Kaspersky Security Center 10.0

ROZPOCZĘCIE PRACY

WERSJA APLIKACJI: 10,0

Drogi Użytkowniku,

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

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

Data korekty dokumentu: 13.12.2012

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

SPIS TREŚCI

INFORMACJE O PODRĘCZNIKU

Dokument ten opisuje kroki, które umożliwią Ci szybko rozpocząć pracę z programem Kaspersky Security Center 10.0 (zwany dalej Kaspersky Security Center) i wdrożyć system ochrony w sieci firmowej w oparciu o aplikacje Kaspersky Lab.

Odbiorcami tego podręcznika są administratorzy sieci firmowych oraz dostawcy usług SaaS (zwani dalej dostawcami usługi).

Ten dokument zawiera szczegółowy opis prostego scenariusza instalacji Kaspersky Security Center, kiedy system ochrony jest instalowany na kilku komputerach działających pod kontrolą systemu Microsoft® Windows® w sieci firmowej. Scenariusz nie obejmuje wykorzystania hierarchii wielu Serwerów administracyjnych.

W sytuacjach, gdy instrukcje przeznaczone dla dostawcy usługi różnią się od instrukcji dla administratora, instrukcje dla dostawcy usługi są opisane oddzielnie.

Dokument opisuje również procedurę aktualizacji aplikacji z wersji 9.0 do 10.0.

Szczegółowe informacje dotyczące Kaspersky Security Center znajdziesz w *Przewodniku instalacji i Podręczniku administratora Kaspersky Security Center*.

W TEJ SEKCJI

W TYM DOKUMENCIE

Dokument *Rozpoczęcie pracy z Kaspersky Security Center* zawiera wprowadzenie, sekcje opisujące typowe zadania wykonywane przez Kaspersky Security Center oraz wnioski.

Źródła informacji o aplikacji (patrz strona 7)

Sekcja zawiera opis źródeł informacji o aplikacji i listę stron internetowych, na których możesz porozmawiać o programie.

Kaspersky Security Center (patrz strona 9)

Znajdują się tu informacje o przeznaczeniu programu Kaspersky Security Center, jego funkcjach i modułach.

Licencjonowanie aplikacji (patrz strona 10)

Ta sekcja zawiera informacje dotyczące ogólnych zasad związanych z aktywacją aplikacji. Należy zapoznać się z informacjami zawartymi w tej sekcji, aby dowiedzieć się więcej o przeznaczeniu umowy licencyjnej, typach licencji, sposobach aktywacji aplikacji i odnawianiu licencji.

Interfejs aplikacji (patrz strona 15)

Ta sekcja opisuje główne funkcje interfejsu Kaspersky Security Center.

Uruchamianie aplikacji (patrz strona 16)

Sekcja ta opisuje uruchamianie programu Kaspersky Security Center.

Wdrażanie systemu ochrony (patrz strona 17)

Ta sekcja opisuje możliwe scenariusze wdrażania systemu ochrony w sieci firmowej:

Wykonywanie podstawowych zadań (patrz strona 19)

Ta sekcja opisuje podstawowe działania, które można wykonać, korzystając z Kaspersky Security Center.

Aktualizowanie z Kaspersky Security Center 9.0 do Kaspersky Security Center 10.0

Ta sekcja opisuje procedurę aktualizacji programu Kaspersky Security Center 9.0 do Kaspersky Security Center 10.0, a także podstawowe działania, które należy wykonać podczas wstępnej konfiguracji aplikacji w nowej wersji.

Podsumowanie (patrz strona 33)

Ta sekcja podsumowuje informacje zawarte w dokumencie.

Kontakt z działem pomocy technicznej (patrz strona 34)

Sekcja zawiera informacje dotyczące sposobu kontaktu z pomocą techniczną.

Kaspersky Lab ZAO (patrz strona 36)

Sekcja zawiera informacje o firmie Kaspersky Lab ZAO.

Informacje o kodzie firm trzecich (patrz strona 37)

Z tej sekcji można się dowiedzieć o kodzie firm trzecich wykorzystanym w aplikacji Kaspersky Security Center.

Informacje o znakach towarowych (patrz strona 38)

Ta sekcja zawiera nazwy stanowiące zastrzeżone znaki towarowe.

OZNACZENIA STOSOWANE W DOKUMENCIE

W tekście znajdują się elementy znaczeniowe, na które należy zwrócić szczególną uwagę - ostrzeżenia, porady, przykłady.

Oznaczenia stosowane w dokumencie służą do wyróżnienia elementów znaczeniowych. Oznaczenia stosowane w dokumencie i przykłady ich użycia przedstawione zostały w poniższej tabeli.

Tabela 1. Oznaczenia stosowane w dokumencie

PRZYKŁADOWY TEKST	OPIS OZNACZENIA STOSOWANEGO W DOKUMENCIE
Pamiętaj, że...	Ostrzeżenia są wyróżnione kolorem czerwonym i znajdują się w ramkach. Ostrzeżenia zawierają informacje o prawdopodobnie niechcianych akcjach, które mogą prowadzić do utraty danych, błędów w działaniu sprzętu lub problemów z systemem operacyjnym.
Zalecamy korzystać z...	Uwagi znajdują się w ramkach. Uwagi mogą zawierać przydatne porady, zalecenia, szczególne wartości ustawień lub pewne ważne, nietypowe przypadki dotyczące działania aplikacji.
Przykład: ...	Przykłady znajdują się na żółtym tle pod nagłówkiem "Przykład".

PRZYKŁADOWY TEKST	OPIS OZNACZENIA STOSOWANEGO W DOKUMENCIE
Aktualizacja to... Występuje zdarzenie *Bazy danych są nieaktualne*.	Następujące elementy znaczeniowe 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 • Tekst wiadomości wyświetlanych na ekranie przez aplikację • Dane, które powinien wprowadzić użytkownik.
<Nazwa użytkownika>	Zmienne znajdują się w nawiasach ostrych. Zamiast zmiennej należy wpisywać odpowiadającą jej wartość, pomijając nawiasy.

ŹRÓDŁA INFORMACJI O APLIKACJI

Sekcja zawiera opis źródeł informacji o aplikacji i listę stron internetowych, na których możesz porozmawiać o programie.

Możesz wybrać dogodne źródło informacji w zależności od tego, jak pilne i ważne jest dane pytanie.

W TEJ SEKCJI

ŹRÓDŁA INFORMACJI O PRODUKCIE

Do wyszukania informacji dotyczących aplikacji możesz wykorzystać następujące źródła:

- strona aplikacji na witrynie internetowej firmy Kaspersky Lab;
- Baza wiedzy na stronie pomocy technicznej;
- pomoc elektroniczna;
- dokumentacja.

Jeśli nie potrafisz rozwiązać problemu samodzielnie, zalecamy skontaktować się z pomocą techniczną firmy Kaspersky Lab (sekcja "Pomoc techniczna za pośrednictwem telefonu" na stronie 34).

Aby skorzystać ze źródeł informacji dostępnych na witrynie Kaspersky Lab, konieczne jest nawiązanie połączenia z internetem.

Strona aplikacji na witrynie internetowej firmy Kaspersky Lab

Witryna Kaspersky Lab zawiera osobną stronę dla każdej aplikacji.

Na takiej stronie internetowej (www.kaspersky.pl/kaspersky_security_center) znajdziesz ogólne informacje o aplikacji, jej funkcjach i właściwościach.

Strona http://www.kaspersky.pl zawiera odnośnik do sklepu internetowego. Możesz w nim kupić lub odnowić licencję dla aplikacji.

Baza Wiedzy na stronie działu pomocy technicznej

Baza wiedzy jest oddzielną sekcją strony pomocy technicznej, która zawiera zalecenia dotyczące korzystania z aplikacji Kaspersky Lab. Baza wiedzy zawiera odnośniki do artykułów pogrupowane według tematów.

Na stronie internetowej aplikacji w Bazie wiedzy (http://support.kaspersky.com/pl/ksc10) możesz przeczytać artykuły zawierające przydatne informacje, zalecenia i odpowiedzi na najczęściej zadawane pytania dotyczące zakupu, instalacji i korzystania z aplikacji.

Artykuły mogą zawierać odpowiedzi na pytania spoza zakresu programu Kaspersky Security Center, związane z innymi aplikacjami Kaspersky Lab. Mogą zawierać również nowości z działu pomocy technicznej.

Pomoc elektroniczna

Pomoc elektroniczna aplikacji zawiera pliki pomocy.

Pomoc kontekstowa udostępnia informacje o każdym oknie aplikacji, wymienia i opisuje związane z nim ustawienia i listę zadań.

Pełna pomoc zawiera informacje o zarządzaniu ochroną komputera, konfigurowaniu aplikacji i rozwiązywaniu podstawowych problemów.

Dokumentacja

Pakiet dystrybucyjny aplikacji zawiera dokumentację, która pomoże Ci zainstalować i aktywować aplikację na komputerach w sieci LAN, skonfigurować jej ustawienia i odnaleźć informacje dotyczące podstawowych zasad korzystania z aplikacji.

FORUM INTERNETOWE FIRMY KASPERSKY LAB

Jeżeli zapytanie nie wymaga natychmiastowej odpowiedzi, można przedyskutować je ze specjalistami firmy Kaspersky Lab lub innymi użytkownikami jej oprogramowania na forum internetowym znajdującym się pod adresem http://forum.kaspersky.com.

Na tym forum możesz przeglądać istniejące tematy, pozostawiać swoje komentarze i tworzyć nowe tematy.

KONTAKT Z ZESPOŁEM TWORZĄCYM DOKUMENTACJĘ TECHNICZNĄ

Jeżeli masz jakiekolwiek pytania dotyczące tej dokumentacji, skontaktuj się z zespołem tworzącym dokumentację techniczną. Na przykład, jeśli chciałbyś wyrazić swoją opinię.

KASPERSKY SECURITY CENTER

Znajdują się tu informacje o przeznaczeniu programu Kaspersky Security Center, jego funkcjach i modułach.

Kaspersky Security Center służy do scentralizowanego wykonywania podstawowych zadań dotyczących administracji i zarządzania w sieci firmy. Aplikacja zapewnia administratorowi dostęp do szczegółowych informacji dotyczących poziomu ochrony sieci firmy; pozwala na skonfigurowanie wszystkich składników ochrony opartych o aplikacje Kaspersky Lab.

Kaspersky Security Center jest przeznaczony dla administratorów sieci firmowych oraz dla pracowników odpowiedzialnych za ochronę antywirusową organizacji.

Wersja SPE aplikacji jest przeznaczona dla dostawców SaaS (Software as Service - oprogramowanie jako usługa) (zwanych dalej *dostawcami usług*).

Korzystając z Kaspersky Security Center możesz:

- Utworzyć hierarchię Serwerów administracyjnych, aby zarządzać siecią firmy oraz sieciami odległych biur lub organizacji klienckich.

  Organizacja kliencka to organizacja, której ochrona antywirusowa jest zapewniana przez dostawcę usługi.
- Utworzyć hierarchię grup administracyjnych, aby zarządzać wyborem komputerów klienckich jako całością.
- Zarządzać systemem ochrony antywirusowej zbudowanym w oparciu o aplikacje Kaspersky Lab.
- Tworzyć obrazy systemów operacyjnych i instalować je na komputerach klienckich w sieci oraz wykonywać zdalną instalację aplikacji stworzonych przez Kaspersky Lab i innych dostawców oprogramowania.
- Zdalnie zarządzać aplikacjami stworzonymi przez Kaspersky Lab i innych dostawców oprogramowania zainstalowanymi na urządzeniach klienckich: instalować aktualizacje, wykrywać i naprawiać luki.
- Wykonywać scentralizowane rozsyłanie kluczy dla aplikacji Kaspersky Lab na komputery klienckie, monitorować ich wykorzystanie i odnawiać licencje.
- Otrzymywać statystyki i raporty dotyczące pracy aplikacji i urządzeń.
- Otrzymywać powiadomienia na temat zdarzeń krytycznych występujących w aplikacjach Kaspersky Lab.
- Kontrolować dostęp urządzeń do sieci firmy przy pomocy reguł ograniczania dostępu i białej listy urządzeń. Agenty NAC są wykorzystywane do zarządzania dostępem urządzeń do sieci organizacji.
- Zarządzać urządzeniami przenośnymi obsługującymi protokoły Exchange ActiveSync® lub iOS Mobile Device Management (iOS MDM).
- Zarządzać szyfrowaniem informacji przechowywanych na dyskach twardych urządzeń i nośników wymiennych oraz dostępem użytkowników do zaszyfrowanych danych.
- Wykonywać inwentaryzację sprzętu podłączonego do sieci firmy.
- Centralnie zarządzać plikami umieszczonymi w kwarantannie lub kopii zapasowej przez aplikacje antywirusowe, a także obiektami, których przetwarzanie zostało odłożone.

