TREND MICRO

XG

OfficeScan™

Podręcznik administratora

Dla przedsiębiorstw i średnich firm

Endpoint Security

Protected Cloud

Web Security

TREND MICRO SMART Protection Network™

Numer części dokumentu: OSPMXG7608/161028

Data wydania: październik 2016 r.

Niniejsza dokumentacja zawiera opis głównych funkcji produkt oraz instrukcje instalacji w środowisku produkcyjnym. Należy ją przeczytać przed zainstalowaniem lub rozpoczęciem użytkowania produkt.

Szczegółowe informacje na temat użycia określonych funkcji w ramach produkt można znaleźć w centrum pomocy online firmy Trend Micro lub w bazie wiedzy firmy Trend Micro.

Firma Trend Micro stara się zawsze ulepszać swoją dokumentację. W przypadku pytań, komentarzy lub sugestii na temat tego lub dowolnego innego dokumentu firmy Trend Micro prosimy o kontakt pod adresem docs@trendmicro.com.

Prosimy o ocenę tego dokumentu w witrynie:

http://www.trendmicro.com/download/documentation/rating.asp

Spis treści

Rozdział 3: Wprowadzenie do modułu Ochrona danych

Część II: Ochrona agentów OfficeScan

Rozdział 4: Korzystanie z usługi Trend Micro Smart Protection

Rozdział 5: Instalowanie agenta OfficeScan

Rozdział 6: Aktualizowanie ochrony

Rozdział 7: Skanowanie w poszukiwaniu zagrożeń bezpieczeństwa

Rozdział 8: Ochrona przed nieznanymi zagrożeniami

Rozdział 9: Korzystanie z funkcji Monitorowanie zachowań

Rozdział 10: Korzystanie z funkcji kontroli urządzeń

Rozdział 11: Używanie funkcji Zapobieganie utracie danych

Rozdział 12: Korzystanie z usług Web Reputation

Rozdział 13: Korzystanie z zapory OfficeScan

Część III: Zarządzanie serwerem OfficeScan i agentami

Rozdział 14: Zarządzanie serwerem OfficeScan

Rozdział 15: Zarządzanie agentem OfficeScan

Część IV: Zapewnienie dodatkowej ochrony

Rozdział 16: Ochrona agentów zdalnych

Rozdział 17: Używanie programu Plug-In Manager

Rozdział 18: Zasoby dotyczące rozwiązywania problemów

Rozdział 19: Pomoc techniczna

Załączniki

Dodatek A: Obsługa protokołu IPv6 w programie OfficeScan

Dodatek B: Obsługa systemu Windows Server Core

Dodatek C: Obsługa systemów Windows 8/8.1/10 i Windows Server 2012/2016

Dodatek D: Przywracanie poprzedniej wersji programu OfficeScan

Dodatek E: Słownik

Indeks

Wstęp

Wstęp

Ten dokument dotyczy informacji wstępnych, procedur instalacji agenta oraz zarządzania serwerem i agentami OfficeScan.

Rozdział składa się z następujących tematów:

Dokumentacja programu OfficeScan

Dokumentacja programu OfficeScan zawiera następujące elementy:

TABELA 1. Dokumentacja programu OfficeScan

DOKUMENTACJA	OPIS
Podręcznik instalacji oraz uaktualniania	Dokument PDF zawierający omówienie wymogów i procedur dotyczących instalacji serwera OfficeScan oraz uaktualnienia serwera i agentów.
Wymagania systemowe	Dokument PDF zawierający omówienie minimalnych i zalecanych wymagań systemowych w celu zainstalowania serwera OfficeScan oraz uaktualnienia serwera i agentów.
Podręcznik administratora	Dokument PDF obejmujący wprowadzenie, procedury instalacji Agent OfficeScan oraz zarządzanie agentami i serwerem OfficeScan.
Pomoc	Pliki HTML skompilowane w formacie WebHelp lub CHM, zawierające instrukcje korzystania, porady i informacje dotyczące określonych zastosowań programu. Pomoc jest dostępna z poziomu konsoli serwera i agenta OfficeScan oraz z głównego okna konfiguracji programu OfficeScan.
Plik Readme	Zawiera listę znanych problemów i podstawowych czynności instalacyjnych. Plik ten może również zawierać najnowsze informacje o produkcie, które nie znajdują się w systemie pomocy ani w dokumentacji drukowanej.
Baza wiedzy	Baza danych online zawierająca informacje dotyczące rozwiązywania problemów. Zawiera najnowsze informacje o znanych problemach dotyczących produktu. Aby uzyskać dostęp do Bazy wiedzy, odwiedź następującą witrynę internetową: http://esupport.trendmicro.com

