiniować dla niego ustawienia wiersza poleceń. W tym celu należy dodać do pakietu instalacyjnego sam wybrany plik lub cały folder, w którym ten plik się znajduje. Następnie

konieczne jest utworzenie zadania zdalnej instalacji i wybranie utworzonego pakietu instalacyjnego.

Podczas wykonywania zadania, na komputerach docelowych zostanie uruchomiony określony plik wykonywalny ze zdefiniowanymi ustawieniami wiersza poleceń.

Jeśli używasz instalatorów w formacie Microsoft Windows Installer (msi), Kaspersky Security Center przeanalizuje wyniki instalacji przy użyciu standardowych narzędzi.

Jeśli dostępna jest licencja Zarządzania systemami, Kaspersky Security Center (podczas tworzenia pakietu instalacyjnego dla dowolnej obsługiwanej aplikacji w środowisku korporacyjnym) użyje także reguł do zainstalowania i przeanalizowania wyników instalacji, które znajdują się w jego aktualizowanej bazie danych.

W innym przypadku domyślne zadanie dla plików wykonywalnych poczeka na zakończenie uruchomionych procesów i wszystkich jego procesów podrzędnych. Po zakończeniu wszystkich uruchomionych procesów, zadanie zostanie zakończone pomyślnie niezależnie od kodu zwrotnego procesu instalacji. Aby zmienić zachowanie zadania, przed utworzeniem zadania należy ręcznie zmodyfikować plik .kud, który został wygenerowany przez Kaspersky Security Center w folderze nowo utworzonego pakietu instalacyjnego.

Aby zadanie nie czekało na zakończenie uruchomionych procesów, w sekcji [SetupProcessResult] ustaw wartość ustawienia Wait na 0:

```
[SetupProcessResult]

Wait=0
```

Aby zadanie czekało tylko na zakończenie uruchomionych procesów w systemie Windows, a nie na zakończenie procesów podrzędnych, w sekcji [SetupProcessResult] ustaw wartość ustawienia WaitJob na 0, na przykład:

```
[SetupProcessResult]

WaitJob=0
```

Aby zadanie zakończyło się pomyślnie lub zwróciło kod błędu w zależności od kodu zwrotnego uruchomionego procesu, w sekcji [SetupProcessResult_SuccessCodes] umieść listę pomyślnych kodów zwrotnych, na przykład:

```
[SetupProcessResult_SuccessCodes]

0=

3010=
```

W tym przypadku każdy kod inny niż te znajdujące się na liście będzie zwracany jako błąd.

W celu wyświetlenia wiersza z komentarzem na temat pomyślnego zakończenia zadania lub błędu w wynikach zadania, w sekcji [SetupProcessResult_SuccessCodes] i [SetupProcessResult_ErrorCodes] wpisz krótki opis błędów odpowiadających kodom zwrotnym procesu, na przykład:

```
[SetupProcessResult_SuccessCodes]

0= Instalacja zakończona pomyślnie

3010=Do zakończenia instalacji wymagane jest ponowne uruchomienie

[SetupProcessResult_ErrorCodes]

1602=Instalacja anulowana przez użytkownika

1603=Fatalny błąd podczas instalacji
```

W celu użycia narzędzi Kaspersky Security Center do zarządzania ponownym uruchomieniem komputera (jeśli ponowne uruchomienie jest wymagane do zakończenia działania), w sekcji [SetupProcessResult_NeedReboot] umieść listę kodów zwrotnych procesu, które wskazują na konieczność ponownego uruchomienia komputera:

```
[SetupProcessResult_NeedReboot]

3010=
```

Monitorowanie zdalnej instalacji

Aby monitorować zdalną instalację Kaspersky Security Center, a także sprawdzić dostępność aplikacji antywirusowej i Agenta sieciowego na zarządzanych komputerach, możesz obserwować kolory ikony wskaźnika o nazwie **Zdalna instalacja** znajdującej się w obszarze roboczym węzła Serwera administracyjnego w oknie głównym Konsoli administracyjnej (sekcja "Kolory ikony wskaźnika w Konsoli administracyjnej" na stronie 124).

Kolory wskaźnika odzwierciedlają bieżący stan zdalnej instalacji. Obok wskaźnika wyświetlana jest liczba komputerów, na których jest zainstalowany Agent sieciowy i aplikacje antywirusowe. Jeśli uruchomione są aktywne zadania instalacji, postęp ich wykonania możesz monitorować w tym miejscu. Jeśli zostaną zwrócone jakiekolwiek błędy instalacji, zostanie wyświetlona liczba błędów. Możesz kliknąć odnośnik, aby zapoznać się ze szczegółami dotyczącymi błędu.

Możesz także wykorzystać wykres zdalnej instalacji z obszaru roboczego folderu **Zarządzane komputery** na zakładce Grupy. Wykres odzwierciedla proces zdalnej instalacji i wyświetla liczbę komputerów bez Agenta sieciowego, z Agentem sieciowym lub z Agentem sieciowym i aplikacją antywirusową.

Więcej informacji o postępie wykonania zdalnej instalacji (lub działaniu określonego zadania instalacji) można uzyskać, otwierając okno wyników odpowiedniego zadania zdalnej instalacji. Kliknij zadanie prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Wyniki**. Zostanie otwarte okno wyników wyświetlające dwie listy: górna lista zawiera stany zadania na komputerach docelowych, natomiast dolna lista zawiera zdarzenia zadania na komputerze, który jest aktualnie wybrany na górnej liście.

Informacje o błędach zdalnej instalacji zostaną dodane do dziennika zdarzeń Kaspersky Lab na Serwerze administracyjnym. Informacje o błędach są także dostępne w odpowiednim wyborze zdarzeń, w folderze **Raporty i powiadomienia**, w podfolderze Zdarzenia.

Konfigurowanie instalatorów

Ta sekcja zawiera informacje na temat plików instalatorów Kaspersky Security Center i ustawień instalacji, a także zalecenia dotyczące instalacji Serwera administracyjnego i Agenta sieciowego w trybie cichym.

W tej sekcji:

Informacje ogólne

Instalatory komponentów Kaspersky Security Center 10 (Serwer administracyjny, Agent sieciowy i Konsola administracyjna) bazują na technologii Instalatora Windows. Pakiet msi jest podstawą instalatora. Ten format pakietów umożliwia wykorzystanie wszystkich korzyści oferowanych przez Instalator Windows: skalowalność, dostępność systemu poprawek, system transformacji, scentralizowana instalacja za pośrednictwem rozwiązań firm trzecich oraz niewidoczna rejestracja w systemie operacyjnym.

Instalacja w trybie cichym (z plikiem odpowiedzi)

Instalatory Serwera administracyjnego i Agenta sieciowego mogą pracować z plikiem odpowiedzi (ss_install.xml), w którym zintegrowane są ustawienia instalacji w trybie cichym bez udziału użytkownika. Plik ss_install.xml znajduje się w tym samym folderze co pakiet msi. Jest on używany automatycznie podczas instalacji w trybie cichym. Tryb cichej instalacji jest włączany przy użyciu parametru "/s" wiersza poleceń.

Na przykład:

```
setup.exe /s
```

Plik ss_install.xml jest wewnętrznym formatem ustawień instalatora Kaspersky Security Center. Pakiety dystrybucyjne zawierają plik ss_install.xml z domyślnymi ustawieniami.

> Nie należy ręcznie modyfikować pliku ss_install.xml. Ten plik może być modyfikowany tylko przy użyciu narzędzi Kaspersky Security Center podczas modyfikowania ustawień pakietów instalacyjnych w Konsoli administracyjnej.

Instalacja w trybie cichym (bez pliku odpowiedzi)

Agenta sieciowego można zainstalować przy użyciu jednego pakietu msi, określając wartości właściwości MSI w standardowy sposób. Ten scenariusz umożliwia zainstalowanie Agenta sieciowego przy użyciu profili grupy. Aby uniknąć konfliktów pomiędzy ustawieniami zdefiniowanymi poprzez właściwości MSI a ustawieniami zdefiniowanymi w pliku odpowiedzi, możesz wyłączyć plik odpowiedzi, ustawiając właściwość DONT_USE_ANSWER_FILE=1. Poniżej znajduje się przykład uruchomienia instalatora Agenta sieciowego z pakietem msi.

Przykład:

```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1
SERVERADDRESS=kscserver.mycompany.com
```

Możliwe jest także zdefiniowanie ustawień instalacji dla pakietu msi poprzez wcześniejsze przygotowanie pliku odpowiedzi (z rozszerzeniem .mst). To polecenie wygląda następująco:

Przykład:

```
msiexec /I "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

W jednym poleceniu można określić kilka plików odpowiedzi.

Instalacja w trybie cichym (bez pliku odpowiedzi)

Podczas uruchamiania instalacji produktów z pliku setup.exe, do pakietu msi możesz dodać wartości dowolnych właściwości MSI.

To polecenie wygląda następująco:

Przykład:

/v”PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2”

Ustawienia instalacji Serwera administracyjnego

Poniższa tabela opisuje właściwości MSI, które można skonfigurować podczas instalacji Serwera administracyjnego. Wszystkie ustawienia są opcjonalne, za wyjątkiem EULA.

Tabela 5. Właściwości MSI

Właściwość MSI	Opis	Dostępne wartości
EULA	Akceptacja warunków licencji (wymagane)	• 1 • Null
INSTALLATIONMODETYPE	Typ instalacji Serwera administracyjnego	• Standardowy • Niestandardowy
INSTALLDIR	Folder instalacyjny produktu	

Właściwość MSI	Opis	Dostępne wartości
ADDLOCAL	Lista komponentów przeznaczonych do zainstalowania (oddzielone przecinkami)	CSAdminKitServer, Nagent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86
NETRANGETYPE	Rozmiar sieci	• NRT_1_100—od 1 do 100 komputerów • NRT_100_1000—od 100 do 1 000 komputerów • NRT_GREATER_1000 – 1 000 lub więcej komputerów
SRV_ACCOUNT_TYPE	Sposób określania użytkownika dla działania usługi Serwera administracyjnego	• SrvAccountDefault – konto użytkownika zostanie utworzone automatycznie • SrvAccountUser—konto użytkownika jest określane ręcznie
SERVERACCOUNTNAME	Nazwa użytkownika dla usługi	
SERVERACCOUNTPWD	Hasło użytkownika dla usługi	
DBTYPE		• MySQL • MSSQL
MYSQLSERVERNAME	Pełna nazwa serwera MySQL server	

Właściwość MSI	Opis	Dostępne wartości
MYSQLSERVERPORT	Numer portu używanego do nawiązania połączenia z serwerem MySQL server	
MYSQLDBNAME	Nazwa bazy danych serwera MySQL server	
MYSQLACCOUNTNAME	Nazwa użytkownika nawiązującego połączenie z bazą danych serwera MySQL server	
MYSQLACCOUNTPWD	Hasło użytkownika nawiązującego połączenie z bazą danych serwera MySQL server	
MSSQLCONNECTIONTYPE	Sposób użycia bazy danych MSSQL	• InstallMSSEE – instalacja z pakietu • ChooseExisting—użycie zainstalowanego serwera
MSSQLSERVERNAME	Pełna nazwa instancji serwera SQL Server	

Właściwość MSI	Opis	Dostępne wartości
MSSQLDBNAME	Nazwa bazy danych serwera SQL server	
MSSQLAUTHTYPE	Metoda autoryzacji podczas nawiązywania połączenia z serwerem SQL Server	• Windows • SQLServer
MSSQLACCOUNTNAME	Nazwa użytkownika nawiązującego połączenie z serwerem SQL Server w trybie SQLServer	
MSSQLACCOUNTPWD	Hasło użytkownika nawiązującego połączenie z serwerem SQL Server w trybie SQLServer	

Właściwość MSI	Opis	Dostępne wartości

CREATE_SHARE_TYPE	Metoda określania folderu współdzielonego	• Create—tworzy nowy folder współdzielony. W takim przypadku należy zdefiniować następujące właściwości:
		  • SHARELOCALPATH – ścieżka dostępu do folderu lokalnego
		  • SHAREFOLDERNAME—nazwa sieciowa folderu
		• Null—należy określić właściwość EXISTSHAREFOLDERNAME

EXISTSHAREFOLDERNAME	Pełna ścieżka dostępu do istniejącego folderu współdzielonego	
SERVERPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym	
SERVERSSLPORT	Numer portu używanego do nawiązania bezpiecznego połączenia SSL z Serwerem administracyjnym	

Właściwość MSI	Opis	Dostępne wartości
SERVERADDRESS	Adres Serwera administracyjnego	
MOBILESERVERADDRESS	Adres Serwera administracyjnego do nawiązywania połączenia z urządzeniami mobilnymi; ignorowane, jeśli nie wybrano komponentu MobileSupport	

Ustawienia instalacji Agenta sieciowego

Poniższa tabela opisuje właściwości MSI, które można skonfigurować podczas instalacji Agenta sieciowego. Wszystkie ustawienia są opcjonalne, za wyjątkiem SERVERADDRESS.

Tabela 6. Właściwości MSI

Właściwość MSI	Opis	Dostępne wartości
DONT_USE_ANSWER_FILE	Odczyt ustawień instalacji z pliku odpowiedzi	• 1 • Null
INSTALLDIR	Folder instalacyjny	
INSTALL_NSAC	Czy zainstalować NAC	• 1 • Null
SERVERADDRESS	Adres Serwera administracyjnego (wymagane)	

Właściwość MSI	Opis	Dostępne wartości
SERVERPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym	
SERVERSSLPORT	Numer portu dla połączenia SSL	
USESSL	Czy użyć połączenia SSL	• 1 • Null
OPENUDPPORT	Czy otworzyć port UDP	• 1 • Null
UDPPORT	Numer portu UDP	
USEPROXY	Czy użyć serwera proxy	• 1 • Null
PROXYADDRESS	Adres Proxy	
PROXYPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym	
PROXYLOGIN	Konto używane do nawiązywania połączenia z serwerem proxy	
PROXYPASSWORD	Hasło do konta używanego do nawiązywania połączenia z serwerem proxy	

Właściwość MSI	Opis	Dostępne wartości
GATEWAYMODE	Tryb użycia bramy połączenia	• 0 – nie używaj bramy połączenia • 1—użyj tego Agenta sieciowego jako bramy połączenia • 2—połącz z Serwerem administracyjnym przy użyciu bramy połączenia
GATEWAYADDRESS	Adres bramy połączenia	
CERTSELECTION	Metoda pobierania certyfikatu	• GetOnFirstConnection—uzyskaj certyfikat z Serwera administracyjnego • GetExistent—wybierz istniejący certyfikat. Jeśli ta opcja zostanie wybrana, należy zdefiniować właściwość CERTFILE.
CERTFILE	Ścieżka do pliku certyfikatu	
VMVDI	Włącz tryb dynamiczny dla wirtualnej infrastruktury pulpitu Virtual Desktop Infrastructure (VDI).	• 1 • Null
LAUNCHPROGRAM	Czy uruchomić usługę Agenta sieciowego po instalacji	• 1 • Null

Infrastruktura wirtualna

Kaspersky Security Center obsługuje użycie maszyn wirtualnych. Aplikacja obsługuje instalację Agenta sieciowego i aplikacji antywirusowej na każdej maszynie wirtualnej, a także wdrożenie ochrony maszyn wirtualnych na poziomie hipernadzorcy. W pierwszym przypadku, do ochrony maszyn wirtualnych możesz użyć zwykłej aplikacji antywirusowej lub Kaspersky Security for Virtualization / Light Agent (patrz strona http://support.kaspersky.com/pl/ksv3). W drugim przypadku ochrona maszyn wirtualnych jest realizowana przy użyciu Kaspersky Security for Virtualization / Agentless (patrz strona http://support.kaspersky.com/pl/ksv3nola).

Począwszy od wersji 10 MR1, Kaspersky Security Center obsługuje opcję przywracania poprzedniego stanu maszyn wirtualnych (sekcja "Obsługa przywracania systemu plików dla komputerów z zainstalowanym Agentem sieciowym" na stronie 98).

W tej sekcji:

Wskazówki dotyczące zmniejszenia obciążenia na maszynach wirtualnych

Podczas instalacji Agenta sieciowego na maszynie wirtualnej zalecane jest rozważenie wyłączenia funkcji Kaspersky Security Center, które nie będą zbyt przydatne dla maszyn wirtualnych.

Podczas instalacji Agenta sieciowego na maszynie wirtualnej lub na szablonie przeznaczonym do wygenerowania maszyn wirtualnych, dobrym rozwiązaniem jest wykonanie następujących czynności:

- Jeśli uruchamiasz zadanie zdalnej instalacji, w oknie właściwości pakietu instalacyjnego Agenta sieciowego (sekcja **Zaawansowane**) zaznacz pole **Optymalizuj ustawienia dla wirtualnej infrastruktury pulpitu VDI (Virtual Desktop Infrastructure)**.

- Jeśli uruchamiasz instalację w trybie interaktywnym z udziałem Kreatora, w oknie Kreatora zaznacz pole **Optymalizuj ustawienia Agenta sieciowego dla infrastruktury wirtualnej**.

Zaznaczenie tych pól spowoduje zmianę ustawień Agenta sieciowego w taki sposób, że poniższe funkcje pozostaną domyślnie wyłączone (przed zastosowaniem profilu):

- Zbieranie informacji o zainstalowanym oprogramowaniu
- Zbieranie informacji o sprzęcie
- Zbieranie informacji o wykrytych lukach
- Zbieranie informacji o wymaganych aktualizacjach.

Zazwyczaj te funkcje nie są potrzebne na maszynach wirtualnych, gdyż wykorzystują stałe oprogramowanie i sprzęt wirtualny.

Wyłączenie tych funkcji jest odwracalne. Jeśli jakakolwiek z wyłączonych funkcji jest potrzebna, możesz ją włączyć poprzez profil Agenta sieciowego lub poprzez ustawienia lokalne Agenta sieciowego. Ustawienia lokalne Agenta sieciowego są dostępne poprzez menu kontekstowe odpowiedniego komputera w Konsoli administracyjnej.

Obsługa dynamicznych maszyn wirtualnych

Kaspersky Security Center obsługuje dynamiczne maszyny wirtualne. Jeśli w sieci firmowej została wdrożona infrastruktura wirtualna, w pewnych przypadkach możliwe będzie korzystanie z dynamicznych (tymczasowych) maszyn wirtualnych. Dynamiczne maszyny wirtualne są tworzone pod unikatowymi nazwami w oparciu o szablony, które zostały przygotowane przez administratora. Użytkownik pracuje na maszynie wirtualnej przez jakiś czas, a następnie, po wyłączeniu maszyny zostanie ona usunięta z infrastruktury wirtualnej. Jeśli w sieci firmowej jest zainstalowany program Kaspersky Security Center, maszyna wirtualna z zainstalowanym Agentem sieciowym zostanie dodana do bazy danych Serwera administracyjnego. Po wyłączeniu maszyny wirtualnej, odpowiedni wpis musi także zostać usunięty z bazy danych Serwera administracyjnego.

Aby funkcja automatycznego usuwania wpisów na temat maszyn wirtualnych mogła działać, podczas instalacji Agenta sieciowego na szablonie dla dynamicznych maszyn wirtualnych zaznacz pole **Włącz tryb dynamiczny dla VDI**:

- Dla zdalnej instalacji—w oknie właściwości pakietu instalacyjnego Agenta sieciowego (sekcja **Zaawansowane**)
- Dla instalacji w trybie interaktywnym—w oknie Kreatora instalacji Agenta sieciowego.

> Staraj się unikać zaznaczania opcji **Włącz tryb dynamiczny dla VDI** podczas instalacji Agenta sieciowego na komputerach fizycznych.

Jeśli chcesz, żeby zdarzenia z dynamicznych maszyn wirtualnych były przechowywane na Serwerze administracyjnym przez jakiś czas po usunięciu tych maszyn wirtualnych, w oknie właściwości Serwera administracyjnego, w sekcji **Repozytorium zdarzeń** zaznacz pole **Przechowuj zdarzenia po usunięciu komputerów** i określ maksymalny czas przechowywania zdarzeń (w dniach).

Obsługa kopiowania maszyn wirtualnych

Kopiowanie maszyn wirtualnych z zainstalowanym Agentem sieciowym lub tworzenie maszyny wirtualnej z szablonu z zainstalowanym Agentem sieciowym odbywa się w ten sam sposób co zdalna instalacja Agenta sieciowego poprzez przechwycenie i skopiowanie obrazu dysku twardego. Dlatego też, podczas kopiowania maszyn wirtualnych zazwyczaj postępuje się podobnie jak podczas zdalnej instalacji, kopiując obraz dysku (sekcja "Zdalna instalacja poprzez przechwycenie i skopiowanie obrazu dysku twardego komputera" na stronie 69).

Jednakże w dwóch poniższych przypadkach Agent sieciowy automatycznie wykrywa kopiowanie, dzięki czemu nie ma potrzeby wykonywania wszystkich skomplikowanych działań wymienionych w sekcji "Zdalna instalacja poprzez przechwycenie i skopiowanie obrazu dysku twardego komputera".

- Pole **Włącz tryb dynamiczny dla VDI** zostało zaznaczone po zainstalowaniu Agenta sieciowego—po każdym ponownym uruchomieniu systemu operacyjnego ta maszyna wirtualna będzie rozpoznawana jako nowy komputer, niezależnie do tego, czy została skopiowana.

- Używany jest jeden z następujących hipernadzorców: VMware™, HyperV® lub Xen®: Agent sieciowy wykrywa kopiowanie maszyny wirtualnej po zmienionym numerze ID sprzętu wirtualnego.

Analiza zmian w sprzęcie wirtualnym nie jest całkowicie wiarygodna. Przed szerszym zastosowaniem tej metody należy ją sprawdzić na małej puli maszyn wirtualnych dla wersji hipernadzorcy, który jest aktualnie używany w firmie.

Obsługa przywracania systemu plików dla komputerów z zainstalowanym Agentem sieciowym

Kaspersky Security Center jest aplikacją oferującą wiele funkcji. Przywrócenie poprzedniego stanu systemu plików na komputerze z zainstalowanym Agentem sieciowym doprowadzi do desynchronizacji danych i niepoprawnego działania Kaspersky Security Center.

Wycofanie systemu plików (lub jego części) może zostać wykonane w następujących przypadkach:

- Podczas kopiowania obrazu dysku twardego
- Podczas przywracania stanu maszyny wirtualnej przy użyciu infrastruktury wirtualnej
- Podczas przywracania danych z kopii zapasowej lub punktu odzyskiwania

Scenariusze, w których oprogramowanie firm trzecich na komputerach z zainstalowanym Agentem sieciowym wpływa na zawartość folderu %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\, są dla Kaspersky Security Center tylko krytycznymi scenariuszami. Dlatego też, jeśli to tylko możliwe, powinieneś zawsze wykluczać ten folder z procedury odzyskiwania.

Ponieważ zasady działania niektórych firm dopuszczają możliwość wycofania systemu plików komputerów, obsługa wycofania systemu plików na komputerach z zainstalowanym Agentem sieciowym jest dostępna w Kaspersky Security Center od wersji 10 MR1 (Serwer administracyjny i Agenty sieciowe muszą być w wersjach 10 MR1 lub nowszych). Po wykryciu takich komputerów są one automatycznie ponownie łączone z Serwerem administracyjnym z całkowitym wyczyszczeniem danych i pełną synchronizacją.

Domyślnie obsługa wykrywania wycofania systemu plików jest wyłączona w Kaspersky Security Center 10 MR1.

Aby włączyć tę funkcję, należy zaimportować plik reg (przedstawiony w poniższym przykładzie) do rejestru i uruchomić ponownie usługę Serwera administracyjnego.

System operacyjny na komputerze, na którym jest zainstalowany Serwer administracyjny (32-bitowy):

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]

“KLSRV_HST_VM_REVERT_DETECTION”=dword:00000001
```

System operacyjny na komputerze, na którym jest zainstalowany Serwer administracyjny (64-bitowy):

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Products\1093\1.0.0.0\ServerFlags]