LICENCJONOWANIE APLIKACJI

Ta sekcja zawiera informacje dotyczące ogólnych zasad związanych z aktywacją aplikacji. Należy zapoznać się z informacjami zawartymi w tej sekcji, aby dowiedzieć się więcej o przeznaczeniu umowy licencyjnej, typach licencji, sposobach aktywacji aplikacji i odnawianiu licencji.

W TEJ SEKCJI

INFORMACJE O UMOWIE LICENCYJNEJ

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

Przed rozpoczęciem korzystania z aplikacji przeczytaj dokładnie warunki Umowy licencyjnej.

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

INFORMACJE O LICENCJI

Licencja to czasowo ograniczone prawo do korzystania z aplikacji, zgodne z Umową licencyjną. Licencja zawiera unikalny kod służący do aktywacji Twojej kopii Kaspersky Security Center.

Licencja nadaje Ci prawo do korzystania z następujących usług:

- Używania aplikacji na jednym lub kilku urządzeniach.

  Liczba urządzeń, na których możesz korzystać z aplikacji, jest określona w umowie licencyjnej.

- Pomocy technicznej Kaspersky Lab.
- Korzystania z innych usług świadczonych przez firmę Kaspersky Lab lub jej partnerów w trakcie okresu ważności licencji.

Zakres świadczonych usług oraz czas korzystania z aplikacji zależą od typu licencji użytej do aktywacji aplikacji.

Dostępne są następujące typy licencji:

- *Testowa* – jest to darmowa licencja udostępniana w celu zapoznania użytkowników z programem.

  Licencja testowa ma zazwyczaj krótki okres ważności. Jak tylko wygaśnie licencja testowa, Kaspersky Security Center kontynuuje działanie w trybie częściowo ograniczonej funkcjonalności.

- *Komercyjna* – płatna licencja oferowana podczas zakupu aplikacji. Dla Kaspersky Security Center dostępnych jest kilka opcji licencjonowania.

  Po wygaśnięciu licencji komercyjnej aplikacja nadal działa, ale w trybie częściowo ograniczonej funkcjonalności (sekcja "Informacje o ograniczeniach w podstawowej funkcjonalności" na stronie 12). Aby kontynuować

korzystanie z aplikacji Kaspersky Security Center w trybie pełnej funkcjonalności, musisz odnowić licencję komercyjną.

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

OPCJE LICENCJONOWANIA KASPERSKY SECURITY CENTER

W Kaspersky Security Center licencja może obejmować różne grupy funkcji.

Podstawowe funkcje Konsoli administracyjnej

Dostępne są następujące funkcje:

- Tworzenie wirtualnych Serwerów administracyjnych w celu zarządzania siecią zdalnych biur lub firm klienckich
- Tworzenie hierarchii grup administracyjnych w celu zarządzania wyborem urządzeń jako całością
- Kontrola stanu ochrony antywirusowej firmy
- Zdalna instalacja aplikacji
- Wyświetlanie listy obrazów systemów operacyjnych dostępnych do zdalnej instalacji
- Scentralizowana konfiguracja aplikacji zainstalowanych na komputerach klienckich
- Wyświetlanie i modyfikowanie istniejących grup licencjonowanych aplikacji
- Uzyskiwanie statystyk i raportów z działania aplikacji, a także powiadomień o krytycznych zdarzeniach
- Szyfrowanie danych i zarządzanie ochroną
- Wyświetlanie i ręczne modyfikowanie listy sprzętu wykrytego poprzez przeszukiwanie sieci
- Scentralizowane zarządzanie plikami przeniesionymi do Kwarantanny lub Kopii zapasowej oraz plikami, dla których odroczono przetwarzanie.

Aplikacja Kaspersky Security Center obsługująca podstawowe funkcje Konsoli administracyjnej jest dostępna wśród produktów Kaspersky Lab, zaprojektowanych do ochrony sieci firmowej. Można ją również pobrać ze strony firmy Kaspersky Lab (http://www.kaspersky.pl).

Jednostką zarządzającą dla podstawowych funkcji Konsoli jest wirtualny Serwer administracyjny. Można utworzyć do 10 wirtualnych Serwerów administracyjnych.

Przed aktywacją aplikacji lub po wygaśnięciu licencji komercyjnej Kaspersky Security Center działa w trybie podstawowej funkcjonalności Konsoli administracyjnej (sekcja "Informacje o ograniczeniach w podstawowej funkcjonalności" na stronie 12).

Funkcje programu Kaspersky Security Center, Service Provider Edition (zwany dalej SPE).

Funkcje wersji SPE aplikacji powielają podstawowe funkcje Konsoli administracyjnej, ale w tym przypadku można tworzyć więcej niż 10 wirtualnych Serwerów administracyjnych.

Wersja SPE jest rozpowszechniana wśród partnerów Kaspersky Lab na specjalnych warunkach. Więcej informacji o programie partnerskim można znaleźć na stronie Kaspersky Lab: http://www.kaspersky.pl/partners.html.

Funkcja Zarządzanie systemami

Dostępne są następujące funkcje:

- Zdalna instalacja systemów operacyjnych
- Zdalna instalacja uaktualnień oprogramowania, skanowanie i naprawianie luk
- Zarządzanie dostępem urządzeń do sieci firmy (Network Access Control, NAC)
- Inwentaryzacja sprzętu
- Zarządzanie grupami licencjonowanych aplikacji
- Zdalne podłączanie do komputerów klienckich

Jednostką zarządzająca dla funkcji Zarządzanie systemami jest komputer kliencki w grupie "Zarządzane komputery".

Funkcja Mobile Devices Management (zarządzania urządzeniami przenośnymi)

Funkcja Mobile Devices Management służy do zarządzania urządzeniami przenośnymi Exchange ActiveSync i iOS MDM.

Dla urządzeń przenośnych Exchange ActiveSync dostępne są następujące funkcje:

- Tworzenie i modyfikowanie profili zarządzania dla urządzeń przenośnych, przypisywania profili do skrzynek pocztowych użytkowników
- Konfiguracja urządzeń przenośnych (synchronizacja poczty, korzystanie z aplikacji, hasło użytkownika, szyfrowanie danych i podłączanie nośników wymiennych)
- Instalacja certyfikatów na urządzeniach przenośnych.

Dla urządzeń przenośnych iOS MDM dostępne są następujące funkcje:

- Tworzenie i modyfikowanie profili konfiguracji, instalacja profili konfiguracji na urządzeniach przenośnych
- Instalacja aplikacji na urządzeniu przenośnym za pośrednictwem App Store lub plików manifestu (.plist)
- Opcja blokowania urządzenia przenośnego, resetowania hasła urządzenia mobilnego oraz usuwania wszystkich danych z urządzenia przenośnego.

Funkcja Mobile Devices Management umożliwia również wykonywanie poleceń udostępnionych przez odpowiednie protokoły.

Jednostką zarządzającą funkcji Mobile Devices Management jest urządzenie przenośne. Urządzenie przenośne jest zarządzane od momentu podłączenia go do serwera urządzeń przenośnych.

INFORMACJE O OGRANICZENIACH W PODSTAWOWEJ FUNKCJONALNOŚCI

Przed aktywacją aplikacji lub po wygaśnięciu licencji komercyjnej Kaspersky Security Center działa w trybie podstawowej funkcjonalności Konsoli administracyjnej. Ograniczenia nałożone na działanie aplikacji w tym trybie zostały opisane poniżej.

Zarządzanie urządzeniami przenośnymi

Nie można utworzyć nowego profilu i przypisać go do urządzenia przenośnego (iOS MDM) lub skrzynki pocztowej (Exchange ActiveSync). Funkcje modyfikacji istniejących profili oraz przypisywania profili do skrzynek pocztowych są zawsze dostępne.

Zarządzanie aplikacjami

Nie można uruchomić zadania instalacji aktualizacji i zadania usuwania aktualizacji. Wszystkie zadania, które zostały uruchomione przed wygaśnięciem licencji, zostały zakończone, ale ostanie uaktualnienia nie zostały zainstalowane. Na przykład, jeśli zadanie instalacji krytycznych uaktualnień zostało uruchomione przed wygaśnięciem licencji, zainstalowane zostaną tylko krytyczne uaktualnienia, które zostały odnalezione przed wygaśnięciem licencji.

Funkcje uruchamiania i modyfikacji synchronizacji, wykrywania luk oraz zadania aktualizacji bazy luk są zawsze dostępne. Nie ma również żadnych ograniczeń wyświetlania, wyszukiwania i sortowania wpisów na liście luk i uaktualnień.

Zdalna instalacja systemów operacyjnych i aplikacji

Nie można uruchomić zadań instalacji i przechwytywania obrazu systemu operacyjnego. Zadania, które zostały uruchomione przed wygaśnięciem licencji, zostają zakończone.

Kontrola dostępu do sieci

Agent NAC oraz NAC przechodzą w tryb "Wyłączony" bez opcji ich włączenia.

Inwentaryzacja sprzętu

Nie można użyć informacji o nowych urządzeniach z NAC i serwerem urządzeń przenośnych. Aktualizowane są informacje o komputerach i podłączonych urządzeniach.

Nie otrzymasz powiadomienia o zmianach wprowadzonych w konfiguracjach urządzeń.

Lista sprzętu jest dostępna do przeglądania i modyfikowania.

Zarządzanie grupami licencjonowanych aplikacji

Nie można dodać nowego klucza.

Nie otrzymasz powiadomienia o naruszeniu ograniczeń dotyczących korzystania z klucza.

Zdalne podłączanie do komputerów klienckich

Zdalne podłączanie do komputerów klienckich nie jest dostępne.

Ochrona antywirusowa

Program antywirusowy używa baz danych zainstalowanych przed wygaśnięciem licencji.

INFORMACJE O KODZIE AKTYWACYJNYM

Kod aktywacyjny to kod, który otrzymasz po zakupie licencji komercyjnej dla Kaspersky Security Center. Kod aktywacyjny jest sekwencją dwudziestu cyfr i liter alfabetu łacińskiego w formacie xxxxx-xxxxx-xxxxx-xxxxx.

Aby aktywować aplikację przy pomocy kodu aktywacyjnego, należy połączyć się z serwerami aktywacji Kaspersky Lab przez internet. Jeśli nie ma połączenia z serwerami aktywacji, a dostęp do internetu jest możliwy, aktywacja aplikacji jest wykonywana przy użyciu pliku klucza (sekcja "Informacje o pliku klucza" na stronie 13)..

Okres ważności licencji rozpoczyna się od daty aktywacji aplikacji. Jeśli kupiłeś licencję umożliwiającą korzystanie z Kaspersky Security Center na kilku urządzeniach, okres ważności licencji będzie liczony od daty wprowadzenia kodu na pierwszym z tych urządzeń.

Jeśli utraciłeś lub przypadkowo usunąłeś kod aktywacyjny po aktywacji aplikacji, należy skontaktować się z pomocą techniczną Kaspersky Lab, aby go odzyskać.