“KLSRV_HST_VM_REVERT_DETECTION”=dword:00000001
```

Domyślnie obsługa wykrywania wycofania stanu systemu plików jest włączona w Kaspersky Security Center 10 Service Pack 2.

Jeśli jest to tylko możliwe, unikaj przywracania poprzedniego stanu folderu %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ na komputerach z zainstalowanym Agentem sieciowym, gdyż całkowita ponowna synchronizacja danych zużywa dużą ilość zasobów.

Wycofanie stanu systemu jest całkowicie zabronione na komputerze z zainstalowanym Serwerem administracyjnym. Podobnie jest w przypadku wycofania baz danych używanych przez Serwer administracyjny.

Stan Serwera administracyjnego można przywrócić z kopii zapasowej tylko przy użyciu standardowego narzędzia klbackup (sekcja "Tworzenie kopii zapasowej i przywracanie ustawień Serwera administracyjnego" na stronie 59).

Konfigurowanie profili połączenia dla użytkowników mobilnych

Mobilni użytkownicy laptopów (zwanych dalej również "komputerami") mogą potrzebować zmiany metody łączenia się z Serwerem administracyjnym lub przełączania pomiędzy Serwerami administracyjnymi w zależności od aktualnej lokalizacji komputera w sieci firmowej.

Używanie różnych adresów jednego Serwera administracyjnego

Procedura opisana poniżej jest stosowana tylko do Kaspersky Security Center 10 Service Pack 1 i nowszych wersji.

Komputery z zainstalowanym Agentem sieciowym mogą łączyć się z Serwerem administracyjnym z poziomu wewnętrznej sieci firmowej lub internetu. W tej sytuacji wymagane może być, aby Agent sieciowy używał innych adresów do łączenia się z Serwerem administracyjnym: zewnętrznego adresu Serwera administracyjnego dla połączenia internetowego oraz wewnętrznego adresu Serwera administracyjnego dla wewnętrznego połączenia sieciowego.

W tym celu musisz dodać profil (dla połączenia z Serwerem administracyjnym z poziomu internetu) do profilu Agenta sieciowego. Dodaj profil we właściwościach profilu (sekcja **Sieć**, podsekcja **Połączenie**). W tym samym czasie, w oknie tworzenia profilu musisz odznaczyć pole **Użyj tylko do pobierania uaktualnień** i zaznaczyć opcję **Zsynchronizuj ustawienia połączenia z ustawieniami Serwera określonymi w tym profilu**. Jeśli do łączenia się z Serwerem administracyjnym używasz bramy połączenia (na przykład, w konfiguracji Kaspersky Security Center, opisanej w sekcji "Dostęp do internetu: Agent sieciowy w trybie bramy w strefie

zdemilitaryzowanej (DMZ)" (na stronie 17)), w odpowiednim polu profilu połączenia musisz określić adres bramy połączenia.

Przełączanie pomiędzy Serwerami administracyjnymi w zależności od aktualnej sieci

> Procedura opisana poniżej jest stosowana tylko do Kaspersky Security Center 10 MR 1 i nowszych wersji.

Jeśli organizacja posiada kilka biur z różnymi Serwerami administracyjnymi, a niektóre komputery z zainstalowanym Agentem sieciowym są przenoszone pomiędzy nimi, Agent sieciowy musi łączyć się z Serwerem administracyjnym sieci lokalnej w biurze, w którym znajduje się komputer.

W tej sytuacji konieczne jest utworzenie profilu dla połączenia z Serwerem administracyjnym we właściwościach profilu Agenta sieciowego dla każdego z biur, za wyjątkiem głównego biura, w którym znajduje się oryginalny macierzysty Serwer administracyjny. W profilach połączenia należy określić adresy Serwerów administracyjnych i zaznaczyć lub odznaczyć pole **Użyj tylko do pobierania uaktualnień**:

- Zaznacz to pole, jeśli chcesz, aby Agent sieciowy zsynchronizował się z macierzystym Serwerem administracyjnym, a Serwer lokalny był używany tylko do pobierania uaktualnień.
- Usuń zaznaczenie z tego pola, jeśli Agent sieciowy ma być całkowicie zarządzany przez lokalny Serwer administracyjny.

Następnie powinieneś ustalić warunki przełączania do nowo utworzonych profili: przynajmniej jeden warunek dla każdego z biur, za wyjątkiem głównego biura. Celem każdego warunku jest wykrycie elementów, które są specyficzne dla środowiska sieciowego w biurze. Jeśli warunek jest prawdziwy, odpowiedni profil zostaje aktywowany. Jeśli żaden z warunków nie jest prawdziwy, Agent sieciowy przełączy się do macierzystego Serwera administracyjnego.

Zobacz również:

Umożliwianie uzyskania dostępu do Serwera administracyjnego przez internet..... 14

Dostęp do internetu: Agent sieciowy w trybie bramy w strefie zdemilitaryzowanej (DMZ)..... 17

Wdrażanie funkcji Zarządzanie urządzeniami mobilnymi

W tej sekcji:

Instalowanie serwera urządzeń mobilnych Exchange ActiveSync

Konfigurowanie serwera sieciowego Internetowych usług informacyjnych

Podczas korzystania z Microsoft Exchange Server (wersji 2010 i 2013), w ustawieniach serwera sieciowego Internetowych usług informacyjnych (IIS) należy aktywować mechanizm Uwierzytelniania systemu Windows dla katalogu wirtualnego Windows PowerShell™. Ten mechanizm uwierzytelniania jest aktywowany automatycznie, jeśli w Kreatorze instalacji serwera urządzeń mobilnych Exchange ActiveSync zaznaczone jest pole **Automatyczna konfiguracja IIS** (jest to domyślna opcja).

W innych sytuacjach należy samodzielnie aktywować ten mechanizm uwierzytelniania.

► *W celu ręcznego aktywowania mechanizmu Uwierzytelniania systemu Windows dla katalogu wirtualnego PowerShell:*

1. W konsoli Menedżera internetowych usług informacyjnych (IIS) otwórz właściwości katalogu wirtualnego PowerShell.

2. Przejdź do sekcji **Uwierzytelnianie**.
3. Wybierz **Uwierzytelnianie systemu Windows**, a następnie kliknij przycisk **Włącz**.
4. Otwórz **Ustawienia zaawansowane**.
5. Zaznacz pole **Włącz uwierzytelnianie trybu jądra**.
6. Z listy rozwijalnej **Ochrona rozszerzona** wybierz **Wymagana**.

Jeśli używany jest Microsoft Exchange Server 2007, serwer sieciowy IIS nie wymaga konfiguracji.

Lokalna instalacja serwera urządzeń mobilnych Exchange ActiveSync

W celu przeprowadzenia lokalnej instalacji serwera urządzeń mobilnych Exchange ActiveSync, administrator musi wykonać następujące działania:

1. Skopiować zawartość folderu \Server\Packages\MDM4Exchange\ z pakietu dystrybucyjnego Kaspersky Security Center na komputer kliencki.
2. Uruchomić plik wykonywalny setup.exe.

Lokalna instalacja uwzględnia dwa typy instalacji:

- Standardowa instalacja jest uproszczoną instalacją, która nie wymaga od administratora określenia żadnych ustawień. Zalecana jest w większości przypadków.
- Rozszerzona instalacja wymaga od administratora określenia następujących ustawień:
  - Ścieżki dostępu dla instalacji serwera urządzeń mobilnych Exchange ActiveSync
  - Trybu działania dla instalacji serwera urządzeń mobilnych Exchange ActiveSync: tryb standardowy lub tryb klastra (sekcja "Instalowanie serwera urządzeń mobilnych Exchange ActiveSync" na stronie 26)
  - Możliwości określenia konta, z poziomu którego zostanie uruchomiona usługa serwera urządzeń mobilnych Exchange ActiveSync (sekcja "Konto dla usługi Exchange ActiveSync" na stronie 27)

- Włączenie / wyłączenie automatycznej konfiguracji serwera sieciowego IIS.

Kreator instalacji serwera urządzeń mobilnych Exchange ActiveSync musi zostać uruchomiony z poziomu konta, które posiada wszystkie wymagane uprawnienia (sekcja "Uprawnienia wymagane do zainstalowania serwera urządzeń mobilnych Exchange ActiveSync" na stronie 27).

Zdalna instalacja serwera urządzeń mobilnych Exchange ActiveSync

► *W celu skonfigurowania zdalnej instalacji serwera urządzeń mobilnych Exchange ActiveSync, administrator musi wykonać następujące działania:*

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz folder **Zdalna instalacja**, a następnie podfolder **Pakiety instalacyjne**.

2. W podfolderze **Pakiety instalacyjne** otwórz właściwości pakietu **Exchange ActiveSync Mobile Device Server**.

3. Przejdź do sekcji **Ustawienia**.

   Ta sekcja zawiera te same ustawienia, które są używane w lokalnej instalacji produktu.

Po skonfigurowaniu zdalnej instalacji, możesz uruchomić instalację serwera urządzeń mobilnych Exchange ActiveSync.

► *W celu zainstalowania serwera urządzeń mobilnych Exchange ActiveSync:*

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz folder **Zdalna instalacja**, a następnie podfolder **Pakiety instalacyjne**.

2. W podfolderze **Pakiety instalacyjne** wybierz pakiet **Exchange ActiveSync Mobile Device Server**.

3. Otwórz menu kontekstowe pakietu i wybierz **Zainstaluj aplikację**.

4. W uruchomionym Kreatorze zdalnej instalacji wybierz komputer (lub kilka komputerów dla instalacji w trybie klastra).

5. W polu **Uruchom instalator aplikacji z poziomu określonego konta** określ konto, z poziomu którego na zdalnym komputerze zostanie uruchomiony proces instalacji.

To konto musi posiadać wszystkie wymagane uprawnienia (sekcja "Uprawnienia wymagane do zainstalowania serwera urządzeń mobilnych Exchange ActiveSync" na stronie 27).

Instalowanie serwera urządzeń mobilnych iOS MDM

Liczba kopii serwera urządzeń mobilnych iOS MDM przeznaczonych do zainstalowania może zostać wybrana w oparciu o dostępny sprzęt lub całkowitą liczbę urządzeń mobilnych.

Jednakże należy pamiętać, że zalecana maksymalna liczba urządzeń mobilnych dla pojedynczej instalacji Kaspersky Mobile Device Management wynosi 50 000. Aby zmniejszyć obciążenie, cała pula urządzeń może zostać rozesłana na kilka serwerów, na których jest zainstalowany serwer urządzeń mobilnych iOS MDM.

Autoryzacja urządzeń iOS MDM odbywa się poprzez certyfikaty użytkownika (każdy profil zainstalowany na urządzeniu zawiera certyfikat właściciela urządzenia). Dla serwera urządzeń mobilnych iOS MDM dostępne są dwa schematy wdrożenia:

- Uproszczony schemat instalacji
- Schemat zdalnej instalacji z użyciem delegowania protokołu Kerberos (KCD)

Oba schematy zostały opisane poniżej.

Uproszczony schemat instalacji

Podczas zdalnej instalacji serwera urządzeń mobilnych iOS MDM z użyciem uproszczonego schematu instalacji, urządzenia mobilne łączą się bezpośrednio z usługą sieciową iOS MDM. W tym przypadku certyfikaty użytkownika wydane przez Serwer administracyjny mogą być stosowane tylko do autoryzacji urządzeń. Integracja z infrastrukturą kluczy publicznych (PKI) jest niemożliwa dla certyfikatów użytkownika (sekcja "Standardowa konfiguracja: Kaspersky Mobile Device Management w strefie DMZ" na stronie 31).

Schemat zdalnej instalacji z użyciem delegowania protokołu Kerberos (KCD)

Schemat zdalnej instalacji z użyciem delegowania protokołu Kerberos (KCD) wymaga, aby Serwer administracyjny oraz serwer urządzeń mobilnych iOS MDM znajdował się w wewnętrznej sieci firmowej.

Ten schemat instalacji obejmuje:

- Integrację z Microsoft Forefront TMG
- Użycie KCD do autoryzacji urządzeń mobilnych
- Integrację z PKI do stosowania certyfikatów użytkownika

Podczas korzystania z tego schematu zdalnej instalacji należy:

- W Konsoli administracyjnej, w ustawieniach usługi sieciowej iOS MDM zaznaczyć pole **Zapewnij kompatybilność z Kerberos Constrained Delegation**.
- Jako certyfikat dla usługi sieciowej iOS MDM określić certyfikat niestandardowy, który został zdefiniowany, gdy usługa sieciowa iOS MDM została opublikowana na TMG.
- Certyfikaty użytkownika dla urządzeń iOS muszą być wystawione przez urząd certyfikacji (CA) domeny. Jeśli domena zawiera kilka głównych urzędów certyfikacji, certyfikaty użytkownika muszą być wystawione przez urząd certyfikacji, który został określony, gdy usługa sieciowa iOS MDM została opublikowana na TMG.

  Możesz zapewnić, że certyfikat użytkownika jest zgodny z wymaganiami wystawiania certyfikatów urzędu certyfikacji przy użyciu jednej z następujących metod:

  - Określ certyfikat użytkownika w Kreatorze nowego profilu iOS MDM oraz w Kreatorze instalacji certyfikatu.
  - Zintegruj Serwer administracyjny z infrastrukturą kluczy publicznych domeny oraz zdefiniuj odpowiednie ustawienie w regułach wystawiania certyfikatów:

    1. W Konsoli administracyjnej, w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi / Certyfikaty** kliknij odnośnik **Integruj z infrastrukturą kluczy publicznych**, aby przejść do okna **Reguły wystawiania certyfikatów**.

2. W sekcji **Integracja z PKI** skonfiguruj integrację z infrastrukturą kluczy publicznych.
3. W sekcji **Generowanie certyfikatów ogólnego typu** określ źródło certyfikatów.

Zobacz sekcje:

- Standardowa konfiguracja: Kaspersky Mobile Device Management w lokalnej sieci firmy (sekcja "Standardowa konfiguracja: serwer urządzeń mobilnych iOS MDM w sieci lokalnej firmy" na stronie 32).
- Integracja z PKI (infrastruktura kluczy publicznych) (sekcja "Integracja z infrastrukturą kluczy publicznych" na stronie 116)

Poniżej znajduje się przykład konfiguracji delegowania protokołu Kerberos (KCD) z następującymi założeniami:

- Usługa sieciowa iOS MDM działa na porcie 443.
- Nazwa komputera z TMG to tmg.mydom.local.
- Nazwa komputera z usługą sieciową iOS MDM to iosmdm.mydom.local.
- Nazwa zewnętrznej publikacji usługi sieciowej iOS MDM to iosmdm.mydom.global.

Nazwa główna usługi dla http/iosmdm.mydom.local

W domenie należy zarejestrować nazwę główną usługi (SPN) dla komputera z usługą sieciową iOS MDM (iosmdm.mydom.local):

setspn -a http/iosmdm.mydom.local iosmdm

Konfigurowanie właściwości domeny komputera z TMG (tmg.mydom.local)

Aby przeprowadzić ruch sieciowy, przełącz komputer z TMG (tmg.mydom.local) do usługi, która jest definiowana po SPN (http/iosmdm.mydom.local).

W celu przełączenia komputera z TMG do usługi definiowanej po SPN (http/iosmdm.mydom.local), administrator musi wykonać następujące działania:

1. W przystawce programu MMC o nazwie "Użytkownicy i komputery usługi Active Directory" wybierz komputer z zainstalowanym TMG (tmg.mydom.local).

2. We właściwościach komputera, na zakładce **Delegowanie** ustaw przełącznik **Ufaj temu komputerowi w delegowaniu tylko do określonych usług** na **Użyj dowolnego protokołu uwierzytelniania**.

3. Dodaj SPN (http/iosmdm.mydom.local) do listy **Usługi, którym to konto może przedstawiać delegowane poświadczenia**.

Specjalny (niestandardowy) certyfikat dla opublikowanej usługi sieciowej (iosmdm.mydom.global)

Konieczne jest opublikowanie specjalnego (niestandardowego) certyfikatu dla usługi sieciowej iOS MDM na FQDN iosmdm.mydom.global i określić w Konsoli administracyjnej, w ustawieniach usługi sieciowej iOS MDM, że zastępuje on domyślny certyfikat.

Należy pamiętać, że kontener certyfikatów (plik z rozszerzeniem .p12 lub .pfx) musi także zawierać łańcuch certyfikatów głównych (klucze publiczne).

Publikowanie usługi sieciowej iOS MDM na TMG

Na TMG, dla ruchu przechodzącego z urządzenia mobilnego do portu 443 usługi iosmdm.mydom.global należy skonfigurować KCD na SPN (http/iosmdm.mydom.local), korzystając z certyfikatu opublikowanego dla FQDN (iosmdm.mydom.global). Nie można zapominać, że publikacja oraz opublikowana usługa sieciowa powinny korzystać z tego samego certyfikatu serwera.

Konfigurowanie dostępu do usługi Apple Push Notification

W celu zapewnienia poprawnego działania usługi sieciowej iOS MDM oraz reakcji urządzeń w odpowiednim momencie na polecenia administratora, w ustawieniach serwera urządzeń mobilnych iOS MDM należy określić certyfikat Apple Push Notification Service (zwany dalej certyfikatem APN).

Więcej informacji dotyczących pobierania certyfikatu APN można znaleźć w artykule w Bazie wiedzy, dostępnym na stronie pomocy technicznej: http://support.kaspersky.com/pl/11077.

Podczas interakcji z Apple Push Notification (zwane dalej APN) usługa sieciowa iOS MDM łączy się z zewnętrznym adresem gateway.push.apple.com poprzez port 2195 (wychodzący). Dlatego

też, usługa sieciowa iOS MDM wymaga dostępu do portu TCP 2195 dla zakresu adresów 17.0.0.0/8. Ze strony urządzenia iOS możliwy jest dostęp do portu TCP 5223 dla zakresu adresów 17.0.0.0/8.

Jeśli chcesz uzyskać dostęp do APN ze strony usługi sieciowej iOS MDM poprzez serwer proxy, na komputerze z zainstalowaną usługą sieciową iOS MDM musisz wykonać następujące działania:

1. Dodaj do rejestru następujące wiersze:

   - W 32-bitowych systemach operacyjnych:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset]

"ApnProxyHost"="<Nazwa Hosta Proxy>"

"ApnProxyPort"="<Port Proxy>"

"ApnProxyLogin"="<Login Proxy>"

"ApnProxyPwd"="<Hasło Proxy>"
```

   - W 64-bitowych systemach operacyjnych:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset]

"ApnProxyHost"="<Nazwa Hosta Proxy>"

"ApnProxyPort"="<Port Proxy>"

"ApnProxyLogin"="<Login Proxy>"

"ApnProxyPwd"="<Hasło Proxy>"
```

2. Uruchom ponownie usługę sieciową iOS MDM.

Połączenie urządzeń KES z Serwerem administracyjnym

W zależności od metody używanej do łączenia urządzeń z Serwerem administracyjnym, dla Kaspersky Mobile Device Management istnieją dwa schematy zdalnej instalacji na urządzeniach KES:

- Schemat zdalnej instalacji z bezpośrednim połączeniem urządzeń z Serwerem administracyjnym
- Schemat zdalnej instalacji uwzględniający TMG

Bezpośrednie połączenie urządzeń z Serwerem administracyjnym

Urządzenia KES mogą łączyć się bezpośrednio z portem 13292 Serwera administracyjnego.

W zależności od metody używanej do autoryzacji, dla połączenia urządzeń KES z Serwerem administracyjnym możliwe są dwie opcje:

- Łączenie urządzeń z użyciem certyfikatu użytkownika
- Łączenie urządzeń bez użycia certyfikatu użytkownika

Łączenie urządzeń z użyciem certyfikatu użytkownika

Podczas łączenia urządzeń z użyciem certyfikatu użytkownika, to urządzenie jest kojarzone z kontem użytkownika, do którego odpowiedni certyfikat został przypisany poprzez narzędzia Serwera administracyjnego.

W tym przypadku używane będzie dwukierunkowe uwierzytelnianie SSL (uwierzytelnianie obustronne) - Serwer administracyjny i urządzenie będą uwierzytelniani przy użyciu certyfikatów.

Łączenie urządzeń bez użycia certyfikatu użytkownika

Podczas łączenia urządzenia bez użycia certyfikatu użytkownika, to urządzenie nie jest kojarzone z żadnym kontem użytkownika na Serwerze administracyjnym. Jednakże, gdy urządzenie pobierze dowolny certyfikat, to urządzenie zostanie skojarzone z kontem użytkownika, do którego odpowiedni certyfikat został przypisany poprzez narzędzia Serwera administracyjnego.

Podczas łączenia tego urządzenia z Serwerem administracyjnym zostanie zastosowane jednokierunkowe uwierzytelnianie SSL, co oznacza, że tylko Serwer administracyjny będzie uwierzytelniony przy użyciu certyfikatu. Po pobraniu przez urządzenie certyfikatu użytkownika, typ autoryzacji zmieni się na dwukierunkowe uwierzytelnianie SSL (uwierzytelnianie obustronne) (sekcja "Umożliwianie uzyskania dostępu do Serwera administracyjnego przez internet" na stronie 14).

Schemat łączenia urządzeń KES z Serwerem wykorzystujący delegowanie protokołu Kerberos (KCD)

Schemat łączenia urządzeń KES z Serwerem wykorzystujący delegowanie protokołu Kerberos (KCD) uwzględnia:

- Integrację z Microsoft Forefront TMG
- Użycie delegowania protokołu Kerberos (zwane również KCD) do uwierzytelnia urządzeń mobilnych
- Integrację z infrastrukturą kluczy publicznych (zwana również PKI) w celu zastosowania certyfikatów użytkownika.

Podczas korzystania z tego schematu połączenia należy pamiętać, że:

- Typem połączenia urządzeń KES z TMG ma być "dwukierunkowe uwierzytelnianie SSL", czyli urządzenie musi łączyć się z TMG poprzez swój własny certyfikat użytkownika. W tym celu należy zintegrować certyfikat użytkownika z pakietem instalacyjnym programu Kaspersky Endpoint Security for Android, który został zainstalowany na urządzeniu. Ten pakiet KES musi być utworzony przez Serwer administracyjny specjalnie dla tego urządzenia (użytkownika).
- Dla protokołu mobilnego powinieneś określić specjalny (niestandardowy) certyfikat zamiast domyślnego certyfikatu serwera:

    1. W oknie właściwości Serwera administracyjnego, w sekcji **Ustawienia** zaznacz pole **Otwórz port dla urządzeń mobilnych**, a następnie z listy rozwijalnej wybierz **Dodaj certyfikat...**.

2. W otwartym oknie określ ten sam certyfikat, który został ustawiony na TMG, gdy punkt dostępu do protokołu mobilnego został opublikowany na Serwerze administracyjnym.

- Certyfikaty użytkownika dla urządzeń KES muszą być wystawione przez urząd certyfikacji (CA) domeny. Należy pamiętać, że jeśli domena zawiera kilka głównych urzędów certyfikacji, certyfikaty użytkownika muszą być wystawione przez urząd certyfikacji, który został ustawiony w publikacji na TMG.

  Możesz upewnić się, że certyfikat użytkownika jest zgodny z wyżej opisanymi wymaganiami przy użyciu jednej z następujących metod:

  - Określ specjalny certyfikat użytkownika w Kreatorze nowego pakietu instalacyjnego oraz w Kreatorze instalacji certyfikatu.

  - Zintegruj Serwer administracyjny z infrastrukturą kluczy publicznych domeny oraz zdefiniuj odpowiednie ustawienie w regułach wystawiania certyfikatów:

    1. W Konsoli administracyjnej, w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi / Certyfikaty** kliknij odnośnik **Integruj z infrastrukturą kluczy publicznych**, aby przejść do okna **Reguły wystawiania certyfikatów**.
    2. W sekcji **Integracja z PKI** skonfiguruj integrację z infrastrukturą kluczy publicznych.
    3. W sekcji **Generowanie certyfikatów ogólnego typu** określ źródło certyfikatów.

Zobacz sekcje:

- Integracja z PKI (infrastruktura kluczy publicznych) (sekcja "Integracja z infrastrukturą kluczy publicznych" na stronie 116)

- Umożliwianie uzyskania dostępu do Serwera administracyjnego przez internet (na stronie 14).

Poniżej znajduje się przykład konfiguracji delegowania protokołu Kerberos (KCD) z następującymi założeniami:

- Punkt dostępu do protokołu mobilnego po stronie Serwera administracyjnego jest ustawiony na porcie 13292

- Nazwa komputera z TMG to tmg.mydom.local

- Nazwa komputera z Serwerem administracyjnym to ksc.mydom.local
- Nazwa zewnętrznej publikacji punktu dostępu do protokołu mobilnego to kes4mob.mydom.global.

Konto domeny dla Serwera administracyjnego

Należy utworzyć konto domeny (na przykład: KSCMobileSrvcUsr), z poziomu którego będzie uruchamiana usługa Serwera administracyjnego. Konto dla usługi Serwera administracyjnego można określić podczas instalacji Serwera administracyjnego lub poprzez narzędzie klsrvswch. Narzędzie klsrvswch znajduje się w folderze instalacyjnym Serwera administracyjnego.

Konto domeny musi zostać określone z następujących względów:

- Funkcja zarządzania urządzeniami KES jest integralną częścią Serwera administracyjnego
- Aby zapewnić poprawne działanie delegowania protokołu Kerberos (KCD), strona odbierająca (czyli Serwer administracyjny) musi być uruchomiona z poziomu konta domeny.

Nazwa główna usługi dla http/kes4mob.mydom.local

W domenie, z poziomu konta KSCMobileSrvcUsr, dodaj SPN dla publikacji usługi protokołu mobilnego na porcie 13292 komputera z Serwerem administracyjnym. Dla komputera kes4mob.mydom.local z Serwerem administracyjnym będzie to wyglądało w następujący sposób:

setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr

Konfigurowanie właściwości domeny komputera z TMG (tmg.mydom.local)

Aby przeprowadzić ruch sieciowy, przełącz komputer z TMG (tmg.mydom.local) do usługi, która jest definiowana po SPN (http/kes4mob.mydom.local:13292).

W celu przełączenia komputera z TMG do usługi definiowanej po SPN (http/kes4mob.mydom.local:13292), administrator musi wykonać następujące działania:

1. W przystawce programu MMC o nazwie "Użytkownicy i komputery usługi Active Directory" wybierz komputer z zainstalowanym TMG (tmg.mydom.local).

2. We właściwościach komputera, na zakładce **Delegowanie** ustaw przełącznik **Ufaj temu komputerowi w delegowaniu tylko do określonych usług** na **Użyj dowolnego protokołu uwierzytelniania**.

3. Na liście **Usługi, którym to konto może przedstawiać delegowane poświadczenia** dodaj SPN http/kes4mob.mydom.local:13292.

Specjalny (niestandardowy) certyfikat dla publikacji (kes4mob.mydom.global)

Aby opublikować protokół mobilny Serwera administracyjnego, należy wystawić specjalny (niestandardowy) certyfikat dla FQDN kes4mob.mydom.global, a także określić go w miejsce domyślnego certyfikatu serwera w ustawieniach protokołu mobilnego Serwera administracyjnego, w Konsoli administracyjnej. W tym celu, w oknie właściwości Serwera administracyjnego, w sekcji **Ustawienia** zaznacz pole **Otwórz port dla urządzeń mobilnych**, a następnie z listy rozwijalnej wybierz **Dodaj certyfikat...**.

Należy pamiętać, że kontener certyfikatów serwera (plik z rozszerzeniem .p12 lub .pfx) musi także zawierać łańcuch certyfikatów głównych (klucze publiczne).

Konfigurowanie publikacji na TMG

Na TMG, dla ruchu przechodzącego z urządzenia mobilnego do portu 13292 usługi kes4mob.mydom.global należy skonfigurować KCD na SPN (http/kes4mob.mydom.local:13292), korzystając z certyfikatu serwera opublikowanego dla FQDN kes4mob.mydom.global. Nie można zapominać, że publikacja oraz opublikowany punkt dostępu (port 13292 Serwera administracyjnego) powinny korzystać z tego samego certyfikatu serwera.

Korzystanie z Google Cloud Messaging

Aby zapewnić reakcję urządzeń KES z systemem Android w odpowiednim momencie na polecenia administratora, musisz włączyć korzystanie z usługi Google™ Cloud Messaging (zwana również GCM) we właściwościach Serwera administracyjnego.

► *W celu włączenia korzystania z GCM:*

1. W Konsoli administracyjnej wybierz węzeł **Zarządzanie urządzeniami mobilnymi**, a następnie folder **Urządzenia mobilne**.

2. Z menu kontekstowego folderu **Urządzenia mobilne** wybierz **Właściwości**.

3. We właściwościach folderu wybierz sekcję **Ustawienia usługi Google Cloud Messaging**.
4. W polach **ID nadawcy** i **Klucz API** określ ustawienia GCM: ID_NADAWCY i Klucz API.

Usługa DCM działa w następujących zakresach adresów:

- Ze strony urządzenia KES dostęp jest wymagany do portów 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) oraz 5230 (HTTPS) dla następujących adresów:
  - google.com
  - android.googleapis.com
  - android.apis.google.com
  - Wszystkie adresy IP w ASN Google'a dla portu15169.
- Ze strony Serwera administracyjnego dostęp jest wymagany do portu 443 (HTTPS) dla następujących adresów:
  - android.googleapis.com
  - Wszystkie adresy IP w ASN Google'a dla portu15169.

Jeśli ustawienia serwera proxy (**Zaawansowane / Ustawienia połączenia internetowego**) zostały zdefiniowane we właściwościach Serwera administracyjnego w Konsoli administracyjnej, będą używane do interakcji z GCM.

Konfigurowanie GCM: uzyskiwanie ID_NADAWCY, Klucza API

W celu skonfigurowania GDM, administrator musi wykonać następujące akcje:

1. Zarejestrować się na portalu Google https://accounts.google.com.
2. Przejść na portal deweloperów https://console.developers.google.com/project.
3. Utworzyć nowy projekt, klikając przycisk **Create Project**, określić nazwę projektu oraz ID.
4. Zaczekać, aż projekt zostanie utworzony.

   Na pierwszej stronie projektu, w górnej części strony pole **Project Number** wyświetli odpowiedni ID_NADAWCY.

5. Przejść do sekcji **APIs & auth / APIs** i włączyć **Google Cloud Messaging for Android**.
6. Przejść do sekcji **APIs & auth / Credentials** i kliknąć przycisk **Create New Key**.
7. Kliknąć przycisk **Server key**.
8. Nałożyć ograniczenia (jeśli są) i kliknąć przycisk **Create**.
9. Uzyskać klucz API z właściwości nowo utworzonego klucza (pole **API key**).

Integracja z infrastrukturą kluczy publicznych

Integracja z infrastrukturą kluczy publicznych (zwana również PKI) jest przeznaczona głównie do uproszenia wystawiania certyfikatów użytkownika domeny przez Serwer administracyjny.

Administrator może przypisać certyfikat domeny dla użytkownika w Konsoli administracyjnej. Można to zrobić przy użyciu jednej z następujących metod:

- Przydziel użytkownikowi specjalny (niestandardowy) certyfikat z pliku w Kreatorze tworzenia nowego połączenia z urządzeniem lub w Kreatorze instalacji certyfikatu.
- Przeprowadź integrację z PKI i wskaż PKI jako źródło certyfikatów dla określonego typu certyfikatów lub dla wszystkich typów certyfikatów.

Ustawienia integracji z PKI są dostępne w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi / Certyfikaty** po kliknięciu odnośnika **Integruj z infrastrukturą kluczy publicznych**.

Ogólne zasady integracji z PKI dla publikacji certyfikatów użytkownika domeny

W Konsoli administracyjnej, w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi / Certyfikaty** kliknij odnośnik **Integruj z infrastrukturą kluczy publicznych**, aby określić konto domeny, które będzie używane przez Serwer administracyjny do wystawiania certyfikatów użytkownika domeny poprzez urząd certyfikacji domeny (zwany również kontem, z poziomu którego wykonywana jest integracja z PKI).

Należy pamiętać, że:

- Ustawienia integracji z PKI oferują możliwość określenia domyślnego szablonu dla wszystkich typów certyfikatów. Nie wolno też zapominać, że reguły wystawiania certyfikatów (dostępne w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi / Certyfikaty** po kliknięciu odnośnika **Reguły generowania certyfikatów**) pozwalają na określenie indywidualnego szablonu dla każdego typu certyfikatu.

- Specjalny certyfikat Agenta rejestracji (EA) powinien zostać zainstalowany na komputerze z Serwerem administracyjnym, w repozytorium certyfikatów konta, z poziomu którego wykonywana jest integracja z PKI. Certyfikat Agenta rejestracji (EA) jest wystawiany przez administratora urzędu certyfikacji domeny (CA).

Konto, z poziomu którego wykonywana jest integracja z PKI, musi spełniać następujące kryteria.

- Jest to użytkownik domeny.

- Jest to lokalny administrator komputera z Serwerem administracyjnym, z poziomu którego została zainicjowana integracja z PKI.

- Posiada uprawnienie do **Zalogowania w trybie usługi**.

- Komputer z Serwerem administracyjnym musiał być wcześniej zalogowany przynajmniej raz z poziomu tego konta w celu utworzenia trwałego profilu użytkownika.

Operator Kaspersky Security Center

Serwer sieciowy Kaspersky Security Center (zwany również serwerem sieciowym) jest składnikiem Kaspersky Security Center. Serwer sieciowy został zaprojektowany do publikowania autonomicznych pakietów instalacyjnych, autonomicznych pakietów instalacyjnych dla urządzeń mobilnych, profili iOS MDM oraz plików z folderu współdzielonego.

Profile iOS MDM oraz utworzone pakiety instalacyjne są automatycznie publikowane na serwerze sieciowym, a następnie są usuwane po pierwszym pobraniu. Administrator może wysłać użytkownikowi nowy odnośnik w dowolny sposób, na przykład za pośrednictwem poczty elektronicznej.

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

Ustawienia serwera sieciowego

Jeśli wymagane jest dostrojenie serwera sieciowego, właściwości serwera sieciowego w Konsoli administracyjnej oferują możliwość zmiany portów dla HTTP (8060) i HTTPS (8061). Oprócz zmiany portów, możesz zastąpić certyfikat serwera dla HTTPS i zmienić FQDN serwera sieciowego dla HTTP.

Konfigurowanie i korzystanie z NAC

Ta sekcja zawiera zalecenia dotyczące wstępnej konfiguracji i korzystania z NAC. Poniżej znajdują się zalecenia dotyczące komputerów przeznaczonych do używania jako Agenty NAC, a także priorytety ograniczeń nałożonych na urządzenia sieciowe, określone w regułach NAC.

Dostępne są również przykłady ustawień NAC dla niektórych standardów konfiguracji.

W tej sekcji:

Zobacz również:

Przydzielanie Agentów NAC

Podczas przydzielania Agenta NAC musisz wybrać komputer, który spełnia następujące kryteria:

- Posiada wolne zasoby, a zużycie procesora i obciążenie usługi sieciowej jest niskie.
- Jest najmocniejszy wśród dostępnych komputerów.

- Jest rzadko uruchamiany ponownie / wyłączany.

Wskazanie komputera spełniającego powyższe wymagania jako Agenta NAC spowoduje przyspieszenie gromadzenia i skanowania danych, a także zwiększenie wydajności zastosowanych profili NAC. Jeśli Agent NAC będzie działał w domenie rozgłoszeniowej, która już zawiera urządzenia sieciowe (których aktywność musi być ograniczona), może upłynąć czas zanim sieć zostanie przeanalizowana, a profil NAC zostanie zastosowany. Zazwyczaj profil zaczyna obowiązywać w przeciągu 10-15 minut od jego zastosowania.

Liczba urządzeń obsługiwanych przez pojedynczego Agenta NAC zależy od infrastruktury oraz skali domeny rozgłoszeniowej sieci, a także od liczby reguł i obiektów sieci. NAC działa solidnie, gdy na jednego Agenta NAC przypada 1 000 urządzeń.

Aby sprawdzić wydajność profilu NAC, Agent NAC oferuje tryb symulacji. Tryb symulacji obejmuje transmisję profilu NAC na sterowniku, ale rzeczywista aktywność sieciowa urządzeń objętych ograniczeniami dostępu nie jest wcale ograniczona. Podczas działania trybu symulacji Agent sieciowy tylko pobiera ze sterownika NAC informację o konieczności zastosowania reguły dla urządzenia. Ta informacja jest dostępna w pliku $klnac.log (sekcja "Określanie stosowania reguły NAC" na stronie 135). Pod innymi względami tryb ten przypomina tryb normalny (standardowy).

Podczas działania Agent NAC tworzy dodatkowe karty wirtualne (po jednej dla każdej karty fizycznej w systemie), a ich adresy MAC są losowo generowane przez Serwer administracyjny. Ta lista adresów MAC jest generowana tylko raz, przy pierwszym uruchomieniu Serwera administracyjnego, i nie może być później zmodyfikowana. Na etapie inicjowania karta Agenta MAC podejmuje kilka prób konfiguracji DHCP przy użyciu jednego z dostępnych adresów MAC na liście. Jeśli infrastruktura sieci nie zawiera serwera DHCP lub jeśli konfiguracja serwera DHCP używa zastrzeżenia statycznego MAC–IPv4, Agent NAC wymaga ręcznej konfiguracji interfejsu.

Ręczna konfiguracja Agenta NAC (niezalecane)

Możesz ręcznie skonfigurować Agenta NAC poprzez rejestr systemu Windows, importując następujący plik:

W 32-bitowych wersjach systemu Windows:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
]
```

"EnfUseDHCP"=dword:00000000

"EnfIpv4"="10.16.72.2"

"EnfSubnetMask"="255.255.252.0"

"EnfIpv4Gateway"="10.16.72.1"

W 64-bitowych wersjach systemu Windows:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags]

"EnfUseDHCP"=dword:00000000

"EnfIpv4"="10.16.72.2"

"EnfSubnetMask"="255.255.252.0"

"EnfIpv4Gateway"="10.16.72.1"

Ręczna konfiguracja jest dostępna tylko dla Agentów NAC z jednym aktywnym interfejsem fizycznym. Jeśli używanych jest kilka aktywnych interfejsów fizycznych, nowo ustawiona konfiguracja zostanie zastosowana na karcie wirtualnej pierwszego losowo wybranego interfejsu.

Ograniczenia w regułach NAC

Ograniczenia w regułach NAC posiadają następujące priorytety (w kolejności malejącej):

- Agenty NAC (priorytet najwyższego poziomu, do wewnętrznego użycia).

  Komputery z Agentami NAC są zawsze dostępne do interakcji sieci z urządzeniami, niezależnie od ograniczeń nałożonych na aktywność tych urządzeń.

- Biała lista. Agenty NAC nie nakładają żadnych ograniczeń na urządzenia z listy.

- Zablokowane ręcznie w Konsoli administracyjnej.

- Zalogowany do Portalu autoryzacji. Agenty NAC nie nakładają żadnych ograniczeń na urządzenia z listy.
- Zablokowane. Dostęp do tych urządzeń sieciowych będzie zablokowany.
- Zablokowane, za wyjątkiem listy adresów specjalnych (typ ograniczenia "Zezwól na dostęp do adresów usługi").

  Urządzenia znajdujące się na tej liście będą miały dostęp tylko do listy adresów specjalnych reguły. Dostęp do innych adresów będzie zablokowany.
- Urządzenia z nałożonym ograniczeniem "Przekieruj na portal autoryzacji" (priorytet najniższego poziomu).