INFORMACJE O PLIKU KLUCZA

Plik klucza to plik z nazwą w postaci xxxxxxxx.key.

Plik klucza jest używany do aktywacji aplikacji. Plik klucza zawiera wszystkie informacje wymagane do aktywacji; przy aktywacji przy pomocy pliku klucza nie musisz łączyć się z serwerami aktywacji ani nawiązywać połączenia internetowego.

W celu uzyskania pliku klucza lub odzyskania wcześniejszego pliku klucza po jego przypadkowym usunięciu, wyślij zgłoszenie do pomocy technicznej (sekcja "Kontakt z działem pomocy technicznej" na stronie 34).

Plik klucza zawiera następujące informacje:

- Klucz – unikalna sekwencja znaków alfanumerycznych. Klucza można użyć, na przykład, do uzyskania pomocy technicznej od firmy Kaspersky Lab.
- Ograniczenia w korzystaniu z aplikacji. Plik klucza Kaspersky Security Center może zawierać do trzech ograniczeń: liczba wirtualnych Serwerów administracyjnych, liczba zarządzanych komputerów i liczba zarządzanych urządzeń przenośnych. Typ ograniczenia jest określany przez bieżącą licencję (sekcja "Opcje licencjonowania Kaspersky Security Center" na stronie 11).
- Data utworzenia pliku klucza – data utworzenia pliku klucza na serwerze aktywacji.
- Okres ważności licencji to okres korzystania z aplikacji zastrzeżony przez umowę licencyjną i zliczany począwszy od dnia pierwszej aktywacji aplikacji przy pomocy danego pliku klucza (na przykład jeden rok).

  Okres ważności wygasa nie później, niż okres ważności pliku klucza, użytego do aktywacji aplikacji wykorzystującej tę licencję.

- Okres ważności pliku klucza – przedział czasu, który rozpoczyna się od dnia utworzenia pliku klucza. Aplikacja może zostać aktywowana przy użyciu pliku klucza tylko zanim zakończy się jego okres ważności.

Okres ważności pliku klucza wygasa automatycznie po wygaśnięciu licencji aplikacji aktywowanej przy pomocy tego pliku klucza.

INFORMACJE O PRZEKAZYWANIU DANYCH

Zaakceptowanie postanowień umowy licencyjnej wiąże się z wyrażeniem zgody na wysyłanie w trybie automatycznym informacji o sumach kontrolnych przetworzonych plików (MD5), informacji niezbędnych do określenia reputacji adresów internetowych, a także danych statystycznych dla ochrony antyspamowej. Zezwolisz również aplikacji na dostęp do komputerów klienckich zarządzanych przez Kaspersky Security Center w celu zbierania i przesyłania informacji o zainstalowanych narzędziach programowych i kodach zwrotnych generowanych w trakcie instalacji tych narzędzi programowych. Informacje przekazywane z komputerów klienckich zostaną wykorzystane do rozwiązywania problemów z oprogramowaniem lub do udoskonalenia funkcji oprogramowania.

Informacje te nie zawierają osobistych danych ani innych poufnych informacji. Firma Kaspersky Lab chroni uzyskane informacje zgodnie z wymogami ustanowionymi przez prawo. Więcej szczegółowych informacji o dostarczaniu danych można znaleźć na naszej stronie internetowej http://support.kaspersky.com/pl/ oraz w Oświadczeniu o gromadzeniu danych Kaspersky Security Network dostępnym w aplikacji.

INTERFEJS APLIKACJI

Ta sekcja opisuje główne funkcje interfejsu Kaspersky Security Center.

Przeglądanie, tworzenie, modyfikowanie i konfigurowanie grup administracyjnych, a także scentralizowane zarządzanie aplikacjami Kaspersky Lab zainstalowanymi na urządzeniach klienckich, wykonywane jest z poziomu stacji roboczej administratora. Interfejs zarządzania zapewniany jest przez Konsolę administracyjną. Jest to specjalne niezależne rozszerzenie zintegrowane z konsolą Microsoft Management Console (MMC); interfejs Kaspersky Security Center jest więc standardowy dla konsoli MMC. W celu uzyskania bardziej szczegółowych informacji zajrzyj do *Podręcznika administratora dla Kaspersky Security Center*.

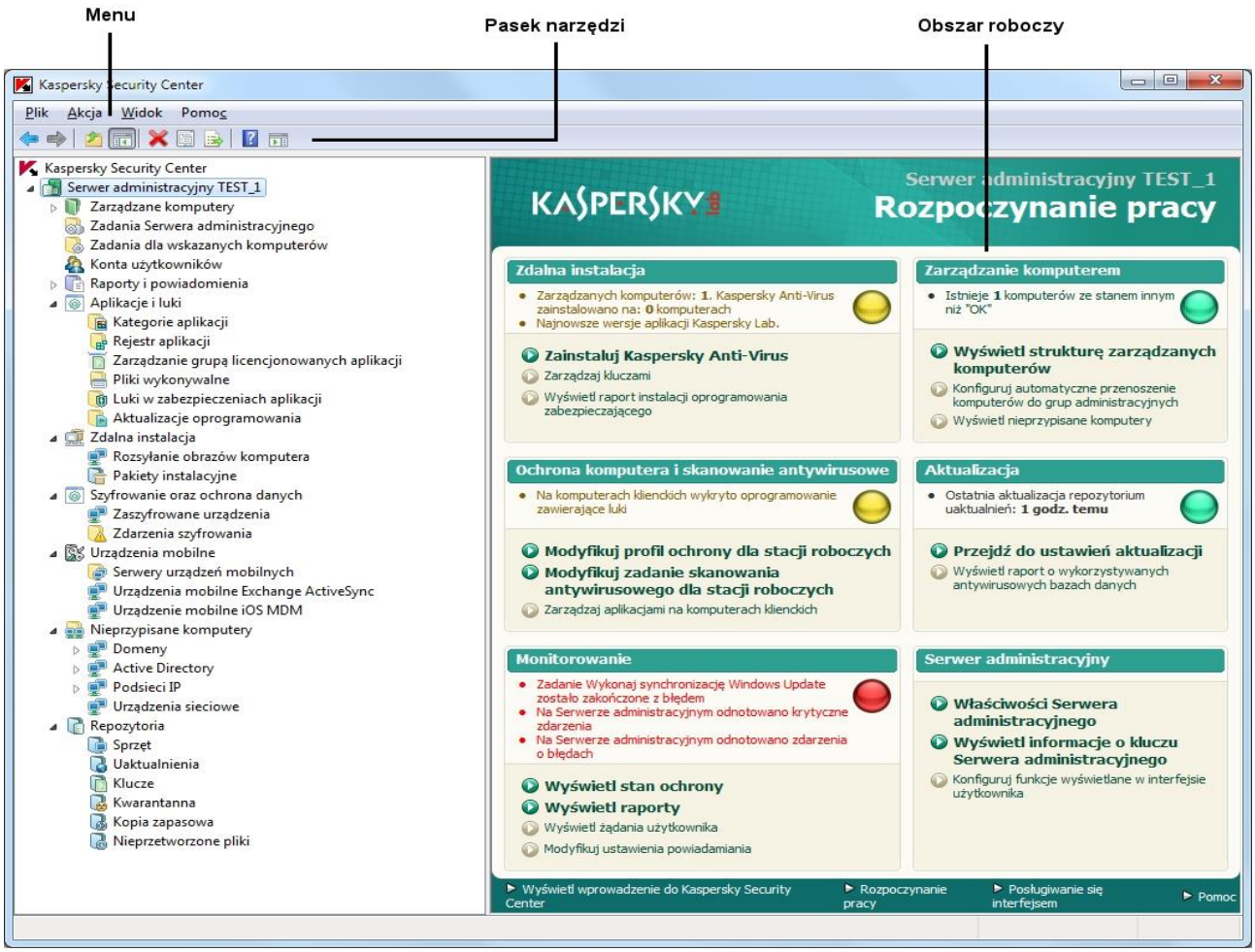
Okno główne aplikacji (zobacz rysunek poniżej) zawiera menu, pasek narzędzi, panel podglądu i obszar roboczy.

Pasek menu pozwala korzystać z okien i umożliwia dostęp do systemu pomocy. Podmenu **Akcja** duplikuje polecenia menu kontekstowego dla obiektu z drzewa konsoli.

Panel podglądu wyświetla przestrzeń nazw **Kaspersky Security Center** w postaci drzewa konsoli.

Zestaw przycisków paska narzędzi umożliwia bezpośredni dostęp do niektórych elementów menu. Zestaw przycisków dostępnych na pasku narzędzi zmienia się w zależności od bieżącego węzła lub foldera wybranego w drzewie konsoli.

Wygląd obszaru roboczego okna głównego zależy od tego, do którego węzła (foldera) drzewa konsoli obszar się odnosi i jakie funkcje pełni.



Rysunek 1. Okno główne aplikacji Kaspersky Security Center

URUCHAMIANIE APLIKACJI

Sekcja ta opisuje uruchamianie programu Kaspersky Security Center.

Program Kaspersky Security Center włącza się automatycznie podczas uruchamiania Serwera administracyjnego.

- *W celu uruchomienia Konsoli administracyjnej aplikacji:*

  wybierz **Kaspersky Security Center** z grupy programów **Kaspersky Security Center** ze standardowego menu **Start** → **Wszystkie programy**.

Grupa programów **Kaspersky Security Center** jest tworzona na stacjach roboczych administratorów w trakcie instalacji Konsoli administracyjnej.

WDRAŻANIE SYSTEMU OCHRONY

Ta sekcja opisuje dwa możliwe scenariusze wdrażania systemu ochrony w sieci firmowej:

- Wdrażanie systemu ochrony w obrębie firmy.
- Wdrażanie systemu ochrony w sieci firmowej klienta (podczas korzystania z wersji SPE).

Jeżeli musisz wdrożyć system ochrony w firmie posiadającej odległe biura, które nie znajdują się w sieci firmowej, możesz skorzystać ze scenariusza wdrażania ochrony antywirusowej dla dostawców usługi.

Szczegółowe informacje dotyczące działań zawartych w wyżej wymienionych scenariuszach wdrażania ochrony znajdziesz w sekcji "Wykonywanie podstawowych zadań" (patrz strona 19).

W TEJ SEKCJI

WDRAŻANIE OCHRONY ANTYWIRUSOWEJ W OBRĘBIE FIRMY

W celu wdrożenia systemu ochrony w sieci firmowej:

1. Zainstaluj i skonfiguruj Serwer administracyjny i Konsolę administracyjną (patrz sekcja "Instalowanie składników Kaspersky Security Center" na stronie 19).
2. Utwórz grupy administracyjne i dodaj do nich komputery klienckie (patrz sekcja "Tworzenie grup administracyjnych" na stronie 20).
3. Zainstaluj zdalnie Agenta sieciowego i wymagane aplikacje Kaspersky Lab na komputerach klienckich (patrz sekcja "Zdalne instalowanie aplikacji" na stronie 24).
4. W razie konieczności zaktualizuj bazy danych aplikacji Kaspersky Lab na komputerach klienckich (szczegółowe informacje znajdziesz w *Podręczniku administratora dla Kaspersky Security Center*).
5. Jeśli jest to konieczne, przeprowadź zaawansowaną konfigurację zainstalowanych aplikacji, korzystając z profili (patrz sekcja "Konfigurowanie profili aplikacji" na stronie 27) i lokalnych ustawień aplikacji (patrz sekcja "Przeglądanie i modyfikowanie lokalnych ustawień aplikacji" na stronie 27).
6. Dostosuj ustawienia powiadamiania administratora o zdarzeniach występujących na urządzeniach klienckich (patrz sekcja "Konfigurowanie powiadomień" na stronie 28).
7. Sprawdź działanie powiadamiania o zdarzeniach w trakcie działania ochrony systemu (patrz sekcja "Sprawdzanie pobranych uaktualnień" na stronie 26).
8. Wyświetl raporty (patrz sekcja "Tworzenie i przeglądanie raportu" na stronie 28) i skonfiguruj ich automatyczne dostarczanie za pośrednictwem poczty elektronicznej (patrz sekcja "Tworzenie zadania dostarczania raportów" na stronie 29).
9. Skonfiguruj automatyczną instalację oprogramowania na nowych komputerach w sieci (patrz sekcja "Konfigurowanie automatycznej instalacji aplikacji" na stronie 25).

Po wykonaniu opisanych czynności system ochrony antywirusowej zostanie wdrożony w sieci firmowej.

WDRAŻANIE SYSTEMU OCHRONY W SIECI FIRMOWEJ KLIENTA

W celu wdrożenia ochrony antywirusowej w sieci firmowej:

1. Zainstaluj Serwer administracyjny i Konsolę administracyjną na stacji roboczej administratora (patrz sekcja "Instalowanie składników Kaspersky Security Center" na stronie 19).
2. Zainstaluj Kaspersky Security Center Web-Console na stacji roboczej administratora (patrz sekcja "Instalowanie Kaspersky Security Center Web-Console" na stronie 21).
3. Skonfiguruj Serwer administracyjny do pracy z Kaspersky Security Center Web-Console (szczegółowe informacje znajdziesz w *Przewodniku instalacji dla Kaspersky Security Center*).
4. Utwórz i skonfiguruj wirtualny Serwer administracyjny zarządzający siecią firmową klienta (patrz sekcja "Tworzenie wirtualnego Serwera administracyjnego" na stronie 21).
5. Określ i skonfiguruj Agenta aktualizacji w sieci firmowej (patrz sekcja "Definiowanie Agenta aktualizacji. Konfigurowanie Agenta aktualizacji" na stronie 21).
6. Skonfiguruj pakiet instalacyjny Agenta sieciowego, który chcesz użyć do instalacji Agenta sieciowego na komputerach w sieci firmowej (patrz sekcja "Konfigurowanie pakietu instalacyjnego Agenta sieciowego" na stronie 22).
7. Zainstaluj zdalnie Agenta sieciowego i wymagane aplikacje Kaspersky Lab na komputerach klienckich (patrz sekcja "Zdalne instalowanie aplikacji" na stronie 24).
8. Jeśli jest to konieczne, przeprowadź zaawansowaną konfigurację zainstalowanych aplikacji, korzystając z profili (patrz sekcja "Konfigurowanie profili aplikacji" na stronie 27) i lokalnych ustawień aplikacji (patrz sekcja "Przeglądanie i modyfikowanie lokalnych ustawień aplikacji" na stronie 27).

Po wykonaniu opisanych czynności system ochrony antywirusowej zostanie wdrożony w sieci firmowej.

WYKONYWANIE PODSTAWOWYCH ZADAŃ

Ta sekcja opisuje podstawowe działania, które można wykonać, korzystając z Kaspersky Security Center.

W TEJ SEKCJI

INSTALOWANIE SKŁADNIKÓW KASPERSKY SECURITY CENTER

W celu zainstalowania Serwera administracyjnego i Konsoli administracyjnej:

1. Wybierz komputer, na którym zostanie zainstalowany Serwer administracyjny i Konsola administracyjna. Zalecamy instalację modułów na komputerze znajdującym się w domenie.

   Możesz zainstalować Konsolę administracyjną i Serwer administracyjny Kaspersky Security Center 10.0 na komputerze, na którym uruchomiona jest Konsola administracyjna i Serwer administracyjny w wersji 9.0.

   Zalecamy również przeprowadzenie instalacji, korzystając z praw administratora domeny. Umożliwi to automatyczne utworzenie grup użytkowników **KLAdmins** oraz **KLOperators** i zapewni niezbędne uprawnienia kontu, na którym będzie działał Serwer administracyjny.

2. Uruchom plik setup.exe i postępuj zgodnie z instrukcjami Kreatora Instalacji.
3. Wybierz typową instalację. Większość ustawień jest określona automatycznie.

Proces instalacji niestandardowej jest szczegółowo opisany w *Przewodniku instalacji dla Kaspersky Security Center*.

Zainstalowane zostaną także niezbędne aplikacje (jeżeli nie zostały wcześniej zainstalowane):

- Microsoft Windows Installer 3.1;
- Microsoft Data Access Components (MDAC) 2.8;
- Microsoft .NET Framework 2.0;
- Microsoft SQL Server® 2008 R2 Express Edition.

Aplikacje te nie wymagają obsługi i administracji przez użytkownika.

W następnym kroku kreatora pliki aplikacji zostaną skopiowane na komputer i utworzona zostanie baza danych na Serwerze administracyjnym, który będzie przechowywał informacje o ochronie antywirusowej firmy.

Po zakończeniu pracy Kreatora możesz uruchomić Konsolę administracyjną i przeprowadzić wstępną konfigurację przy pomocy Kreatora automatycznej konfiguracji.

TWORZENIE GRUP ADMINISTRACYJNYCH

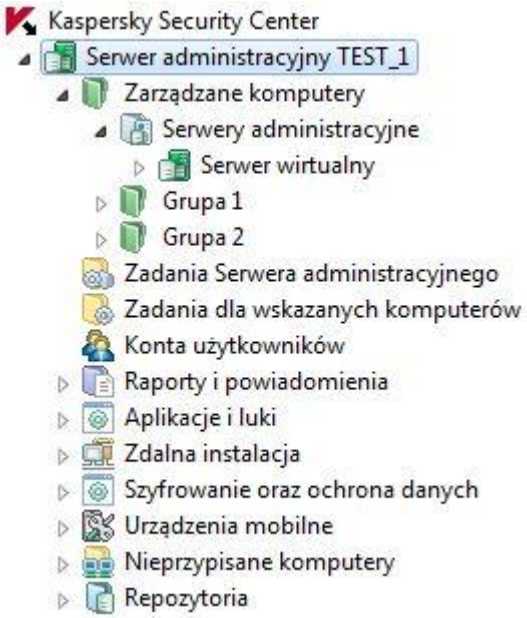
Hierarchia grup informacyjnych jest tworzona w oknie głównym aplikacji Kaspersky Security Center, w folderze **Zarządzane komputery**. Grupy administracyjne są wyświetlane w drzewie konsoli jako foldery (zobacz rysunek poniżej).

Po zainstalowaniu Kaspersky Security Center folder **Zarządzane komputery** zawiera jedynie pusty folder **Serwery administracyjne**.

Ustawienia interfejsu użytkownika określają, czy folder **Serwery administracyjne** jest wyświetlany w drzewie konsoli. Aby sekcja ta była wyświetlana, przejdź na zakładkę **Widok Konfiguracja interfejsu** i w otwartym oknie **Konfiguracja interfejsu** zaznacz pole **Wyświetlaj podrzędne Serwery administracyjne**.

Przy tworzeniu hierarchii grup administracyjnych możesz dodać komputery klienckie i maszyny wirtualne do foldera **Zarządzane komputery**, a także możesz dodać zagnieżdżone grupy. Możesz dodać podrzędne Serwery administracyjne do foldera **Serwery administracyjne**.

Tak jak w grupie **Zarządzane komputery** każda utworzona grupa początkowo zawiera tylko pusty folder **Serwery administracyjne**, który służy do obsługi podrzędnych Serwerów administracyjnych tej grupy. Informacje o profilach, zadaniach tej grupy i komputerach klienckich znajdujących się w niej, wyświetlane są w odpowiednich zakładkach obszaru roboczego tej grupy.



Rysunek 2. Wyświetlanie hierarchii grup administracyjnych

- *W celu utworzenia grupy administracyjnej:*

  1. W drzewie konsoli otwórz folder **Zarządzane komputery**.
  2. Jeśli chcesz utworzyć podgrupę dla istniejącej grupy administracyjnej, w folderze **Zarządzane komputery** wybierz zagnieżdżony folder odpowiadający grupie, do której chcesz dodać nową grupę administracyjną.

     Jeśli tworzysz nową grupę administracyjną na najwyższym poziomie hierarchii, możesz pominąć ten krok.
  3. Uruchom proces tworzenia grupy administracyjnej w jeden z następujących sposobów:
     - Przy pomocy polecenia **Nowa** → **Grupa** z menu kontekstowego
     - Klikając odnośnik **Utwórz podgrupę**, znajdujący się w obszarze roboczym okna głównego aplikacji, na zakładce **Grupy**.
  4. W oknie **Nazwa grupy**, które zostanie otwarte, wprowadź nazwę grupy i kliknij przycisk **OK**.

  W rezultacie w drzewie konsoli pojawi się nowy folder grupy administracyjnej o określonej nazwie.

INSTALOWANIE KASPERSKY SECURITY CENTER WEB-CONSOLE

- *W celu zainstalowania Kaspersky Security Center Web-Console na stacji roboczej administratora:*

  uruchom plik setup.exe znajdujący się w pakiecie dystrybucyjnym Kaspersky Security Center Web-Console.

Zostanie uruchomiony Kreator instalacji Kaspersky Security Center Web-Console, który poprowadzi Cię przez instalację konsoli. Postępuj zgodnie z jego poleceniami.

TWORZENIE WIRTUALNEGO SERWERA ADMINISTRACYJNEGO

- *W celu dodania wirtualnego Serwera administracyjnego do wybranej grupy administracyjnej:*

  1. W drzewie konsoli, w folderze grupy administracyjnej wybierz węzeł **Serwery administracyjne**.
  2. Uruchom proces tworzenia wirtualnego Serwera administracyjnego na jeden z następujących sposobów:
     - z menu kontekstowego węzła **Serwery administracyjne** wybierz **Nowy** → **Wirtualny Serwer administracyjny**.
     - kliknij odnośnik **Dodaj wirtualny Serwer administracyjny** dostępny w obszarze roboczym.

  Zostanie uruchomiony Kreator nowego wirtualnego Serwera administracyjnego. Postępuj zgodnie z jego poleceniami.

DEFINIOWANIE AGENTA AKTUALIZACJI

KONFIGUROWANIE AGENTA AKTUALIZACJI

- *W celu wyznaczenia komputera w sieci firmowej organizacji klienckiej na Agenta aktualizacji:*

  1. Utwórz autonomiczny pakiet dla Agenta sieciowego. Wykonaj następujące czynności:
     a. W drzewie konsoli wybierz wirtualny Serwer administracyjny, zarządzający siecią firmową organizacji klienckiej.
     b. W folderze **Zdalna instalacja** wirtualnego Serwera administracyjnego wybierz podfolder **Pakiety instalacyjne**.
     c. W obszarze roboczym foldera wybierz lub utwórz pakiet instalacyjny Agenta sieciowego.
     d. Otwórz okno właściwości pakietu instalacyjnego Agenta sieciowego.

e. W sekcji **Połączenie**, w polu **Adres serwera** sprawdź adres wirtualnego Serwera administracyjnego. Adres musi być podany w następującym formacie: `<Adres głównego Serwera administracyjnego>/<Nazwa wirtualnego Serwera administracyjnego>`.

f. Uruchom proces tworzenia autonomicznego pakietu dla tego pakietu instalacyjnego, korzystając z jednej z następujących metod:

- Wybierz **Utwórz autonomiczny pakiet instalacyjny** z menu kontekstowego pakietu instalacyjnego
- Kliknij odnośnik **Utwórz autonomiczny pakiet instalacyjny** w sekcji służącej do zarządzania wybranym pakietem instalacyjnym.

g. Otwórz listę utworzonych autonomicznych pakietów instalacyjnych Agenta sieciowego, korzystając z jednej z następujących metod:

- W ostatnim oknie Kreatora tworzenia autonomicznego pakietu instalacyjnego zaznacz pole **Otwórz listę pakietów instalacyjnych**
- Z menu kontekstowego pakietu instalacyjnego wybierz **Wyświetl listę autonomicznych pakietów**.

h. Na otwartej liście autonomicznych pakietów wybierz utworzony autonomiczny pakiet i określ sposób, w jaki ma on zostać dostarczony administratorowi firmy klienckiej.