  Natychmiast po autoryzacji urządzenie zostanie dodane do listy "Zalogowany do Portalu autoryzacji" i nie będzie już ograniczone przez Agenta NAC. Przed zalogowaniem do Portalu autoryzacji, urządzenia z tym ograniczeniem zawsze mają dostęp do listy serwerów DNS w sieci.

Podczas określania obiektów sieci zwróć uwagę, czy urządzenie odpowiada typowi obiektu sieciowego. Na przykład, jeśli obiekt sieciowy należy do typu "Komputery", kryteria tego obiektu zostaną spełnione tylko przez urządzenia z typem "Komputery" wykrytym po aktywnym skanowaniu.

Włączanie NAC

W celu włączenia NAC:

1. W Konsoli administracyjnej utwórz profil Agenta sieciowego, a we właściwościach profilu (sekcja **Ustawienia**, **Tryb działania NAC**) włącz NAC w trybie **standardowym**.
2. Przypisz Agenty NAC w domenach rozgłoszeniowych zawierających urządzenia, dla których chcesz ograniczyć aktywność sieciową.
3. We właściwościach Agenta sieciowego dla odpowiednich Agentów NAC wybierz tryb **Standardowy** dla Agenta NAC.

Standardowe konfiguracje NAC

Poniżej znajdują się przykłady konfiguracji NAC w niektórych standardowych konfiguracjach sieci.

Konfiguracja "Tylko urządzenia firmowe"

Kilka urządzeń sieciowych (komputery, laptopy, drukarki sieciowe) łączy się z domeną rozgłoszeniową w sieci Ethernet. Administrator jest świadom ich pochodzenia, dlatego w Konsoli administracyjnej, w węźle **Repozytoria/Sprzęt** przypisuje do nich atrybut "Firmowe". Administrator chce całkowicie ograniczyć dostęp do zasobów sieciowych na wszystkich urządzeniach, które nie zostały oznaczone jako "Firmowe" (komputery, serwery plików, drukarki itd.).

W tym celu administrator powinien wykonać następujące działania:

1. Włączyć NAC (sekcja "Włączanie NAC" na stronie 121).
2. We właściwościach profilu musi utworzyć obiekt sieciowy o nazwie "Urządzenia niefirmowe" (dla obiektu można wprowadzić dowolną nazwę) należący do typu "Urządzenia dowolnego typu". Dodać kryterium "Urządzenia nie oznaczone jako firmowe" do listy kryteriów.
3. Utworzyć regułę ograniczającą dostęp, której przeznaczeniem będzie "Zablokuj dostęp do sieci". Dodać obiekt "Urządzenia niefirmowe" do listy obiektów sieciowych reguły.

Konfiguracja "Dostęp tylko do drukarki sieciowej"

Kilka urządzeń sieciowych (komputery, laptopy, drukarki sieciowe) łączy się z domeną rozgłoszeniową w sieci Ethernet. Administrator nie jest świadomy ich pochodzenia, ale musi udzielić dostępu do drukarki sieciowej o adresie IP 192.168.1.135 wszystkim urządzeniom, które zostały oznaczone jako "Komputer" w obrębie tego segmentu.

W tym celu administrator powinien wykonać następujące działania:

1. Włączyć NAC (sekcja "Włączanie NAC" na stronie 121).
2. We właściwościach profilu musi utworzyć obiekt z typem "Adresy sieciowe" o nazwie "Drukarka 192.168.1.135", która opisuje adres IP 192.168.1.135.

3. Utworzyć obiekt sieciowy o nazwie "Wszystkie komputery w tym segmencie". Dodać kryterium "Według atrybutów sieci" do listy kryteriów, który opisuje zakres adresów IP w tym segmencie (na przykład: 192.168.1.2 – 192.168.1.254).

4. Utworzyć regułę ograniczającą dostęp, której przeznaczeniem będzie "Zezwól na dostęp do adresów sieciowych". Dodać obiekt "Wszystkie komputery w tym segmencie" do listy obiektów sieciowych reguły, a następnie dodać obiekt "Drukarka 192.168.1.135" do listy dozwolonych adresów sieciowych.

Konfiguracja "Dostęp poprzez Portal autoryzacji"

Kilka urządzeń sieciowych łączy się z domeną rozgłoszeniową w sieci Ethernet. Administrator nie jest świadomy ich pochodzenia, ale musi zezwolić na dostęp do zasobów sieciowych komputerom, na których użytkownicy zalogowali się do Portalu autoryzacji.

W tym celu administrator powinien wykonać następujące działania:

1. Włączyć NAC (sekcja "Włączanie NAC" na stronie 121).

2. We właściwościach profilu musi utworzyć konto dla Portalu autoryzacji o nazwie "Gość".

3. Utworzyć obiekt sieciowy o nazwie "Wszystkie komputery w tym segmencie". Dodać kryterium "Według atrybutów sieci" do listy kryteriów, który opisuje zakres adresów IP w tym segmencie (na przykład: 192.168.1.2 – 192.168.1.254).

4. Utworzyć regułę ograniczającą dostęp, której przeznaczeniem będzie "Przekieruj na portal autoryzacji". Dodać obiekt "Wszystkie komputery w tym segmencie" do listy obiektów sieciowych reguły.

Usługa Kaspersky Captive Portal service zostanie automatycznie uruchomiona na Agencie NAC. Ruch sieciowy urządzeń (zdefiniowanych jako "Komputery") zostanie przekierowany na Portal autoryzacji, który spowoduje otwarcie strony autoryzacyjnej w przeglądarce użytkownika. Jeśli użytkownik wprowadzi dane uwierzytelniające konta Gość, komputer zostanie oznaczony jako uwierzytelniony, a użytkownikowi zostanie udzielony pełny dostęp do zasobów sieciowych.

W przeglądarkach użytkowników Portalu autoryzacji musi być włączona obsługa JavaScript.

Podstawowe zadania

W tej sekcji:

Kolory ikony wskaźnika w Konsoli administracyjnej

Główny wskaźnik stanu Kaspersky Security Center i zarządzanych komputerów to zestaw wskaźników odpowiadających sygnalizacji świetlnej w obszarze roboczym węzła **Serwer administracyjny** w Konsoli administracyjnej (**Rozpoczęcie pracy**). Wyświetlanych jest sześć zestawów. Każdy zestaw reprezentuje inny zakres funkcji Kaspersky Security Center.

Tabela 7. Kolory ikony wskaźnika w Konsoli administracyjnej

Nazwa zestawu	Zakres funkcji
Zdalna instalacja	Instalacja Agenta sieciowego i aplikacji antywirusowej na komputerach w sieci firmowej.
Zarządzanie komputerami	Struktura grup administracyjnych. Skanowanie sieci. Reguły przenoszenia komputerów
Ochrona komputerów i skanowanie	Funkcjonalność aplikacji antywirusowej: stan ochrony, skanowanie antywirusowe

antywirusowe	
Aktualizacja	Uaktualnienia i łaty
Monitorowanie	Stan ochrony
Serwer administracyjny	Funkcje i właściwości Serwera administracyjnego

Każdy zestaw posiada trzy możliwe kolory:

Tabela 8. Kolory zestawów

Stan	Kolor	Znaczenie koloru
Informacja	Zielony	Nie jest wymagana interwencja administratora
Ostrzeżenie	Żółty	Wymagana jest interwencja administratora
Krytyczny	Czerwony	Wystąpiły poważne problemy. W celu rozwiązania tych problemów wymagana jest interwencja administratora

Wszystkie zestawy wskaźników muszą być zielone.

Zdalny dostęp do zarządzanych komputerów

W tej sekcji:

Dostęp do statystyk i zadań lokalnych, pole "Nie odłączaj od Serwera administracyjnego"

Domyślnie Kaspersky Security Center nie oferuje stałego połączenia pomiędzy zarządzanymi komputerami a Serwerem administracyjnym. Agenty sieciowe na zarządzanych komputerach okresowo nawiązują połączenie i synchronizują się z Serwerem administracyjnym. Przerwa między tymi synchronizacjami (domyślnie jest to 15 minut) jest definiowana w profilu Agenta sieciowego. Jeśli wymagana jest wcześniejsza synchronizacja (na przykład, aby wymusić zastosowanie profilu), Serwer administracyjny wysyła podpisany pakiet sieciowy do Agenta sieciowego na port UDP o numerze 15000. Jeśli z jakiegoś powodu nie jest możliwe nawiązanie połączenia między Serwerem administracyjnym a zarządzanym komputerem przy użyciu UDP, synchronizacja zostanie uruchomiona przy następnym regularnym połączeniu Agenta sieciowego z Serwerem administracyjnym w trakcie interwału synchronizacji.

Niektóre działania nie mogą zostać wykonane bez wcześniejszego nawiązania połączenia między Agentem sieciowym a Serwerem administracyjnym. Do tych działań należą: uruchamianie i zatrzymywanie zadań lokalnych, pobieranie statystyk dla zarządzanego produktu (aplikacji antywirusowej lub Agenta sieciowego), tworzenie połączeń itd. Aby rozwiązać ten problem, we właściwościach zarządzanego komputera (sekcja **Ogólne**) zaznacz pole **Nie odłączaj od Serwera**

administracyjnego. Maksymalna dozwolona liczba komputerów z zaznaczonym polem **Nie odłączaj od Serwera administracyjnego** to 300.

Sprawdzanie czasu połączenia pomiędzy komputerem a Serwerem administracyjnym

Po wyłączeniu komputera, Agent sieciowy powiadamia Serwer administracyjny o tym zdarzeniu. W Konsoli administracyjnej ten komputer jest wyświetlany jako wyłączony. Jednakże Agent sieciowy nie może powiadamiać Serwera administracyjnego o wszystkich tego typu zdarzeniach. Dlatego też Serwer administracyjny okresowo analizuje atrybut **Czas ostatniego połączenia** (wartość tego atrybutu jest wyświetlana w Konsoli administracyjnej, we właściwościach komputera, w sekcji **Ogólne**) dla każdego komputera i porównuje go z interwałem synchronizacji z aktualnych ustawień Agenta sieciowego. Jeśli komputer nie odpowiedział w ponad trzech pomyślnych interwałach synchronizacji, ten komputer zostanie oznaczony jako wyłączony.

Wymuszona synchronizacja

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

W menu kontekstowym zarządzanych komputerów w Konsoli administracyjnej komputera element menu **Wszystkie zadania** zawiera polecenie **Wymuś synchronizację**. Jeśli Kaspersky Security Center 10 Service Pack 2 wykona to polecenie, a pole **Przypisz wymuszoną synchronizację** będzie zaznaczone we właściwościach komputera, to Serwer administracyjny spróbuje nawiązać połączenie z komputerem. Jeśli ta próba się powiedzie, wymuszona synchronizacja zostanie wykonana, a pole zostanie odznaczone. W innym przypadku synchronizacja zostanie wymuszona, a pole zostanie odznaczone dopiero po kolejnym zaplanowanym połączeniu nawiązanym pomiędzy Agentem sieciowym a Serwerem administracyjnym. Odznaczone pole będzie znakiem dla administratora, że synchronizacja się powiodła.

Tunelowanie połączeń

Kaspersky Security Center umożliwia tunelowanie połączeń TCP z Konsoli administracyjnej poprzez Serwer administracyjny, a następnie poprzez Agenta sieciowego do określonego portu na zarządzanym komputerze. Tunelowanie połączeń jest przeznaczone dla połączenia aplikacji klienckiej na komputerze z zainstalowaną Konsolą administracyjną z portem TCP na zarządzanym komputerze—jeśli nie jest możliwe bezpośrednie połączenie między Konsolą administracyjną a komputerem docelowym.

Na przykład, tunelowanie jest wykorzystywane dla połączeń ze zdalnym pulpitem - zarówno do łączenia się z istniejącą sesją, jak i do tworzenia nowej zdalnej sesji.

Tunelowanie połączeń może zostać włączone także przy użyciu narzędzi zewnętrznych. Na przykład, administrator może uruchomić w ten sposób narzędzie putty, klienta VNC oraz inne narzędzia.

Zarządzanie urządzeniami mobilnymi

W tej sekcji:

Serwer urządzeń mobilnych Exchange ActiveSync

Po pomyślnej instalacji, serwer urządzeń mobilnych Exchange ActiveSync będzie wyświetlany w Konsoli administracyjnej Kaspersky Security Center, w folderze **Zarządzanie urządzeniami mobilnymi**.

Zarządzanie profilami Exchange ActiveSync

Po zainstalowaniu serwera urządzeń mobilnych Exchange ActiveSync, w sekcji **Skrzynki pocztowe** okna właściwości Serwera możesz wyświetlić informacje dotyczące kont serwera Microsoft Exchange Server, które zostały pobrane poprzez przeszukiwanie aktualnej domeny lub lasu domeny.

Dodatkowo, w oknie właściwości serwera urządzeń mobilnych Exchange ActiveSync możesz użyć następujących przycisków:

- **Zmień profile** umożliwia otwarcie okna **Profile zasad**, które zawiera listę profili pobranych z serwera Microsoft Exchange Server. W tym oknie możesz utworzyć, zmodyfikować lub usunąć profile Exchange ActiveSync. Okno **Profile zasad** jest prawie takie samo jak okno do modyfikowania profilu w Konsoli zarządzania programu Exchange.
- **Przypisz profile do urządzeń mobilnych**— umożliwia przypisanie wybranego profilu Exchange ActiveSync do jednego lub kilku kont.
- **Włącz/wyłącz ActiveSync**— umożliwia włączenie lub wyłączenie protokołu HTTP Exchange ActiveSync dla jednego lub kilku kont.

Konfigurowanie obszaru skanowania

We właściwościach zainstalowanego serwera urządzeń mobilnych Exchange ActiveSync, w sekcji **Ustawienia** możesz skonfigurować obszar skanowania. Domyślnie obszar skanowania to bieżąca domena, w której zainstalowany jest serwer urządzeń mobilnych Exchange ActiveSync. Wybranie wartości **Cały las domen** rozszerzy obszar skanowania o cały las domen.

Praca z urządzeniami EAS

Urządzenia wykryte poprzez skanowanie serwera Microsoft Exchange Server zostaną dodane do standardowej listy urządzeń, która znajduje się w węźle **Zarządzanie urządzeniami mobilnymi**, w folderze **Urządzenia mobilne**.

Jeśli chcesz, żeby w folderze **Urządzenia mobilne** były wyświetlane tylko urządzenia Exchange ActiveSync (zwane również urządzeniami EAS), filtruj listę urządzeń, klikając odnośnik **Exchange ActiveSync (EAS)**, który znajduje się nad tą listą.

Urządzeniami EAS można zarządzać przy użyciu poleceń. Na przykład, polecenie **Usuń dane** umożliwia usunięcie wszystkich danych z urządzenia i przywrócenie ustawień fabrycznych urządzenia. Polecenie jest przydatne, gdy urządzenie zostanie zgubione lub skradzione i będziesz chciał zapobiec uzyskaniu danych firmowych i osobowych przez pracowników firm trzecich.

> Jeśli wszystkie dane zostały usunięte z urządzenia, zostaną ponownie usunięte przy kolejnym połączeniu urządzenia z serwerem Microsoft Exchange Server. Wykonanie polecenia będzie powtarzane, aż do usunięcia urządzenia z listy urządzeń. To zachowanie jest spowodowane przez zasady działania serwera Microsoft Exchange Server.

Aby usunąć urządzenie EAS z listy, w menu kontekstowym urządzenia wybierz **Usuń**. Jeśli konto Exchange ActiveSync nie zostało usunięte z urządzenia EAS, urządzenie to pojawi się ponownie na liście urządzeń po kolejnej synchronizacji urządzenia z serwerem Microsoft Exchange Server.

Serwer urządzeń mobilnych iOS MDM

Ta sekcja opisuje główne funkcje dla urządzeń zarządzanych przez serwer urządzeń mobilnych iOS MDM (zwane również urządzeniami iOS MDM).