2. Skontaktuj się z administratorem firmy klienckiej, aby zainstalować Agenta sieciowego lokalnie na komputerze klienckim wyznaczonym jako Agent aktualizacji.

   Po zainstalowaniu Agenta sieciowego na komputerze klienckim wyznaczonym jako Agent aktualizacji, komputer ten jest wyświetlany w folderze **Zarządzane komputery** wirtualnego Serwera administracyjnego.

   Kaspersky Security Center wyznaczy ten komputer jako Agenta aktualizacji i skonfiguruje go jako bramę połączenia przy pierwszym połączeniu z Serwerem administracyjnym.

   Jeśli chcesz ręcznie wyznaczyć komputer jako Agenta aktualizacji:

   a. Otwórz okno właściwości foldera **Zarządzane komputery** wirtualnego Serwera administracyjnego.

   b. W sekcji **Agenty aktualizacji** wybierz komputer kliencki, który będzie Agentem aktualizacji, klikając przycisk **Dodaj**.

   c. Otwórz okno właściwości Agenta sieciowego i wykonaj następujące czynności:

   - Skonfiguruj przeszukiwanie sieci przez Agenta aktualizacji w sekcji **Wykrywanie sieci**.
   - Wybierz sekcję **Zaawansowane** i zaznacz pole **Brama połączenia**, które włącza korzystanie z Agenta aktualizacji jako bramy połączenia w sieci firmy klienckiej.

W rezultacie, wybrany komputer kliencki stanie się Agentem aktualizacji dla firmy klienckiej i będzie wykorzystywany w tej firmie jako brama połączenia przy łączeniu z wirtualnym Serwerem administracyjnym.

Możesz przypisać komputerowi zadanie Agenta aktualizacji ręcznie tylko wtedy, gdy automatyczne przypisywanie jest wyłączone (sekcja **Ustawienia** okna właściwości wirtualnego Serwera administracyjnego).

KONFIGUROWANIE PAKIETU INSTALACYJNEGO AGENTA SIECIOWEGO

Przed instalacją Agenta sieciowego na komputerach w firmie klienckiej należy skonfigurować pakiet instalacyjny Agenta sieciowego, który zostanie wykorzystany do zdalnej instalacji.

➧ *W celu skonfigurowania pakietu instalacyjnego Agenta sieciowego przed jego instalacją na komputerach firmy klienckiej:*

1. W drzewie konsoli wybierz wirtualny Serwer administracyjny, zarządzający siecią firmową organizacji klienckiej.
2. W folderze **Zdalna instalacja** wirtualnego Serwera administracyjnego wybierz podfolder **Pakiety instalacyjne**.
3. W obszarze roboczym wybierz lub utwórz pakiet instalacyjny Agenta sieciowego, który zostanie użyty do instalacji Agenta sieciowego na komputerach firmy klienckiej.
4. Z menu kontekstowego pakietu instalacyjnego Agenta sieciowego wybierz **Właściwości**.

   Zostanie otwarte okno właściwości pakietu instalacyjnego Agenta sieciowego.

5. W oknie właściwości dostosuj następujące ustawienia pakietu instalacyjnego:

- W sekcji **Połączenie**, w wierszu **Adres serwera** określ adres tego samego wirtualnego Serwera administracyjnego, który określono w Agencie aktualizacji podczas lokalnej instalacji Agenta sieciowego (sekcja "Definiowanie Agenta aktualizacji. Konfigurowanie Agenta aktualizacji" na stronie 21).
- W sekcji **Zaawansowane** zaznacz pole **Połącz z Serwerem administracyjnym przy użyciu bramy połączenia**. W wierszu **Adres bramy połączenia** określ adres Agenta aktualizacji. Można użyć adresu IP lub nazwy komputera w sieci Windows.

6. Kliknij **OK**.

ZARZĄDZANIE URZĄDZENIAMI PRZENOŚNYMI

Kaspersky Security Center umożliwia zarządzanie urządzeniami przenośnymi obsługującymi protokoły Exchange ActiveSync i iOS Mobile Device Management (iOS MDM).

Opcja gromadzenia informacji o urządzeniach przenośnych i przechowywania ich profili jest udostępniana przez serwery urządzeń przenośnych. *Serwer urządzeń przenośnych* jest to składnik Kaspersky Security Center umożliwiający administratorowi dostęp do urządzeń przenośnych i zarządzanie nimi za pośrednictwem Konsoli administracyjnej.

Istnieją dwa typy serwerów urządzeń przenośnych:

- Serwer urządzeń przenośnych obsługujący Exchange ActiveSync. Serwer jest instalowany na komputerze klienckim, na którym zainstalowano serwer Microsoft Exchange. Umożliwia on pobieranie danych z serwera Microsoft Exchange i przesyłanie ich do Serwera administracyjnego. Ten serwer urządzeń przenośnych jest używany do zarządzania urządzeniami mobilnymi, które obsługują protokół Exchange ActiveSync.
- Serwer urządzeń przenośnych iOS MDM. Jest on zainstalowany na komputerze klienckim i umożliwia połączanie urządzeń przenośnych z systemem iOS z Serwerem administracyjnym oraz zarządzanie urządzeniami przenośnymi z iOS za pośrednictwem usługi Apple Push Notifications (APNs).

Dla urządzeń przenośnych Exchange ActiveSync dostępne są następujące funkcje:

- Tworzenie i modyfikowanie profili zarządzania dla urządzeń przenośnych, przypisywania profili do skrzynek pocztowych użytkowników
- Konfiguracja urządzeń przenośnych (synchronizacja poczty, korzystanie z aplikacji, hasło użytkownika, szyfrowanie danych i podłączanie nośników wymiennych)
- Instalacja certyfikatów na urządzeniach przenośnych.

Dla urządzeń przenośnych iOS MDM dostępne są następujące funkcje:

- Tworzenie i modyfikowanie profili konfiguracji, instalacja profili konfiguracji na urządzeniach przenośnych
- Instalacja aplikacji na urządzeniu przenośnym za pośrednictwem App Store lub plików manifestu (.plist)
- Opcja blokowania urządzenia przenośnego, resetowania hasła urządzenia mobilnego oraz usuwania wszystkich danych z urządzenia przenośnego.

Szczegółowe informacje o sposobach zarządzania urządzeniami przenośnymi znajdziesz w *Podręczniku administratora dla Kaspersky Security Center*.

W poniższej części dostępny jest krótki opis działań, jakie należy wykonać, aby podłączyć urządzenia przenośne obsługujące protokoły Exchange ActiveSync i iOS MDM do Serwera administracyjnego.

PODŁĄCZANIE URZĄDZEŃ PRZENOŚNYCH OBSŁUGUJĄCYCH EXCHANGE ACTIVESYNC

W celu połączenia urządzeń przenośnych obsługujących Exchange ActiveSync z Serwerem administracyjnym:

1. Na komputerze klienckim z zainstalowanym serwerem Microsoft Exchange zainstaluj serwer urządzeń przenośnych Exchange ActiveSync.
2. Utwórz profile zarządzające dla urządzeń przenośnych Exchange ActiveSync.
3. Przypisz profile zarządzające urządzeniami przenośnymi Exchange ActiveSync do skrzynek pocztowych użytkowników.

   Użytkownika urządzenia przenośnego podłącza urządzenie przenośne do serwera Microsoft Exchange i otrzymuje powiadomienie informujące, że skrzynka pocztowa użytkownika jest zarządzana przez profil, który nakłada ograniczenia na podłączane urządzenie. Szczegółowe informacje o działaniach, jakie może wykonać

użytkownik urządzenia przenośnego Exchange ActiveSync, znajdują się w *Przewodniku instalacji dla Kaspersky Endpoint Security 10 for Mobile Devices*.

Urządzenie przenośne podłączone do serwera Microsoft Exchange jest wyświetlane w podfolderze **Urządzenia przenośne Exchange ActiveSync**, znajdującym się w folderze **Urządzenia przenośne**.

Szczegółowe informacje o sposobach połączenia urządzeń przenośnych Exchange ActiveSync z Serwerem administracyjnym znajdziesz w *Przewodniku instalacji dla Kaspersky Security Center*.

Administrator może zarządzać urządzeniami przenośnymi Exchange ActiveSync połączonymi z Serwerem administracyjnym. Szczegółowe informacje o sposobach zarządzania urządzeniami przenośnymi Exchange ActiveSync znajdziesz w Podręczniku administratora dla Kaspersky Security Center.

PODŁĄCZANIE URZĄDZEŃ PRZENOŚNYCH IOS MDM

- *W celu połączenia urządzeń przenośnych iOS MDM z Serwerem administracyjnym:*

1. Administrator instaluje na wybranym komputerze klienckim serwer urządzeń przenośnych iOS MDM, domyślnie znajdujący się w pakietach instalacyjnych Serwera administracyjnego.
2. Zainstaluj na Serwerze administracyjnym certyfikat Apple Push Notification Service (APNs).
3. Skonfiguruj połączenia urządzeń przenośnych z serwerem urządzeń przenośnych iOS MDM.
4. Wyślij do użytkowników urządzeń przenośnych iOS odnośnik do pobrania profilu iOS MDM.

   Użytkownicy urządzeń przenośnych otrzymują powiadomienie zawierające odnośnik do pobrania profilu iOS MDM z portalu internetowego, po czym instalują na swoich urządzeniach przenośnych profil iOS MDM.

Urządzenia przenośne nawiązują połączenie z serwerem urządzeń przenośnych iOS MDM. Połączone urządzenia przenośne iOS MDM są wyświetlane w folderze **Urządzenia przenośne iOS MDM**, znajdującym się w folderze **Urządzenia przenośne**.

Szczegółowe informacje o sposobach połączenia urządzeń przenośnych iOS MDM z Serwerem administracyjnym znajdziesz w *Przewodniku instalacji dla Kaspersky Security Center*.

Po połączeniu urządzenia przenośnego iOS MDM z Serwerem administracyjnym, na urządzeniu przenośnym iOS MDM możesz zainstalować profil konfiguracji i profil zabezpieczeń. Szczegółowe informacje dotyczące sposobu instalacji profilu konfiguracji i profilu zabezpieczeń znajdziesz w *Przewodniku instalacji dla Kaspersky Security Center*.

Administrator może zarządzać urządzeniami przenośnymi iOS MDM połączonymi z Serwerem administracyjnym. Szczegółowe informacje dotyczące sposobu zarządzania urządzeniami przenośnymi iOS MDM znajdziesz w *Podręczniku administratora dla Kaspersky Security Center*.

ZDALNE INSTALOWANIE APLIKACJI

Pewne aplikacje firmy Kaspersky Lab obsługujące zarządzanie przez Kaspersky Security Center mogą zostać zainstalowane na urządzeniach klienckich wyłącznie lokalnie (szczegółowe informacje na ten temat znajdują się w podręcznikach dla konkretnych aplikacji Kaspersky Lab).

- *W celu zdalnego zainstalowania aplikacji na komputerach klienckich:*

1. W drzewie konsoli wybierz węzeł Serwera administracyjnego, który zarządza urządzeniami klienckimi.
2. W folderze **Instalacja zdalna**, dostępnym w drzewie konsoli, kliknij odnośnik **Uruchom Kreator instalacji zdalnej** w celu uruchomienia Kreatora instalacji zdalnej.
3. W oknie **Wybierz pakiet instalacyjny** wskaż pakiet instalacyjny aplikacji, którą chcesz zainstalować.
4. Postępuj zgodnie z jego poleceniami.

Działania Kreatora spowodują utworzenie zadania instalacji zdalnej odpowiedzialnego za instalację aplikacji na komputerach klienckich. Kreator zdalnej instalacji tworzy i uruchamia zadanie zdalnej instalacji wybranej aplikacji. W zależności od wybranego urządzenia lub grupy administracyjnej, utworzone zadanie jest umieszczone w folderze **Zadania dla wskazanych komputerów** lub w obszarze roboczym wybranej grupy administracyjnej, na zakładce **Zadania**.