W tej sekcji:

Dodanie nowego urządzenia poprzez opublikowanie odnośnika do profilu

W Konsoli administracyjnej administrator tworzy nowy profil iOS MDM, korzystając z Kreatora tworzenia nowego połączenia z urządzeniem. Kreator wykonuje następujące działania:

- Profil iOS MDM jest automatycznie publikowany na serwerze sieciowym.
- Do użytkownika zostaje wysłany odnośnik do profilu iOS MDM w wiadomości SMS lub e-mail. Po odebraniu wiadomości z odsyłaczem, użytkownik instaluje profil iOS MDM na urządzeniu.
- Urządzenie łączy się z serwerem urządzeń mobilnych iOS MDM.

Zobacz również:

Operator Kaspersky Security Center 117

Dodanie nowego urządzenia poprzez zainstalowanie profilu przez administratora

W celu połączenia urządzenia z serwerem urządzeń mobilnych iOS MDM poprzez zainstalowanie profilu iOS MDM na tym urządzeniu, administrator musi wykonać następujące czynności:

1. W Konsoli administracyjnej powinien otworzyć Kreator tworzenia nowego połączenia z urządzeniem.
2. Utworzyć nowy profil iOS MDM, zaznaczając pole **Pokaż certyfikat po zakończeniu wprowadzania** w oknie Kreatora.
3. Zapisać profil iOS MDM.
4. Zainstalować profil iOS MDM na urządzeniu użytkownika przy pomocy narzędzia Apple Configurator.

Urządzenie połączy się z serwerem urządzeń mobilnych iOS MDM.

Zobacz również:

Operator Kaspersky Security Center 117

Wysyłanie poleceń na urządzenie

► *W celu wysłania polecenia na urządzenie iOS MDM, administrator musi wykonać następujące czynności:*

1. W Konsoli administracyjnej powinien otworzyć węzeł **Zarządzanie urządzeniami mobilnymi**.
2. Wybrać folder **Urządzenia mobilne**.
3. W folderze **Urządzenia mobilne** wybrać urządzenie, na które zostaną wysłane polecenia.
4. W menu kontekstowym urządzenia wybrać **Polecenia dla urządzeń iOS** lub **Zarządzaj urządzeniem**. Z wyświetlonej listy wybierz polecenie, które ma zostać wysłane na urządzenie.

Sprawdzanie stanu wykonania wysłanych poleceń

► *W celu sprawdzenia stanu polecenia, które zostało wysłane na urządzenie, administrator musi wykonać następujące działania:*

1. W Konsoli administracyjnej powinien otworzyć węzeł **Zarządzanie urządzeniami mobilnymi**.
2. Wybrać folder **Urządzenia mobilne**.
3. W folderze **Urządzenia mobilne** wybrać urządzenie, na którym ma być sprawdzony stan wykonania wybranych poleceń.
4. Z menu kontekstowego urządzenia powinien wybrać **Pokaż raport poleceń**.

NAC: Zdarzenia i standardowe scenariusze

Ta sekcja zawiera opisy zdarzeń NAC, które są publikowane przez Agenty NAC, a także zalecenia dotyczące korzystania z NAC w standardowych scenariuszach dla tej funkcji.

Zdarzenia NAC

Istnieją dwa rodzaje zdarzeń publikowanych przez Agenty NAC:

- Wykryto urządzenie. To zdarzenie jest publikowane przy pierwszym wykryciu urządzenia przez Agenta NAC. Treść zdarzenia zawiera adres MAC oraz adres IP urządzenia (w momencie wykrycia).
- Urządzenie uwierzytelnione. To zdarzenie jest publikowane przy każdym pomyślnym zalogowaniu urządzenia do Portalu autoryzacji. Treść zdarzenia zawiera adres MAC oraz adres IP urządzenia (w momencie wykrycia).

Standardowe scenariusze dla NAC

W tej sekcji są opisane standardowe scenariusze wykorzystania NAC do monitorowania aktywności urządzeń sieciowych.

W tej sekcji:

Kontrola aktywności urządzeń sieciowych

Kontrola aktywności urządzeń sieciowych może odbywać się w trybie online, w Konsoli administracyjnej, w folderze **Urządzenia nieprzypisane/Urządzenia sieciowe**. Obszar roboczy tego folderu wyświetla listę urządzeń, które kiedykolwiek zostały wykryte w sieci. Możesz wykorzystać menu kontekstowe do ręcznego zablokowania lub odblokowania urządzenia

Kontrola aktywności urządzeń sieciowych może odbywać się także w trybie offline, w Konsoli administracyjnej, w folderze **Raporty i powiadomienia/Zdarzenia**.

Ograniczanie aktywności sieciowej urządzenia

Istnieją dwa sposoby ograniczenia aktywności sieciowej urządzenia:

- W Konsoli administracyjnej, w obszarze roboczym folderu **Urządzenia nieprzypisane** odszukaj urządzenie, a następnie z menu kontekstowego urządzenia wybierz **Zablokuj**.
- W profilu Agenta sieciowego utwórz obiekt sieciowy o typie **Urządzenia dowolnego typu** i dodaj dostępny zestaw kryteriów do listy kryteriów. Jeśli znany jest adres MAC urządzenia, będzie to kryterium **Według atrybutów sieci** z wartością atrybutu, która odpowiada adresowi MAC urządzenia.

Znoszenie ograniczeń nałożonych na aktywność sieciową urządzenia

Istnieją również dwa sposoby odblokowania urządzenia:

- Jeśli urządzenie zostało zablokowane przez administratora ręcznie, możesz je odblokować, odznaczając pole w elemencie **Zablokuj** menu kontekstowego, w folderze **Urządzenia nieprzypisane** Konsoli administracyjnej.
- Jeśli aktywność sieciowa urządzenia została ograniczona przez pewne reguły NAC, te ograniczenia można znieść, dodając odpowiedni obiekt sieciowy do białej listy urządzeń w ustawieniach Agenta sieciowego (sekcja **Network Access Control (NAC)**) lub modyfikując obiekt sieciowy w taki sposób, że urządzenie nie spełnia już jego kryteriów.

Określanie stosowania reguły NAC

Po zakończeniu konfiguracji, profil z regułami NAC (zwany również profilem NAC) zostanie dostarczony Agentom NAC. Stosowanie profilu na urządzeniu rozpoczyna się natychmiast po wykryciu dowolnej wychodzącej aktywności sieciowej tego urządzenia.

Aby określić, czy reguła NAC (i która reguła) jest stosowana do urządzenia w sieci, musisz znać domenę rozgłoszeniową, w obrębie której działa urządzenie, a także musisz mieć zdalny dostęp do Agenta NAC, który stosuje profil NAC w tej domenie.

Na przykład, w domenie rozgłoszeniowej *X* urządzenie *Y* działa z adresem MAC *Z*. W profilu Agenta sieciowego opisane jest to urządzenie (przy pomocy obiektu sieciowego), a reguła *R* została utworzona w celu ograniczenia dostępu urządzenia do sieci. W domenie rozgłoszeniowej *X* działa Agent NAC *E*. Kontrola aktywności Agenta NAC może zostać przeprowadzona przy pomocy pliku $klnac.log. Procedura kontroli Agenta NAC E została przedstawiona poniżej.

Kontrola aktywności Agenta NAC

W celu przeprowadzenia kontroli aktywności Agenta NAC E, administrator musi wykonać następujące czynności:

1. Uzyskać zdalny dostęp do systemu plików Agenta NAC E.
2. W folderze %WINDIR%\Temp musi odszukać plik $klnac.log, a następnie otworzyć go przy użyciu dowolnego edytora tekstu, który obsługuje UNIX®, na przykład Wordpad.
3. W pliku tekstowym powinien odszukać wiersze skojarzone z aktywnością Rule, gdzie po wierszu RuleName występuje nazwa reguły, która zostanie zastosowana (*R*). Po znaku minus (-) znajdują się następujące atrybuty sieciowe, których aktywność jest ograniczona: MAC SRC i IPv4 SRC. Jeśli zostanie wykryty adres MAC *Z*, oznacza to, że reguła *R* została zastosowana i jest wykonywana.

   Dodatkowo, w pliku $klnac.log można sprawdzić, kiedy urządzenie zostało wykryte po raz pierwszy i do którego zasobu sieciowego próbowało uzyskać dostęp w tym czasie (w wierszach skojarzonych z Device discovery).

Dodatki

Ta sekcja zawiera dodatkowe informacje i fakty związane z korzystaniem z Kaspersky Security Center:

- Informacje dotyczące ograniczeń nałożonych przez aktualną wersję aplikacji (maksymalna liczba zarządzanych komputerów, profile, zadania itd.)
- Wymagania sprzętowe dla instalacji Serwera administracyjnego i DBMS
- Dodatkowe informacje na temat miejsca na dysku niezbędnego do działania komponentów aplikacji
- Dodatkowe informacje na temat przeciętnego dziennego ruchu sieciowego pomiędzy Agentem sieciowym a Serwerem administracyjnym
- Informacje dotyczące rozwiązywania podstawowych problemów, które mogą pojawić się podczas korzystania z Kaspersky Security Center, w tym związanych z zarządzaniem urządzeniami mobilnymi użytkowników.

W tej sekcji:

Ograniczenia Kaspersky Security Center

Poniższa tabela wyświetla ograniczenia bieżącej wersji Kaspersky Security Center 10 Service Pack 2.

Tabela 9. Ograniczenia Kaspersky Security Center 10 Service Pack 2

Rodzaj ograniczenia	Wartość
Maksymalna liczba zarządzanych komputerów	50 000
Maksymalna dozwolona liczba komputerów z zaznaczonym polem **Nie odłączaj od Serwera administracyjnego**.	300
Maksymalna liczba grup administracyjnych	10 000
Maksymalna liczba przechowywanych zdarzeń	15 000 000
Maksymalna liczba profili	2 000
Maksymalna liczba zadań	2 000
Maksymalna dozwolona liczba obiektów Active Directory (jednostek organizacyjnych i kont użytkowników, komputerów oraz grup bezpieczeństwa)	1 000 000
Maksymalna liczba profili w zasadzie	100
Maksymalna liczba podrzędnych Serwerów administracyjnych w jednym nadrzędnym Serwerze administracyjnym	500
Maksymalna liczba wirtualnych Serwerów administracyjnych	200

Rodzaj ograniczenia	Wartość
Maksymalna liczba komputerów, które może obsługiwać jeden Agent aktualizacji	500

Wymagania sprzętowe dla systemu zarządzania bazą danych i Serwera administracyjnego

W poniższej tabeli zostały uwzględnione minimalne wymagania sprzętowe dla DBMS i Serwera administracyjnego obejmującego 50 000 komputerów.

Serwer administracyjny i serwer SQL Server są instalowane na tym samym komputerze

Tabela 10. Wymagania sprzętowe dla komputera

Procesor	8 rdzeni, 2500 do 3000 MHz
Pamięć RAM	16 GB
Dysk twardy	500 GB, SATA RAID
Karta sieciowa	1 Gbit
System operacyjny	Windows x86–64

Serwer administracyjny i serwer SQL Server są instalowane na różnych komputerach

Tabela 11. Wymagania sprzętowe dla komputera z Serwerem administracyjnym

Procesor	4 rdzeni, 2500 do 3000 MHz
Pamięć RAM	8 GB

Dysk twardy	300 GB, zalecany RAID
Karta sieciowa	1 Gbit
System operacyjny	Windows x86–64

Tabela 12. Wymagania sprzętowe dla komputera z serwerem SQL Server

Procesor	4 rdzeni, 2500 do 3000 MHz
Pamięć RAM	16 GB
Dysk twardy	200 GB, SATA RAID
Karta sieciowa	1 Gbit
System operacyjny	Windows x86–64

Założenia są następujące:

- Agenty aktualizacji są przydzielane w sieci firmowej, a każdy z nich obejmuje od 100 do 200 komputerów.
- Zadanie tworzenia kopii zapasowej zapisuje kopie zapasowe w zasobie plików znajdującym się na dedykowanym serwerze.
- Interwał synchronizacji dla Agentów sieciowych jest ustawiony w taki sposób, w jaki opisano to w poniższej tabeli.

Tabela 13. Interwał synchronizacji dla Agentów sieciowych

Okres synchronizacji (minuty)	Liczba zarządzanych komputerów
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000

Określanie przestrzeni dyskowej dla Agenta aktualizacji

Agent aktualizacji wymaga przynajmniej 4 GB wolnej przestrzeni na dysku.

Jeśli jakiekolwiek zadanie zdalnej instalacji jest dostępne na Serwerze administracyjnym, komputer z zainstalowanym Agentem aktualizacji będzie wymagał także wolnej przestrzeni na dysku równej całkowitemu rozmiarowi pakietów instalacyjnych przeznaczonych do zainstalowania.

Jeśli na Serwerze administracyjnym jest dostępne jedno lub kilka zadań instalacji uaktualnień (łat) i naprawy luk, komputer z zainstalowanym Agentem aktualizacji będzie wymagał także wolnej przestrzeni na dysku równej podwojonej wartości całkowitego rozmiaru wszystkich łat przeznaczonych do zainstalowania.

Wstępna ocena miejsca niezbędnego dla bazy danych i dysku twardego Serwera administracyjnego

Ocenianie miejsca niezbędnego dla bazy danych Serwera administracyjnego

Przybliżoną ilość miejsca, jaką powinna zajmować baza danych, można określić, korzystając z następującego wzoru:

(200 * C + 2.3 * E + 2.5 * A), kB

gdzie:

C to	Liczba komputerów
E to	Liczba przechowywanych zdarzeń
A to	Całkowita liczba obiektów Active Directory: • Konta komputerów • Konta użytkowników • Konta grup bezpieczeństwa • Jednostki organizacyjne Active Directory. Jeśli skanowanie Active Directory jest wyłączone, zmienna A będzie równa zero.

Jeśli Serwer administracyjny rozsyła aktualizacje systemu Windows (zachowując się przy tym jak serwer Windows Server Update Services (WSUS)), baza danych będzie wymagała dodatkowych 2,5 GB na dysku.

Zauważ, że gdy uruchomiona jest aplikacja, w bazie danych zawsze pojawia się jakaś ilość nieprzydzielonego miejsca. Dlatego też, rzeczywisty rozmiar pliku bazy danych (domyślnie jest to plik KAV.MDF, jeśli jako DBMS używasz serwera SQL Server) okazuje się być około dwukrotnie większy niż ilość miejsca zajmowanego przez bazę danych.

Dziennik transakcji (domyślnie jest to plik KAV_log.LDF, jeśli jako DBMS używasz serwera SQL Server) może osiągać rozmiar 2 GB.

Ocenianie miejsca na komputerze z zainstalowanym Serwerem administracyjnym

Przybliżona ilość miejsca na dysku w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit na komputerze z zainstalowanym Serwerem administracyjnym może zostać oszacowana przy użyciu następującego wzoru:

(220 * C + 0.15 * E + 0.17 * A), kB

W celu poznania wartości zmiennych C, E i A należy zapoznać się z powyższą tabelą.

Uaktualnienia

Folder współdzielony potrzebuje przynajmniej 4 GB do przechowywania uaktualnień.

Pakiety instalacyjne

Jeśli niektóre pakiety instalacyjne są przechowywane na Serwerze administracyjnym, folder współdzielony będzie wymagał dodatkowej ilości miejsca na dysku, równej całkowitemu rozmiarowi tych wszystkich pakietów instalacyjnych.

Zadania zdalnej instalacji

Jeśli jakiekolwiek zadanie zdalnej instalacji jest dostępne na Serwerze administracyjnym, komputer z zainstalowanym Serwerem administracyjnym będzie wymagał dodatkowej wolnej przestrzeni na dysku (w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit) równej całkowitemu rozmiarowi wszystkich pakietów instalacyjnych przeznaczonych do zainstalowania.

Łaty

Jeśli Serwer administracyjny jest zaangażowany w instalację łat, niezbędna jest dodatkowa ilość wolnego miejsca na dysku:

- W folderze z łatami—ilość miejsca na dysku równa całkowitemu rozmiarowi wszystkich pobranych łat. Domyślny folder do przechowywania łat to %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\wusfiles. Folder można zmienić przy użyciu narzędzia klsrvswch. Jeśli Serwer administracyjny jest używany jako serwer WSUS, zalecane jest przydzielenie temu folderowi przynajmniej 100 GB.

- W folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit—ilość miejsca na dysku równa całkowitemu rozmiarowi łat, do których odwołuje się istniejące zadanie instalacji aktualizacji (łat) i eliminacji luk.

Ocenianie ilości ruchu między Agentem sieciowym a Serwerem administracyjnym

Tabela znajdująca się poniżej zawiera przeciętny dzienny ruch sieciowy pomiędzy Serwerem administracyjnym Kaspersky Security Center 10 MR1 (wersja 10.1.249) a zarządzanym komputerem (z Agentem sieciowym Kaspersky Security Center 10 MR1 w wersji 10.1.249 i Kaspersky Endpoint Security 10 MR1 w wersji 10.2.1.23).

Tabela 14. Przeciętny dzienny wskaźnik ruchu sieciowego Kaspersky Security Center 10 MR1

	Z Serwera do zarządzanego komputera (pobranie)	**Z zarządzanego komputera do Serwera administracyjnego (wysłanie)**
Przeciętny dzienny wskaźnik ruchu sieciowego z domyślnymi ustawieniami zadania aktualizacji	27 MB	2,7 MB
Przeciętny dzienny wskaźnik ruchu sieciowego z wyłączonym zadaniem aktualizacji	0,8 MB	1 MB

Tabela znajdująca się poniżej zawiera przeciętny dzienny ruch sieciowy pomiędzy Serwerem administracyjnym Kaspersky Security Center 10 Service Pack 2 a zarządzanym komputerem (z Agentem sieciowym Kaspersky Security Center 10 Service Pack 2 i Kaspersky Endpoint Security 10 Service Pack 2).

Tabela 15. Przeciętny dzienny wskaźnik ruchu sieciowego: Kaspersky Security Center 10 Service Pack 2

	Z Serwera do zarządzanego komputera (pobranie)	Z zarządzanego komputera do Serwera administracyjnego (wysłanie)
Przeciętny dzienny wskaźnik ruchu sieciowego z domyślnymi ustawieniami zadania aktualizacji	17 MB	3,5 MB
Przeciętny dzienny wskaźnik ruchu sieciowego z wyłączonym zadaniem aktualizacji	0,8 MB	1 MB

Rozwiązywanie problemów

Ta sekcja zawiera informacje na temat najczęstszych błędów i problemów, jakie można napotkać podczas zdalnej instalacji i korzystania z Kaspersky Security Center, a także zalecenia dotyczące rozwiązywania tych błędów i problemów.

W tej sekcji:

Problemy ze zdalną instalacją aplikacji

Poniższa tabela zawiera problemy, które mogą wystąpić podczas zdalnej instalacji aplikacji, a także podstawowe przyczyny wystąpienia tych problemów.

Tabela 16. Problemy ze zdalną instalacją aplikacji

Problem	Podstawowe przyczyny i rozwiązania
Uprawnienia do instalacji są niewystarczające	Konto, z poziomu którego uruchomiona jest instalacja, posiada niewystarczające uprawnienia do wykonania działań wymaganych do zainstalowania aplikacji.
Mała ilość miejsca na dysku	Na dysku nie ma wystarczającej ilości miejsca na zakończenie instalacji. Zwolnij miejsce na dysku i spróbuj ponownie zainstalować aplikację.
Niezaplanowane ponowne uruchomienie systemu operacyjnego	Podczas instalacji nastąpiło niezaplanowane ponowne uruchomienie systemu operacyjnego. Dokładny wynik instalacji może być niedostępny. Sprawdź, czy ustawienia instalatora zostały poprawnie skonfigurowane lub skontaktuj się z pomocą techniczną.
Wymagany plik nie został odnaleziony	Wymagany plik nie został odnaleziony w pakiecie instalacyjnym. Sprawdź pakiet instalacyjny pod kątem integralności.
Niekompatybilna platforma	Pakiet instalacyjny nie jest przeznaczony dla tej platformy. Użyj dedykowanego pakietu instalacyjnego.
Niekompatybilna aplikacja	Na komputerze jest już zainstalowana aplikacja niekompatybilna z instalowanym produktem. Przed rozpoczęciem instalacji usuń wszystkie aplikacje, które są wymienione jako niekompatybilne.

Problem	Podstawowe przyczyny i rozwiązania
Słabe wymagania systemowe	Pakiet instalacyjny wymaga dodatkowego oprogramowania w systemie. Sprawdź, czy konfiguracja systemu spełnia wymagania systemowe instalowanej aplikacji.
Niekompletna instalacja	Poprzednia instalacja lub dezinstalacja aplikacji nie zakończyła się normalnie. Aby zakończyć poprzednią instalację lub dezinstalację aplikacji na tym komputerze, należy uruchomić ponownie system operacyjny i spróbować ponownie zainstalować produkt.
Nieodpowiednia wersja instalatora	Instalacja tego pakietu instalacyjnego nie jest obsługiwana przez wersję instalatora, który znajduje się na tym komputerze.
Instalacja jest już uruchomiona	Na tym komputerze jest już uruchomiona instalacja innej aplikacji.
Nie można było otworzyć pakietu instalacyjnego.	Nie można było otworzyć pakietu instalacyjnego Możliwe przyczyny: Brakuje pakietu, pakiet jest uszkodzony, nie ma wystarczających uprawnień dostępu do pakietu.
Niekompatybilna lokalizacja	Pakiet instalacyjny nie jest przeznaczony do instalacji na tej wersji językowej systemu operacyjnego.
Instalacja zablokowana przez profil	Instalacja aplikacji na tym komputerze jest zablokowana przez profil.

Problem	Podstawowe przyczyny i rozwiązania
Błąd zapisu pliku	Podczas instalacji aplikacji wystąpił błąd zapisu. Sprawdź konto, z poziomu którego została uruchomiona instalacja, pod kątem wymaganych uprawnień i oszacuj ilość wolnego miejsca na dysku.
Nieprawidłowe hasło dezinstalacyjne	Hasło do dezinstalacji aplikacji jest niepoprawne.
Słabe wymagania sprzętowe	Sprzęt nie spełnia wymagań aplikacji (pamięć RAM, wolna przestrzeń na dysku twardym itd.).
Nieprawidłowy folder instalacyjny	Aplikacja nie może zostać zainstalowana w określonym folderze, gdyż jest on zablokowany przez profil instalatora.
Po ponownym uruchomieniu systemu wymagane jest podjęcie nowej próby przeprowadzenia instalacji	Po ponownym uruchomieniu komputera należy uruchomić ponownie instalator aplikacji.
W celu kontynuacji instalacji wymagane jest ponowne uruchomienie systemu	Aby kontynuować pracę instalatora, należy uruchomić ponownie komputer.

Niepoprawne kopiowanie obrazu dysku twardego

Jeśli dysk twardy z zainstalowanym Agentem sieciowym został skopiowany bez postępowania zgodnie z regułami zdalnej instalacji (sekcja "Zdalna instalacja poprzez przechwycenie i skopiowanie obrazu dysku twardego komputera" na stronie 69), niektóre komputery mogą zostać wyświetlone w Konsoli administracyjnej pod postacią pojedynczej ikony z ciągle zmieniającą się nazwą.

Ten problem można rozwiązać przy użyciu jednej z następujących metod:

- Usuwając Agenta sieciowego.

  Ta metoda jest najbardziej niezawodna. Na komputerach, które zostały niepoprawnie skopiowane z obrazu, należy usunąć Agenta sieciowego przy użyciu narzędzi innych firm, a następnie zainstalować go ponownie. Agent sieciowy nie może zostać usunięty przy użyciu narzędzi Kaspersky Security Center, ponieważ Serwer administracyjny nie potrafi odróżnić wadliwych komputerów (w Konsoli administracyjnej mają tę samą ikonę).

- Uruchamiając narzędzie klmover z przełącznikiem "-dupfix".

  Użyj narzędzi firm trzecich, aby raz uruchomić narzędzie klmover, znajdujące się w folderze instalacyjnym Agenta sieciowego, z przełącznikiem "-dupfix" (klmover -dupfix) na wadliwych komputerach (tych, które zostały niepoprawnie skopiowane z obrazu). Narzędzie nie może zostać uruchomione przy użyciu narzędzi Kaspersky Security Center, ponieważ Serwer administracyjny nie potrafi odróżnić wadliwych komputerów (w Konsoli administracyjnej mają tę samą ikonę).

  Następnie, przed uruchomienie narzędzia, usuń ikonę, pod którą wadliwe komputery były wyświetlane.

- Wzmacniając regułę wykrywania niepoprawnie skopiowanych komputerów.

  > Ta metoda jest stosowana tylko wtedy, gdy zainstalowany jest Serwer administracyjny oraz Agent sieciowy w wersji 10 SP1 lub nowszej.

  Reguła wykrywania niepoprawnie skopiowanych Agentów sieciowych musi zostać wzmocniona w taki sposób, że zmiana nazwy NetBIOS komputera spowoduje automatyczną "naprawę" tych Agentów sieciowych (przy założeniu, że wszystkie skopiowane komputery posiadają unikatowe nazwy NetBIOS).

  Na komputerze z zainstalowanym Serwerem administracyjnym należy zaimportować plik reg (wyświetlony poniżej) do Rejestru, a następnie uruchomić ponownie usługę Serwera administracyjnego.

  - Jeśli na komputerze z Serwerem administracyjnym zainstalowany jest 32-bitowy system operacyjny:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]

“KLSRV_CheckClones”=dword:00000003
```

- Jeśli na komputerze z Serwerem administracyjnym zainstalowany jest 64-bitowy system operacyjny:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Products\1093\1.0.0.0\ServerFlags]

“KLSRV_CheckClones”=dword:00000003
```

Problemy z serwerem urządzeń mobilnych Exchange ActiveSync

Ta sekcja zawiera informacje o błędach i problemach, które mogą wystąpić podczas korzystania z serwera urządzeń mobilnych Exchange ActiveSync.

Błąd podczas instalacji serwera urządzeń mobilnych Exchange ActiveSync

Jeśli podczas lokalnej lub zdalnej instalacji wystąpił błąd, możesz poznać przyczynę wystąpienia błędu, sprawdzając plik error.log znajdujący się na komputerze, na którym została uruchomiona instalacja produktu, w następującej lokalizacji: C:\Windows\Temp\klmdm4exch-2014-11-28-15-56-37\ (liczby oznaczają datę i czas zainstalowania produktu). W większości przypadków informacje z pliku error.log są wystarczające do rozwiązania problemu.

Poniższa tabela wyświetla przykłady najczęstszych błędów zarejestrowanych w pliku error.log.

Tabela 17. Najczęstsze błędy

Błąd	Opis	Przyczyna
Błąd wystąpił w kroku instalacji: 'Sprawdzanie połączenia z PowerShell'	Błąd: Przetwarzanie danych ze zdalnego serwera nie powiodło się i został zwrócony następujący komunikat o błędzie: Do użytkownika "oreh-security.ru/Users/TestInstall" nie jest przypisana żadna z ról zarządzania.	Konto, z poziomu którego została uruchomiona instalacja produktu, nie posiada roli Zarządzanie organizacją.

Błąd	Opis	Przyczyna
Błąd wystąpił w kroku instalacji: 'Sprawdzanie połączenia z PowerShell'	Nawiązanie połączenia ze zdalnym serwerem nie powiodło się i został zwrócony następujący komunikat o błędzie: Klient WinRM nie może przetworzyć żądania. Mechanizm uwierzytelniania, zażądany przez klienta, nie jest obsługiwany przez serwer lub ruch niezaszyfrowany jest wyłączony w konfiguracji usługi. Sprawdź ustawienia ruchu niezaszyfrowanego w konfiguracji usługi lub określ jeden z mechanizmów uwierzytelniania obsługiwanych przez serwer. Aby użyć mechanizmu Kerberos, określ nazwę komputera jako docelowe miejsce zdalne. Sprawdź także, czy komputer kliencki i komputer docelowy są połączone w domenę. Aby użyć mechanizmu Basic, określ nazwę komputera jako docelowe miejsce zdalne, wybierz uwierzytelnianie Basic oraz podaj nazwę użytkownika i hasło. Możliwe mechanizmy uwierzytelniania zgłoszone przez serwer: Więcej informacji można znaleźć w sekcji "Informacje o zdalnym rozwiązywaniu problemów".	Mechanizm Uwierzytelniania systemu Windows nie jest włączony w ustawieniach serwera sieciowego IIS dla katalogu wirtualnego PowerShell.

Lista urządzeń i kont poczty jest pusta

Aby odkryć przyczynę problemu, który uniemożliwia uzyskanie listy urządzeń i kont poczty, możesz wyświetlić zapisane zdarzenia w Konsoli administracyjnej, w folderze **Raporty**

i powiadomienia/Zdarzenia/Błędy funkcjonalne. Jeśli zdarzenia nie zawierają żadnych informacji, sprawdź połączenie między Agentem sieciowym na komputerze, na którym zainstalowany jest serwer urządzeń mobilnych Exchange ActiveSync, a Serwerem administracyjnym.

Problemy z serwerem urządzeń mobilnych iOS MDM

Ta sekcja zawiera informacje o błędach i problemach, które mogą wystąpić podczas korzystania z serwera urządzeń mobilnych iOS MDM, a także sposoby radzenia sobie z tymi błędami i problemami.

W tej sekcji:

Portal support.kaspersky.com/pl

Informacje o niektórych problemach, występujących podczas korzystania z serwera urządzeń mobilnych iOS MDM, zostały zamieszczone w Bazie wiedzy na stronie działu pomocy technicznej: http://support.kaspersky.com/pl/ks10mob.

Sprawdzanie dostępności usługi APN

W celu sprawdzenia dostępności usługi APN, możesz użyć następujących poleceń z narzędzia Telnet:

- Po stronie usługi sieciowej iOS MDM:

```
$ telnet gateway.push.apple.com 2195
```

- Po stronie urządzenia iOS MDM (sprawdzanie musi się odbyć w sieci, w której znajduje się urządzenie):

```
$ telnet 1-courier.push.apple.com 5223
```

Zalecane metody rozwiązywania problemów z usługą sieciową iOS MDM

Jeśli podczas korzystania z usługi sieciowej iOS MDM napotkasz pewne problemy, wykonaj następujące czynności:

1. Sprawdź prawidłowość certyfikatów.
2. Sprawdź, czy w zdarzeniach Konsoli administracyjnej nie ma błędów oraz niewykonanych poleceń ze strony serwera urządzeń mobilnych iOS MDM.
3. Sprawdź urządzenie przy użyciu konsoli narzędzia iPhone Configuration Utility.
4. Sprawdź pliki śledzenia usługi sieciowej iOS MDM: Wewnętrzne usługi, takie jak usługa RPC oraz usługa sieciowa (100 strumieni), muszą zostać pomyślnie uruchomione.

Sprawdzanie prawdziwości certyfikatów usługi sieciowej iOS MDM przy użyciu wieloplatformowego narzędzia bazującego na OpenSSL

Przykład polecenia:

```
$ openssl s_client -connect mymdm.mycompany.com:443
```

Wynik wykonania

```
CONNECTED(00000003)

...
```

Łańcuch certyfikatu

0 s:/C=RU/ST=Msk/L=Msk/O=My Company/OU=AdminKit/CN=mymdm.mycompany.com

i:/CN=Kaspersky iOS MDM Server CA

...

.

Sprawdzanie plików śledzenia usługi sieciowej iOS MDM

Informacje dotyczące uzyskania plików śledzenia usługi sieciowej iOS MDM można znaleźć w odpowiednim artykule z Bazy wiedzy na stronie działu pomocy technicznej: http://support.kaspersky.com/pl/9792.

Przykład pomyślnego wygenerowania plików śledzenia:

I1117 20:58:39.050226 7984] [MAIN]: Starting service...