Po zakończeniu wykonywania utworzonego zadania aplikacja jest instalowana na wybranych urządzeniach klienckich.

Możesz skorzystać z wyżej opisanej procedury w celu zainstalowania aplikacji antywirusowej na urządzeniach klienckich. Jeśli potrzebujesz informacji dotyczących instalacji aplikacji antywirusowej na komputerach klienckich grupy

administracyjnej, przejdź na zakładkę **Komputery** w obszarze roboczym grupy. Informacje o instalacji aplikacji na komputerach klienckich można przeglądać w obszarze roboczym, w folderze **Nieprzypisane komputery**. Na liście komputerów dostępnej na zakładce **Komputery**, w obszarze roboczym folderu **Nieprzypisane komputery**, w kolumnie **Agent/Antywirus** można zobaczyć, czy na komputerach zainstalowano Agenta sieciowego i aplikację antywirusową. Jeżeli po lewym ukośniku występuje znak "+", oznacza to, że aplikacja antywirusowa została zainstalowana pomyślnie.

KONFIGUROWANIE AUTOMATYCZNEJ INSTALACJI APLIKACJI

W celu skonfigurowania automatycznej instalacji aplikacji na urządzeniach w grupie administracyjnej:

1. W drzewie konsoli wybierz żądaną grupę administracyjną.
2. Otwórz okno właściwości tej grupy administracyjnej.
3. W sekcji **Automatyczna instalacja** wybierz pakiety instalacyjne instalowane na nowych komputerach, zaznaczając pola obok nazw pakietów instalacyjnych wymaganych aplikacji. Kliknij **OK**.

Zostaną utworzone zadania grupowe, które zostaną uruchomione na urządzeniach klienckich natychmiast po dodaniu ich do grupy administracyjnej.

W przypadku, gdy do automatycznej instalacji wybrano tylko niektóre pakiety instalacyjne danej aplikacji, zadanie instalacji zostanie utworzone tylko dla najnowszej wersji aplikacji.

TWORZENIE ZADANIA POBIERANIA UAKTUALNIEŃ DO REPOZYTORIUM

Zadanie Pobierz uaktualnienia do repozytorium jest automatycznie tworzone podczas działania Kreatora automatycznej konfiguracji Kaspersky Security Center. Możesz utworzyć tylko jedno zadanie pobierania uaktualnień do repozytorium. Dlatego też zadanie pobierania uaktualnień do repozytorium możesz utworzyć tylko wtedy, gdy takie zadanie zostało usunięte z listy zadań Serwera administracyjnego.

W celu utworzenia zadania pobierania uaktualnień do repozytorium:

1. Z drzewa konsoli wybierz folder **Zadania Serwera administracyjnego**.
2. Uruchom tworzenie zadania w jeden z następujących sposobów:
   - W drzewie konsoli, z menu kontekstowego foldera **Zadania Serwera administracyjnego** wybierz **Nowy** → **Zadanie**.
   - Kliknij odnośnik **Utwórz zadanie** dostępny w obszarze roboczym.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z jego poleceniami. W oknie **Typ zadania** wybierz **Pobierz uaktualnienia do repozytorium**.

Po zakończeniu działania kreatora zadanie **Pobierz uaktualnienia do repozytorium** zostanie utworzone na liście zadań Serwera administracyjnego.

Podczas wykonywania zadania **Pobierz uaktualnienia do repozytorium** Serwer administracyjny pobiera uaktualnienia baz danych i modułów programu ze źródła uaktualnień i przechowuje je w folderze współdzielonym.

Uaktualnienia są rozsyłane do komputerów klienckich i podrzędnych Serwerów administracyjnych z foldera współdzielonego.

Jako źródła uaktualnień dla Serwera administracyjnego można użyć następujących zasobów:

- Serwery aktualizacji Kaspersky Lab – serwery firmy Kaspersky Lab, na których umieszczane są aktualizacje antywirusowych baz danych oraz modułów aplikacji.
- Nadrzędnego Serwera administracyjnego.
- Serwer FTP / HTTP, folder lokalny lub sieciowy – serwer FTP lub HTTP, folder lokalny lub sieciowy dodany przez użytkownika i zawierający najnowsze uaktualnienia. Podczas wyboru folderu lokalnego powinieneś określić folder na komputerze z zainstalowanym Serwerem administracyjnym.

Aby zaktualizować Serwer administracyjny z serwera FTP / HTP lub folderu sieciowego, powinieneś skopiować do tego zasobu poprawną strukturę folderów z uaktualnieniami, identyczną do tej utworzonej podczas korzystania z serwerów aktualizacji Kaspersky Lab.

Wybór źródła jest uzależniony od ustawień zadania. Domyślnie uaktualnienia są pobierane z serwerów aktualizacji firmy Kaspersky Lab.

SPRAWDZANIE POBRANYCH UAKTUALNIEŃ

W celu skonfigurowania Kaspersky Security Center do sprawdzania pobranych uaktualnień przed rozesłaniem ich na komputery klienckie:

1. W obszarze roboczym foldera **Zadania Serwera administracyjnego**, z listy zadań wybierz zadanie **Pobierz uaktualnienia do repozytorium**.
2. Otwórz okno właściwości zadania w jeden z następujących sposobów:
   - Z menu kontekstowego zadania wybierz **Właściwości**.
   - Kliknij odnośnik **Zmień ustawienia zadania** w obszarze roboczym wybranego zadania.
3. W otwartym oknie właściwości zadania, w sekcji **Weryfikacja uaktualnień** zaznacz pole **Zweryfikuj uaktualnienia przed rozesłaniem** i wybierz zadanie weryfikacji uaktualnień na jeden z następujących sposobów:
   - Kliknij **Wybierz**, aby wybrać istniejące zadanie weryfikacji uaktualnień.
   - Kliknij przycisk **Utwórz**, aby utworzyć zadanie weryfikacji uaktualnień.

     Zostanie uruchomiony Kreator zadania weryfikacji uaktualnień. Postępuj zgodnie z jego poleceniami.

     Przy tworzeniu zadania weryfikacji uaktualnień należy wybrać grupę administracyjną, która zawiera komputery, na których zadanie zostanie uruchomione. Komputery z tej grupy są zwane *komputerami testowymi*.

     Zaleca się wykorzystywać komputery z najbardziej niezawodną ochroną i najpowszechniejszą konfiguracją aplikacji w całej sieci firmowej. Poprawi to jakość skanowań, zminimalizuje ryzyko fałszywych alarmów oraz prawdopodobieństwo wykrycia wirusa podczas skanowania. Jeśli na komputerach testujących zostaną wykryte wirusy, zadanie testowania aktualizacji zakończy się niepowodzeniem.
4. Kliknij **OK**, aby zamknąć okno właściwości zadania pobierania uaktualnień do repozytorium.

W rezultacie zadanie weryfikacji uaktualnień będzie wykonywane wraz z zadaniem pobierania uaktualnień do repozytorium. Serwer administracyjny pobierze uaktualnienia ze źródła, zapisze je w folderze tymczasowym i uruchomi zadanie testowania uaktualnień. Jeżeli zadanie zakończy się powodzeniem, uaktualnienia zostaną skopiowane z folderu tymczasowego do folderu współdzielonego na Serwerze administracyjnym (<folder instalacyjny Kaspersky Security Center>\Share\Updates) i rozesłane do wszystkich komputerów klienckich, dla których Serwer administracyjny jest źródłem uaktualnień.

Jeżeli zadanie weryfikacji uaktualnień wykaże niepoprawność uaktualnień znajdujących się w folderze tymczasowym lub podczas wykonywania tego zadania wystąpi błąd, uaktualnienia nie zostaną skopiowane do foldera współdzielonego, a Serwer administracyjny zachowa poprzednią wersję uaktualnień. Zaplanowane zadania wykonywane zgodnie z opcją terminarza **Po pobraniu nowych uaktualnień do repozytorium** również nie zostaną uruchomione. Te działania zostaną wykonane podczas następnego zadania pobierania uaktualnień Serwera administracyjnego pod warunkiem, że testowanie nowych uaktualnień przebiegło bez problemów.

Zestaw uaktualnień jest uważany za nieprawidłowy, jeżeli przynajmniej na jednym komputerze testowym jest spełniony jeden z następujących warunków:

- Wystąpił błąd zadania aktualizacji
- Stan ochrony w czasie rzeczywistym aplikacji antywirusowej uległ zmianie po zastosowaniu uaktualnień
- W trakcie uruchamiania zadania skanowania wykryto zainfekowany obiekt
- Wystąpił błąd w funkcjonowaniu programu firmy Kaspersky Lab

Jeśli żaden z powyższych warunków nie wystąpił na żadnym komputerze, zestaw uaktualnień jest uważany za poprawny, a zadanie weryfikowania uaktualnień zostaje zakończone pomyślnie.

AUTOMATYCZNE ROZSYŁANIE UAKTUALNIEŃ DO KOMPUTERÓW KLIENCKICH

W celu rozesłania uaktualnień wybranych aplikacji do komputerów klienckich natychmiast po ich pobraniu do repozytorium Serwera administracyjnego:

1. Nawiąż połączenie z Serwerem administracyjnym, który zarządza komputerami klienckimi.
2. Utwórz zadanie rozsyłania uaktualnień dla wybranych komputerów klienckich w jeden z następujących sposobów:
   - Jeśli chcesz rozesłać uaktualnienia do komputerów klienckich należących do wybranej grupy administracyjnej, utwórz zadanie dla wybranej grupy.
   - Jeżeli chcesz rozesłać uaktualnienia do komputerów klienckich należących do różnych grup administracyjnych lub nie będących w żadnej grupie administracyjnej, utwórz zadanie dla wskazanych komputerów.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z jego instrukcjami i wykonaj następujące czynności:

   a. W oknie **Typ zadania**, w węźle żądanej aplikacji wybierz zadanie rozsyłania uaktualnień.

   Nazwa zadania rozsyłania uaktualnień wyświetlana w oknie **Typ zadania** zależy od aplikacji, dla której utworzyłeś to zadanie. Szczegółowe informacje o nazwach zadań aktualizacji dla wybranej aplikacji Kaspersky Lab znajdziesz w odpowiednich podręcznikach użytkownika.

   b. W oknie kreatora **Terminarz** , w polu **Zaplanowane uruchomienie** wybierz **Po pobraniu nowych uaktualnień do repozytorium**.

W rezultacie utworzone zadanie rozsyłania uaktualnień będzie uruchamiane dla wybranych komputerów za każdym razem po pobraniu uaktualnień do repozytorium Serwera administracyjnego.

Jeśli zadanie rozsyłania uaktualnień dla wybranej aplikacji zostało utworzone dla wybranych komputerów, aby automatycznie rozesłać uaktualnienia na komputery klienckie, w oknie właściwości zadania, w sekcji **Terminarz** wybierz opcję **Po pobraniu nowych uaktualnień do repozytorium** w polu **Zaplanowane uruchomienie**.

KONFIGUROWANIE PROFILI APLIKACJI

W celu skonfigurowania profilu dla aplikacji:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której chcesz skonfigurować profil.
2. W obszarze roboczym wybranej grupy, na zakładce **Profile** wybierz profil wymaganej aplikacji.
3. Otwórz okno właściwości profilu i skonfiguruj profil.

Po zastosowaniu zmian profil będzie stosowany ze zmienionymi ustawieniami dla komputerów w grupach administracyjnych.

PRZEGLĄDANIE I MODYFIKOWANIE LOKALNYCH USTAWIEŃ APLIKACJI

System administracyjny Kaspersky Security Center umożliwia zdalne zarządzanie lokalnymi ustawieniami aplikacji na komputerach zdalnych poprzez Konsolę administracyjną.