I1117 20:58:39.050226 7984] [RPC]: Starting rpc service...

...

I1117 20:58:39.081428 7984] [RPC]: Rpc service started

I1117 20:58:39.081428 3724] [WEB]: Starting web service...

I1117 20:58:39.455832 3724] [WEB]: Starting thread [T000]

I1117 20:58:39.455832 3724] [WEB]: Starting thread [T001]

...

I1117 20:58:39.455832 3724] [WEB]: Starting thread [T099]

Przykład śledzenia z zajętym gniazdem:

[WEB]: Starting web service...

Error 28 fault: SOAP-ENV:Server [no subcode] "Only one usage of each socket address (protocol/network address/port) is normally permitted."

Detail: [no detail]

[WEB]: Web service terminated

Sprawdzanie plików śledzenia przy użyciu konsoli narzędzia iPhone Configuration Utility

Przykład pomyślnego wygenerowania plików śledzenia:

Services covering MDM – profiled, mdmd

mdmd[174] <Notice>: (Note) MDM: mdmd starting...

mdmd[174] <Notice>: (Note) MDM: Looking for managed app states to clean up

profiled[175] <Notice>: (Note) profiled: Service starting...

mdmd[174] <Notice>: (Note) MDM: Network reachability has changed.

mdmd[174] <Notice>: (Note) MDM: Network reachability has changed.

mdmd[174] <Notice>: (Note) MDM: Polling MDM server https://10.255.136.71 for commands

mdmd[174] <Notice>: (Note) MDM: Transaction completed. Status: 200

mdmd[174] <Notice>: (Note) MDM: Attempting to perform MDM request: DeviceLock

mdmd[174] <Notice>: (Note) MDM: Handling request type: DeviceLock

mdmd[174] <Notice>: (Note) MDM: Command Status: Acknowledged

profiled[175] <Notice>: (Note) profiled: Recomputing passcode requirement message

profiled[175] <Notice>: (Note) profiled: Locking device

mdmd[174] <Notice>: (Note) MDM: Transaction completed. Status: 200

mdmd[174] <Notice>: (Note) MDM: Server has no commands for this device.

mdmd[174] <Notice>: (Note) MDM: mdmd stopping...

Problemy z urządzeniami KES

Ta sekcja zawiera informacje o błędach i problemach, które mogą wystąpić podczas korzystania z urządzeń KES, a także sposoby radzenia sobie z nimi.

W tej sekcji:

Portal support.kaspersky.com/pl

Informacje o problemach, które mogą pojawić się podczas korzystania z urządzeń KES, można znaleźć w Bazie wiedzy na stronie działu pomocy technicznej http://support.kaspersky.com/pl/ks10mob.

Sprawdzanie ustawień usługi Google Cloud Messaging

Sprawdzanie ustawień Google Cloud Messaging może zostać wykonane na portalu Google https://code.google.com/apis/console/#project:[YOUR PROJECT NUMBER]:access.

Sprawdzanie dostępności usługi Google Cloud Messaging

Aby sprawdzić dostępność usługi Google Cloud Messaging po stronie Kaspersky Security Center (sekcja "Korzystanie z Google Cloud Messaging" na stronie 114), możesz użyć następującego polecenia Telnet:

```
$ telnet android.googleapis.com 443
```

Problemy związane z Network Access Control (NAC)

Ta sekcja zawiera informacje o błędach i problemach, które mogą wystąpić podczas korzystania z Network Access Control (NAC).

Nie można uruchomić Agenta NAC na Agencie sieciowym

Możliwa przyczyna:

- Komponenty NAC nie zostały zainstalowane lub zostały zainstalowane z błędami. Opis tego błędu musi zostać dodany do dziennika zdarzeń Kaspersky Lab.

Możliwe rozwiązanie:

- Wyeliminuj przyczynę błędu (jeśli to możliwe) i uruchom ponownie usługę Kaspersky Network Agent.

Usługa NAC została skonfigurowana w profilu, a Agent NAC jest włączony, ale reguła NAC nie może zostać zastosowana (aktywność urządzenia nie jest ograniczona przez Agenta NAC)

Możliwa przyczyna:

- Niepoprawne ustawienia reguł NAC w profilu

Możliwe rozwiązania:

- Sprawdź, czy urządzenie spełnia kryteria nadane w obiekcie sieciowym.
- Sprawdź, czy Agent NAC działa w trybie standardowym i czy w dzienniku zdarzeń Kaspersky Lab na hoście nie są wyświetlane żadne komunikaty o błędach.
- Sprawdź, czy komputer z Agentem NAC działa w tej samej domenie rozgłoszeniowej co urządzenie.

Usługa NAC została skonfigurowana w profilu, Agent NAC jest uruchomiony, reguła jest stosowana, ale mimo to dostęp urządzenia do zasobów jest nieograniczony (w środowisku wirtualnym)

Możliwa przyczyna:

- Niepoprawne ustawienia infrastruktury sieci.

Możliwe rozwiązania:

- Dla VMvare ESXi™:
    - Opcje Promiscuous Mode, MAC Address Changes i Forged Transmits muszą być włączone w trybie Accept.
- Dla Microsoft Hyper-V:
    - Na serwerze z rolą Hyper-V, dla każdej maszyny wirtualnej <nazwa_maszyny_wirtualnej> należy uruchomić: Set-VMNetworkAdapter –VMName <nazwa_maszyny_wirtualnej> –MacAddressSpoofing On.

Duże obciążenie procesora w trybie jądra

Możliwa przyczyna:

- Olbrzymia aktywność rozgłoszeniowa w domenie sieci (tysiące urządzeń) lub Agent NAC jest przeładowany innymi działaniami niskiego poziomu (I/O dysku, usługi sieciowe plików itd.)

Możliwe rozwiązania:

- Przenieś Agenta NAC na inny komputer, który jest mniej obciążony
- Przenieś lub wyłącz usługi z dużymi wymaganiami odnośnie procesora w trybie jądra.

Reguła "Przekieruj na portal autoryzacji" nie działa

Możliwa przyczyna:

- Niepoprawne ustawienia usługi NAC w profilu
- Niepoprawne ustawienia infrastruktury sieci.

Możliwe rozwiązania:

- Sprawdź, czy reguła może działać i jest stosowana do urządzenia (sekcja "Określanie stosowania reguły NAC" na stronie 135).
- Sprawdź, czy usługa Kaspersky Captive Portal service działa na Agencie NAC, a w dzienniku zdarzeń Kaspersky Lab nie jest wyświetlany żaden błąd związany z tą usługą.
- Sprawdź, czy port TCP o numerze 80 (domyślnie używany przez usługę Kaspersky Captive Portal service) nie jest zajęty przez inne serwery sieciowe. Jeśli port jest zajęty, zwolnij go (przenosząc serwer sieciowy na inny host w sieci) i uruchom ponownie usługę Kaspersky Captive Portal service. Po zwolnieniu portu i ponownym uruchomieniu usługi, sprawdź, czy w przeglądarce na komputerze z Agentem NAC otwiera się strona autoryzacyjna po kliknięciu odnośnika przedstawionego jako `http://<host_kontrolujący>`.

Skanowanie zostało zakończone, ale typ urządzenia lub wersja systemu operacyjnego nie może zostać określona

Możliwa przyczyna:

- Usługa Kaspersky Network Scanner nie jest uruchomiona
- Porty sieciowe są zamknięte na tym urządzeniu.

Możliwe rozwiązania:

- Sprawdź, czy usługa KNS może być uruchomiona, a w dzienniku zdarzeń Kaspersky Lab nie ma żadnego opisu błędu. Jeśli pojawi się błąd, spróbuj go wyeliminować (jeśli to możliwe) i uruchom ponownie usługę.
- Upewnij się, że zapora sieciowa, która może kolidować z aktywnym skanowaniem portów sieciowych, jest wyłączona na tym urządzeniu.

Kontakt z działem pomocy technicznej

Ta sekcja zawiera informacje dotyczące sposobów i warunków świadczenia pomocy technicznej.

W tej sekcji:

Jak uzyskać pomoc techniczną

Jeśli nie znajdziesz rozwiązania swojego problemu w dokumentacji dla aplikacji lub w jednym z dodatkowych źródeł informacji o aplikacji, zalecamy skontaktować się z działem pomocy technicznej. Eksperci z działu pomocy technicznej odpowiedzą na Twoje pytania związane z instalacją i użytkowaniem aplikacji.

Pomoc techniczna jest świadczona tylko tym użytkownikom, którzy zakupili licencję komercyjną. Użytkownicy posiadający licencję testową nie są uprawnieni do otrzymania pomocy technicznej.

Przed skontaktowaniem się z działem pomocy technicznej przeczytaj zasady korzystania z pomocy technicznej (http://support.kaspersky.com/pl/support/rules).

Możesz skontaktować się z działem pomocy technicznej na jeden z następujących sposobów:

- Dzwoniąc do pomocy technicznej (http://support.kaspersky.com/b2b#region2).
- Wysyłając zgłoszenie do pomocy technicznej Kaspersky Lab poprzez portal CompanyAccount (https://companyaccount.kaspersky.com).

Pomoc techniczna za pośrednictwem telefonu

W przypadku problemów wymagających szybkiego rozwiązania, możesz zadzwonić do specjalistów z pomocy technicznej Kaspersky Lab. Informacje dotyczące uzyskania wsparcia technicznego oraz dane kontaktowe pomocy technicznej można znaleźć na stronie internetowej działu pomocy technicznej Kaspersky Lab (http://support.kaspersky.com/b2b#region2).

Przed skontaktowaniem się z działem pomocy technicznej przeczytaj zasady korzystania z pomocy technicznej (http://support.kaspersky.com/pl/support/rules).

Pomoc techniczna poprzez CompanyAccount

CompanyAccount (https://companyaccount.kaspersky.com) jest to portal dla firm korzystających z aplikacji firmy Kaspersky Lab. Portal CompanyAccount został zaprojektowany w celu ułatwienia interakcji między użytkownikami a specjalistami z Kaspersky Lab poprzez zgłoszenia online. Portal CompanyAccount umożliwia monitorowanie stopnia przetworzenia zgłoszenia elektronicznego przez specjalistów z Kaspersky Lab, a także przechowywanie historii zgłoszeń elektronicznych.

Możliwe jest zarejestrowanie wszystkich pracowników firmy pod jednym kontem w serwisie CompanyAccount. Jedno konto umożliwia scentralizowane zarządzanie zgłoszeniami elektronicznymi zarejestrowanych pracowników oraz zarządzanie uprawnieniami tych pracowników poprzez CompanyAccount.

Portal CompanyAccount jest dostępny w następujących językach:

- angielskim
- hiszpańskim
- włoskim
- niemieckim
- polskim

- portugalskim
- rosyjskim
- francuskim
- japońskim.

Więcej informacji o CompanyAccount można znaleźć na stronie pomocy technicznej (http://support.kaspersky.com/pl/faq/companyaccount_help).

AO Kaspersky Lab

Kaspersky Lab jest znanym na całym świecie producentem systemów do ochrony komputerów przed różnymi typami zagrożeń, w tym wirusami, szkodliwym oprogramowaniem, spamem, atakami sieciowymi i hakerskimi.

W 2008 roku firma Kaspersky Lab zajęła miejsce wśród czwórki czołowych producentów światowej klasy oprogramowania do ochrony danych (według rankingu "IDC Worldwide Endpoint Security Revenue by Vendor"). Według badań rynkowych "IDC Endpoint Tracker 2014", zrealizowanych przez agencję badawczą IDC, Kaspersky Lab jest preferowanym producentem systemów do ochrony komputerów w Rosji.

Firma Kaspersky Lab została założona w 1997 roku w Rosji. Obecnie Kaspersky Lab jest międzynarodową grupą firm z 34 biurami w 31 krajach. Firma zatrudnia ponad 3000 wykwalifikowanych specjalistów.

PRODUKTY. Produkty firmy Kaspersky Lab zapewniają ochronę wszystkich systemów— począwszy od komputerów domowych, aż po sieci dużych korporacji.

Linia produktów dla domu i małych biur obejmuje oprogramowanie zabezpieczające dla komputerów stacjonarnych, laptopów, tabletów oraz smartfonów i innych urządzeń mobilnych.

Firma oferuje rozwiązania i technologie służące do ochrony i kontroli stacji roboczych, urządzeń mobilnych, maszyn wirtualnych, serwerów plików i serwerów sieciowych, bram pocztowych oraz zapór sieciowych. Na portfolio firmy składają się także specjalistyczne produkty służące do ochrony przed atakami DDoS, do ochrony środowisk zarządzanych przez przemysłowe systemy kontroli oraz do zapobiegania oszustwom finansowym. W połączeniu ze scentralizowanymi narzędziami do zarządzania firmy Kaspersky Lab rozwiązania te zapewniają różnego rodzaju organizacjom efektywną, zautomatyzowaną ochronę przed zagrożeniami komputerowymi. Produkty Kaspersky Lab posiadają certyfikaty głównych laboratoriów testujących, są kompatybilne z wieloma programami komputerowymi oraz są zoptymalizowane z myślą o działaniu na wielu platformach sprzętowych.

Analitycy wirusów Kaspersky Lab pracują przez dwadzieścia cztery godziny na dobę. Każdego dnia odkrywają oni setki tysięcy nowych zagrożeń oraz tworzą narzędzia do ich wykrywania

i leczenia, które następnie umieszczają w bazach danych używanych przez aplikacje firmy Kaspersky Lab.

TECHNOLOGIE. Wiele technologii, które są obecnie nieodłączną częścią nowoczesnych narzędzi antywirusowych, zostało stworzonych przez Kaspersky Lab. To nie przypadek, że wielu innych producentów oprogramowania używa w swoich produktach silnika Kaspersky Anti-Virus. Należą do nich: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu oraz ZyXEL. Wiele innowacyjnych technologii naszej firmy zostało opatentowanych.

OSIĄGNIĘCIA. Przez lata firma Kaspersky Lab otrzymała setki nagród i wyróżnień za swoje zasługi w walce z zagrożeniami komputerowymi. Na przykład w 2014 roku program Kaspersky Anti-Virus był jednym z dwóch liderów i otrzymał kilka najwyższych nagród Advanced+ w testach przeprowadzonych przez AV-Comparatives, szanowane austriackie laboratorium antywirusowe, uzyskując w efekcie certyfikat "Top Rated". Jednakże największym osiągnięciem Kaspersky Lab jest zaufanie i lojalność użytkowników na całym świecie. Nasze produkty i technologie chronią ponad 400 milionów użytkowników oraz ponad 270 000 klientów korporacyjnych.

Oficjalna strona Kaspersky Lab:	http://www.kaspersky.pl
Encyklopedia Wirusów:	http://www.securelist.pl/
Laboratorium antywirusowe:	http://newvirus.kaspersky.com (do skanowania podejrzanych plików i stron internetowych)
Forum internetowe Kaspersky Lab:	http://forum.kaspersky.com

Informacje o znakach towarowych

Zastrzeżone znaki towarowe i nazwy usług są własnością ich właścicieli.

Apple, iPhone są zastrzeżonymi znakami towarowymi firmy Apple Inc. zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

Xen jest znakiem towarowym firmy Citrix Systems, Inc. i / lub jej oddziałów zarejestrowanych w Urzędzie patentowym w Stanach Zjednoczonych i innych krajach.

Android, Google są zastrzeżonymi znakami towarowymi firmy Google, Inc.

JavaScript jest zastrzeżonym znakiem towarowym firmy Oracle Corporation i / lub jej oddziałów.

Active Directory, ActiveSync, Forefront, Microsoft, HyperV, SQL Server, Windows i Windows PowerShell są zastrzeżonymi znakami towarowymi firmy Microsoft Corporation zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

UNIX jest zastrzeżonym znakiem towarowym w Stanach Zjednoczonych i innych krajach, używanym na licencji firmy X/Open Company Limited.

VMware i ESXi są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy VMware, Inc. zarejestrowanymi w Stanach Zjednoczonych i innych krajach.