Lokalne ustawienia aplikacji są ustawieniami aplikacji określonymi dla komputera klienckiego. Możesz użyć Kaspersky Security Center do określenia lokalnych ustawień aplikacji na komputerach klienckich znajdujących się w grupach administracyjnych.

Szczegółowe opisy ustawień aplikacji firmy Kaspersky Lab znajdują się w odpowiednich dokumentach.

W celu przejrzenia lub modyfikacji lokalnych ustawień aplikacji:

1. W obszarze roboczym grupy, do której należą żądane komputery klienckie, wybierz zakładkę **Komputery**.
2. W oknie właściwości komputera klienckiego, w sekcji **Aplikacje** wybierz żądaną aplikację.

3. Otwórz okno właściwości aplikacji, klikając dwukrotnie nazwę aplikacji lub klikając przycisk **Właściwości**.

Zostanie otwarte okno lokalnych ustawień wybranej aplikacji, w którym będziesz mógł je przeglądać i modyfikować.

Możesz zmienić wartości ustawień, których modyfikowanie nie zostało zablokowane przez profil grupowy (tzn. które nie są oznaczone "kłódką" w profilu).

KONFIGUROWANIE POWIADOMIEŃ

Kaspersky Security Center umożliwia konfigurowanie powiadomień o zdarzeniach występujących na urządzeniach klienckich oraz wybieranie metody powiadamiania:

- poprzez e-mail;
- SMS;
- po uruchomieniu pliku wykonywalnego.

W celu skonfigurowania wysyłania powiadomień o zdarzeniach występujących na urządzeniach klienckich:

1. Otwórz okno właściwości foldera **Raporty i powiadomienia** z drzewa konsoli w jeden z następujących sposobów:
   - Wybierz **Właściwości** z menu kontekstowego foldera **Raporty i powiadomienia** drzewa konsoli.
   - W obszarze roboczym foldera **Raporty i powiadomienia**, na zakładce **Powiadomienia** otwórz okno, klikając odnośnik **Modyfikuj ustawienia dostarczania powiadomień**.
2. Skonfiguruj powiadomienia o zdarzeniach w sekcji **Powiadomienia** okna właściwości foldera **Raporty i powiadomienia**.

W rezultacie skonfigurowane ustawienia powiadamiania zostaną zastosowane do wszystkich zdarzeń występujących na urządzeniach klienckich.

Ustawienia powiadamiania o zdarzeniu można skonfigurować w oknie właściwości tego zdarzenia. Szybki dostęp do ustawień zdarzeń można uzyskać, klikając odnośniki **Skonfiguruj zdarzenia Kaspersky Endpoint Security** i **Modyfikuj ustawienia zdarzeń Serwera administracyjnego**.

SPRAWDZANIE DOSTARCZANIA POWIADOMIEŃ

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

W celu sprawdzenia dostarczania powiadomień o zdarzeniach:

1. Zatrzymaj zadanie ochrony systemu plików w czasie rzeczywistym na komputerze klienckim, a następnie skopiuj na niego "wirusa" EICAR. Teraz ponownie uruchom zadanie ochrony systemu plików w czasie rzeczywistym.
2. Uruchom zadanie skanowania komputerów klienckich dla grupy administracyjnej lub dla zbioru komputerów, gdzie na jednym z komputerów klienckich znajduje się "wirus" EICAR.

   Jeżeli zadanie skanowania jest skonfigurowane poprawnie, "wirus" testowy zostanie wykryty. Jeżeli powiadomienia są skonfigurowane poprawnie, zostaniesz powiadomiony o wykryciu wirusa.

   W folderze **Zdarzenia i powiadomienia** wybór **Ostatnie zdarzenia** podfolderu **Zdarzenia** wyświetla wpisy dotyczące wykrycia "wirusa".

"Wirus" testowy EICAR NIE JEST WIRUSEM, ponieważ nie zawiera kodu mogącego uszkodzić komputer. Jednak większość programów antywirusowych wykrywa ten plik jako wirusa. "Wirusa" testowego możesz pobrać z oficjalnej strony EICAR.

TWORZENIE I PRZEGLĄDANIE RAPORTU

W celu utworzenia i przejrzenia raportu:

1. W drzewie konsoli otwórz folder **Raporty i powiadomienia**, w którym znajdują się szablony raportów.

2. Wybierz wymagany szablon raportu z drzewa konsoli lub z obszaru roboczego na zakładce **Raporty**.

   Obszar roboczy wyświetli raport utworzony na podstawie wybranego szablonu.

Raport wyświetla następujące dane:

- nazwę i typ raportu, jego krótki opis i okres raportowania, a także informacje o grupie urządzeń, dla których został wygenerowany raport;
- wykres odzwierciedlający najważniejsze dane z raportu;
- tabelę podsumowującą dane dotyczące wyliczonych wartości z raportu;
- tabelę ze szczegółowymi danymi z raportu.

ZAPISYWANIE RAPORTU

W celu zapisania utworzonego raportu:

1. W drzewie konsoli otwórz folder **Raporty i powiadomienia**, w którym znajdują się szablony raportów.
2. Wybierz wymagany szablon raportu z drzewa konsoli lub z obszaru roboczego na zakładce **Raporty**.
3. Z menu kontekstowego wybranego szablonu raportu wybierz **Zapisz**.

Zostanie uruchomiony Kreator zapisywania raportu. Postępuj zgodnie z jego poleceniami.

Po zakończeniu działań Kreatora, zostanie otwarty folder, w którym znajduje się zapisany plik raportu.

TWORZENIE ZADANIA DOSTARCZANIA RAPORTU

Dostarczanie raportów w Kaspersky Security Center jest wykonywane przez zadanie dostarczania raportów. Możesz dostarczać raporty poprzez e-mail lub zapisać je w określonym folderze, na przykład w folderze współdzielonym na Serwerze administracyjnym lub na komputerze lokalnym.

W celu utworzenia zadania dostarczania raportu:

1. W drzewie konsoli otwórz folder **Raporty i powiadomienia**, w którym znajdują się szablony raportów.
2. Wybierz wymagany szablon raportu z drzewa konsoli lub z obszaru roboczego na zakładce **Raporty**.
3. Z menu kontekstowego szablonu raportu wybierz polecenie **Wyślij raporty**.

Zostanie uruchomiony Kreator tworzenia zadania dostarczania raportu. Postępuj zgodnie z jego poleceniami.

W celu utworzenia zadania wysyłania kilku raportów:

1. Z drzewa konsoli wybierz folder **Zadania Serwera administracyjnego**.
2. Uruchom tworzenie zadania w jeden z następujących sposobów:
   - W drzewie konsoli, z menu kontekstowego folderu **Zadania Serwera administracyjnego** wybierz **Nowy** → **Zadanie**.
   - Kliknij odnośnik **Utwórz zadanie** dostępny w obszarze roboczym.

   Zostanie uruchomiony Kreator tworzenia zadania Serwera administracyjnego. Postępuj zgodnie z jego poleceniami. W oknie **Typ zadania** kreatora wybierz **Dostarcz raporty**.

Utworzone zadanie dostarczania raportu jest wyświetlane w drzewie konsoli, w folderze **Zadania Serwera administracyjnego**.

Zadanie dostarczania raportu jest tworzone automatycznie, jeśli w trakcie instalacji Kaspersky Security Center określono ustawienia e-mail.

WYŚWIETLANIE RAPORTU O WYKRYTYCH WIRUSACH

W celu wygenerowania raportu o wykrytych wirusach:

1. Z drzewa konsoli wybierz folder **Raporty i powiadomienia**.

2. W obszarze roboczym foldera, na zakładce **Statystyki** wybierz stronę **Statystyki antywirusowe**.

Podsumowanie aktywności z okresu poprzednich 24 godzin jest domyślnie wyświetlane w panelach informacyjnych strony:

- historia aktywności wirusów;
- najczęściej występujące wirusy;
- komputery z największą liczbą wykrytych wirusów;
- użytkownicy, na komputerach których wykryto największą liczbę wirusów.

W folderze **Raporty i powiadomienia**, znajdującym się w drzewie konsoli, na zakładce **Raporty** możesz również wyświetlić szczegółowy raport o wirusach wykrytych w sieci. Na tej zakładce, w sekcji ustawień **Statystyki ochrony antywirusowej** możesz przejrzeć raporty szczegółowe, klikając następujące odnośniki:

- **Raport o wirusach**
- **Raport o najbardziej zainfekowanych komputerach**
- **Raport o użytkownikach zainfekowanych komputerów**

Po wybraniu wymaganego raportu, w obszarze roboczym zostaną wyświetlone szczegółowe informacje o wykrytych wirusach zgromadzone od czasu instalacji Serwera administracyjnego.

Możesz zmienić ustawienia dla każdego raportu, na przykład, okres czasu, dla którego ma być tworzony raport, bądź zestaw pól wyświetlanych w raporcie (więcej szczegółowych informacji znajdziesz w *Podręczniku administratora Kaspersky Security Center*).

WYŚWIETLANIE INFORMACJI O ZDARZENIACH

W celu wyświetlenia informacji o działaniu aplikacji:

1. Z folderu **Raporty i powiadomienia**, znajdującego się w drzewie konsoli, wybierz podfolder **Zdarzenia**.
2. Otwórz wybór zdarzeń w jeden z następujących sposobów:
   - W drzewie konsoli rozwiń folder **Zdarzenia** i wybierz podfolder zawierający wymagany wybór zdarzeń.
   - W obszarze roboczym foldera **Zdarzenia**, w sekcji **Wybory predefiniowane** kliknij odnośnik odpowiadający wymaganemu wyborowi zdarzeń.

   W rezultacie obszar roboczy będzie wyświetlać listę zdarzeń wybranego typu, przechowywanych na Serwerze administracyjnym.

Możesz także utworzyć swój własny wybór zdarzeń (w celu uzyskania szczegółowych informacji zajrzyj do *Podręcznika administratora Kaspersky Security Center*).

WYŚWIETLANIE OBECNEGO STANU OCHRONY ANTYWIRUSOWEJ

Możesz monitorować stan ochrony komputerów klienckich i urządzeń zarządzanych przez Serwer administracyjny **<Nazwa Serwera>** w obszarze roboczym węzła **<Nazwa Serwera>**. W sekcjach zarządzających obszaru roboczego wyświetlane są ogólne informacje o stanie następujących modułów działania aplikacji:

- Wdrożenie ochrony na komputerach w sieci (sekcja **Zdalna instalacja**)
- Tworzenie struktury grup administracyjnych zawierających zarządzane komputery (sekcja **Zarządzanie komputerem**)
- Wydajność ochrony na urządzeniach klienckich (sekcja **Ochrona komputera i skanowanie antywirusowe**)
- Aktualizowanie baz danych i modułów aplikacji (sekcja **Aktualizacja**)
- Monitorowanie i wysyłanie powiadomień (sekcja **Monitorowanie**).

Stan systemu ochrony można sprawdzić, korzystając z ikon przypominających sygnalizację świetlną, znajdujących się w sekcjach do zarządzania. Jeżeli ikona jest zielona, wszystkie wymagane zadania dla tej strefy funkcjonalności zostały zakończone powodzeniem. Jeżeli ikona jest żółta lub czerwona, ta strefa funkcjonalności wymaga Twojej uwagi, gdyż może być konieczne wykonanie kilku czynności.

Oprócz koloru każda sekcja zawiera krótki opis stanu systemu ochrony lub istniejącego problemu, a także odnośniki, których możesz używać do uruchamiania głównych zadań w sekcji.

W celu uzyskania szczegółowych informacji o stanie systemu ochrony wybierz folder **Raporty i powiadomienia**.

TWORZENIE KOPII ZAPASOWEJ DANYCH SERWERA ADMINISTRACYJNEGO

Kreator automatycznej konfiguracji z Kaspersky Security Center tworzy Zadanie tworzenia kopii zapasowej danych Serwera administracyjnego. Domyślnie kopia zapasowa jest tworzona codziennie na komputerze, na którym zainstalowany jest Serwer administracyjny, w podfolderze Kopia zapasowa foldera instalacyjnego aplikacji.

W celu ręcznego uruchomienia tworzenia kopii zapasowej danych Serwera administracyjnego:

1. Z drzewa konsoli wybierz folder **Zadania Serwera administracyjnego**.
2. W obszarze roboczym foldera wybierz zadanie tworzenia kopii zapasowej danych Serwera administracyjnego (domyślnie jest to zadanie **Utwórz kopię zapasową danych Serwera administracyjnego**).
3. Uruchom wybrane zadanie.

Ponieważ wirtualne Serwery administracyjne korzystają z bazy danych głównego Serwera administracyjnego, tworzenie kopii zapasowej i przywracanie danych wirtualnego Serwera administracyjnego jest wykonywane jedynie w trakcie tworzenia kopii zapasowej i przywracania danych na głównym Serwerze administracyjnym.

AKTUALIZOWANIE Z KASPERSKY SECURITY CENTER 9.0 DO KASPERSKY SECURITY CENTER 10.0

Ta sekcja opisuje procedurę aktualizacji programu Kaspersky Security Center 9.0 do Kaspersky Security Center 10.0, a także podstawowe działania, które należy wykonać podczas wstępnej konfiguracji aplikacji w nowej wersji.

W celu aktualizacji z wersji 9.0 do Kaspersky Security Center 10.0:

1. Dla Kaspersky Security Center 9.0 utwórz kopię zapasową danych Serwera administracyjnego, korzystając z narzędzia *klbackup*. Narzędzie to jest zawarte w pakiecie dystrybucyjnym aplikacji i znajduje się w głównym folderze instalacyjnym Kaspersky Security Center.
2. Zainstaluj Serwer administracyjny i Konsolę administracyjną (wersja 10.0).

   Możesz zainstalować Serwer administracyjny na komputerze, na którym zainstalowano wcześniejszą wersję Serwera administracyjnego. Po zaktualizowaniu Serwera administracyjnego do wersji 10.0 zapisane zostaną wszystkie dane i ustawienia z poprzedniej wersji aplikacji.

   Jeżeli zainstalujesz Serwer administracyjny na innym komputerze, możesz przywrócić ustawienia poprzedniej wersji, korzystając z narzędzia do tworzenia kopii zapasowej i przywracania danych (*klbackup*).
3. Jeżeli ustawienia nie zostały skopiowane z poprzedniej wersji Serwera administracyjnego, przeprowadź wstępną konfigurację Serwera administracyjnego.
4. Utwórz strukturę grup administracyjnych.
5. Wybierz komputery klienckie, na których powinna zostać zainstalowana nowa wersja Serwera administracyjnego oraz nowe wersje aplikacji Kaspersky Lab.
6. Dla wybranych komputerów utwórz zadanie zdalnej instalacji nowej wersji Agenta sieciowego oraz nowych wersji żądanych aplikacji. Aby przeprowadzić zdalną instalację aplikacji, możesz użyć pakietów instalacyjnych utworzonych automatycznie podczas instalacji Kaspersky Security Center 10.0.
7. Uruchom utworzone zadanie.

   W wyniku tego nowa wersja Agenta sieciowego i nowe wersje aplikacji Kaspersky Lab zostaną zainstalowane na wybranych komputerach klienckich.
8. Do hierarchii grup administracyjnych dodaj komputery klienckie, na których aplikacje zostały zaktualizowane do nowych wersji.

System ochrony stworzony przez poprzednie wersje aplikacji będzie zarządzany przez Kaspersky Security Center 10.0.

Możesz konwertować profile i zadania utworzone dla poprzednich wersji aplikacji firmy Kaspersky Lab do profili i zadań dla nowych wersji, korzystając z Kreatora konwersji profili i zadań. Szczegółowe informacje można znaleźć w *Podręczniku administratora dla Kaspersky Security Center*.

PODSUMOWANIE

Ta sekcja podsumowuje informacje zawarte w dokumencie.

Dokument opisuje prosty scenariusz wdrażania ochrony w sieci firmowej, a także działania niezbędne do szybkiego wdrożenia ochrony i rozpoczęcia korzystania z Kaspersky Security Center. Szczegółowe informacje o funkcjach Kaspersky Security Center i scenariuszach wdrażania ochrony można znaleźć w *Przewodniku instalacji* i *Podręczniku administratora dla Kaspersky Security Center*.

KONTAKT Z DZIAŁEM POMOCY TECHNICZNEJ

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

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 (patrz strona 7), zalecamy skontaktowanie się z działem pomocy technicznej firmy Kaspersky Lab. Eksperci z działu pomocy technicznej odpowiedzą na wszelkie pytania związane z instalacją i użytkowaniem aplikacji.

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:

- Za pośrednictwem telefonu. Metoda ta pozwala na skonsultowanie się ze specjalistami z naszej pomocy technicznej w języku polskim.
- Przesyłając zgłoszenie poprzez system Kaspersky CompanyAccount na stronie internetowej działu pomocy technicznej. Metoda ta pozwala na kontakt ze specjalistami pomocy technicznej za pośrednictwem formularza zgłoszeniowego.

POMOC TECHNICZNA ZA POŚREDNICTWEM TELEFONU

W przypadku naglącego problemu możesz zadzwonić do specjalistów z pomocy technicznej (http://www.kaspersky.pl/services.html?s=support).

Przed skontaktowaniem się z działem pomocy technicznej przeczytaj zasady korzystania z pomocy technicznej (http://support.kaspersky.com/pl/support/details). Umożliwi to specjalistom szybkie rozwiązanie problemu.

UZYSKIWANIE POMOCY TECHNICZNEJ POPRZEZ COMPANYACCOUNT

Kaspersky CompanyAccount to usługa sieciowa (https://companyaccount.kaspersky.com) służąca do przesyłania i śledzenia zgłoszeń wysyłanych do Kaspersky Lab.

Aby uzyskać dostęp do CompanyAccount, zarejestruj się na stronie rejestracyjnej (https://support.kaspersky.com/companyaccount/register?LANG=pl) i uzyskaj nazwę użytkownika oraz hasło. W tym celu należy określić kod aktywacyjny lub plik klucza (sekcja "Informacje o pliku klucza" na stronie 13).

Przy użyciu Kaspersky CompanyAccount możesz wykonać następujące czynności:

- skontaktować się z działem pomocy technicznej i laboratorium antywirusowym;
- skontaktować się z działem pomocy technicznej bez konieczności używania poczty;
- śledzić stan swojego zgłoszenia w czasie rzeczywistym;

- przeglądać szczegółową historię Twoich zgłoszeń wysyłanych do działu pomocy technicznej;
- uzyskać kopię pliku klucza w przypadku jego zagubienia lub usunięcia.

Pomoc techniczna za pośrednictwem poczty elektronicznej

Zgłoszenie do działu pomocy technicznej można wysłać w języku polskim.

W polach formularza internetowego zgłoszenia należy określić następujące dane:

- typ zapytania;
- nazwę aplikacji i numer wersji;
- treść zapytania.

W razie konieczności możesz również załączyć pliki do elektronicznego formularza zgłoszenia.

Specjaliści z pomocy technicznej będą wysyłać odpowiedzi na Twoje pytania za pośrednictwem Kaspersky CompanyAccount na adres e-mail określony w trakcie rejestracji.

Zgłoszenie internetowe do Laboratorium antywirusowego

Niektóre pytania należy wysyłać do laboratorium antywirusowego, a nie do pomocy technicznej.

Do laboratorium antywirusowego możesz wysyłać zgłoszenia następujących typów:

- *Nieznany szkodliwy program* – podejrzewasz, że plik zawiera wirusa, ale Kaspersky Security Center nie rozpoznał pliku go jako zainfekowanego.

  Specjaliści z laboratorium antywirusowego przeanalizują przysłany szkodliwy kod. Jeśli wykryją oni nieznanego wirusa, dodadzą odpowiedni opis do bazy danych, która stanie się dostępna przy aktualizacji aplikacji antywirusowych.

- *Fałszywy alarm* – Kaspersky Security Center błędnie klasyfikuje plik jako wirusa.

Możesz również wysłać zgłoszenie do laboratorium antywirusowego ze strony z formularzem zgłoszenia (http://support.kaspersky.com/virlab/helpdesk.html?LANG=pl), nie rejestrując się w usłudze Kaspersky CompanyAccount. Na tej stronie nie musisz określać kodu aktywacyjnego aplikacji. Priorytety zgłoszeń wygenerowanych za pośrednictwem formularza zgłoszeniowego są niższe, niż zgłoszeń utworzonych poprzez Kaspersky CompanyAccount.

KASPERSKY LAB ZAO

Kaspersky Lab jest znaną na całym świecie firmą zajmującą się tworzeniem oprogramowania do ochrony komputerów przed wirusami, szkodliwymi programami, 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"). Zgodnie z ankietą "TGI-Russia 2009" przeprowadzoną przez COMCON, Kaspersky Lab jest preferowanym dostawcą oprogramowania chroniącego komputery w Rosji.

Firma Kaspersky Lab została założona w 1997 roku w Rosji. Obecnie Kaspersky Lab jest międzynarodową grupą firm z główną siedzibą w Moskwie i pięcioma regionalnymi oddziałami zarządzającymi aktywnością firmy w Rosji, Europie Zachodniej i Wschodniej, na Bliskim wschodzie, w Afryce, Ameryce Północnej i Południowej, Japonii, Chinach i innych krajach Dalekiego wschodu. Firma zatrudnia ponad 2000 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 antywirusowe dla komputerów stacjonarnych, laptopów, PDA oraz smartfonów i innych urządzeń mobilnych.

Ponadto firma oferuje także aplikacje i usługi do ochrony stacji roboczych, serwerów plików i serwerów sieciowych, bram pocztowych oraz zapór sieciowych. W połączeniu ze scentralizowanym systemem zarządzania Kaspersky Lab rozwiązania te zapewniają firmom i organizacjom efektywną 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 nowych zagrożeń oraz tworzą narzędzia do ich wykrywania i leczenia, które następnie umieszczają w bazach danych używanych przez aplikacje firmy Kaspersky Lab. *Firma Kaspersky Lab uaktualnia antywirusowe bazy danych raz na godzinę*, a *antyspamowe bazy danych co 5 minut*.

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: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Izrael), Clearswift (Wielka Brytania), CommuniGate Systems (USA), Critical Path (Irlandia), D-Link (Tajwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (Francja), NETGEAR (USA), Parallels (Rosja), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Tajwan). 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 2010 roku program Kaspersky Anti-Virus otrzymał kilka najwyższych nagród Advanced+ w teście przeprowadzonym przez AV-Comparatives, szanowane austriackie laboratorium antywirusowe. Jednakże największym osiągnięciem Kaspersky Lab jest zaufanie i lojalność użytkowników na całym świecie. Nasze produkty i technologie chronią ponad 300 milionów użytkowników oraz ponad 200 000 klientów korporacyjnych.

Oficjalna strona Kaspersky Lab:	http://www.kaspersky.pl
Encyklopedia Wirusów:	http://www.securelist.pl/
Laboratorium antywirusowe:	nowywirus@kaspersky.pl (tylko do wysyłania podejrzanych plików w archiwach) http://support.kaspersky.com/virlab/helpdesk.html?LANG=pl (do wysyłania pytań do analityków wirusów)
Forum internetowe Kaspersky Lab:	http://forum.kaspersky.com

INFORMACJE O KODZIE FIRM TRZECICH

Informacje o kodzie firm trzecich znajdują się w pliku o nazwie legal_notices.txt przechowywanym w folderze instalacyjnym aplikacji.

INFORMACJE O ZNAKACH TOWAROWYCH

Zastrzeżone znaki towarowe i nazwy usług są własnością ich właścicieli.

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

Apple to zastrzeżony znak towarowy firmy Apple Inc.