Najnowsze wersje dokumentów PDF i plików Readme znajdują się pod adresem:

http://docs.trendmicro.com/pl-pl/enterprise/officescan.aspx

Odbiorcy

Dokumentacja oprogramowania OfficeScan jest przeznaczona dla następujących użytkowników:

- Administratorzy programu OfficeScan: osoby odpowiedzialne za zarządzanie programem OfficeScan, w tym również za instalację i zarządzanie serwerami i agentami programu OfficeScan. Od użytkowników tego typu oczekuje się zaawansowanej wiedzy na temat zarządzania serwerem i siecią.
- Użytkownicy końcowi: użytkownicy, którzy mają na punktach końcowych zainstalowanego agenta OfficeScan.. Poziom umiejętności takich osób w zakresie punktów końcowych jest różny — od początkujących po zaawansowanych.

Konwencje przyjęte w dokumentacji

W dokumentach zostały zastosowane następujące konwencje.

TABELA 2. Konwencje przyjęte w dokumentacji

KONWENCJA	OPIS
WIELKIE LITERY	Akronimy, skróty, nazwy poleceń oraz klawisze klawiatury
Pogrubienie	Menu, polecenia menu, przyciski, karty i opcje
Kursywa	Odwołania do innych dokumentów
`Stała szerokość liter`	Przykładowe polecenia, kod programu, adresy URL, nazwy plików oraz dane wyjściowe programu
Ścieżka > **nawigacji**	Ścieżka nawigacji umożliwiająca dotarcie do określonego ekranu. Na przykład **Plik** > **Zapisz** oznacza, że należy najpierw kliknąć w interfejsie menu **Plik**, a następnie polecenie **Zapisz**.
Uwaga	Uwagi dotyczące konfiguracji

KONWENCJA	OPIS
 Porada	Zalecenia lub sugestie
 Ważne	Informacje dotyczące wymaganych lub domyślnych ustawień konfiguracji i ograniczeń produktu
 OSTRZEŻENIE!	Krytyczne operacje i opcje konfiguracji

Terminologia

W poniższej tabeli przedstawiono oficjalną terminologię stosowaną w dokumentacji programu OfficeScan:

TABELA 3. Terminologia OfficeScan

TERMINOLOGIA	OPIS
Agent OfficeScan	Program OfficeScan agent
Agent punkt końcowy	Punkt końcowy, na którym jest zainstalowany Agent OfficeScan.
Użytkownik agenta (lub użytkownik)	Osoba zarządzająca agentem OfficeScan na punkcie końcowym agenta
Serwer	Program serwera OfficeScan
Komputer serwera	Punkt końcowy, na którym jest zainstalowany serwer OfficeScan.
Administrator (lub administrator programu OfficeScan)	Osoba zarządzająca serwerem OfficeScan.

TERMINOLOGIA	OPIS
Konsola	Interfejs użytkownika umożliwiający konfigurowanie i zarządzanie ustawieniami serwera OfficeScan i agenta. Konsola programu serwera OfficeScan jest nazywana „konsolą Web”, a konsola programu agenta OfficeScan — „konsolą agenta”.
Zagrożenie bezpieczeństwa	Zbiorczy termin, określający wirusy/złośliwe oprogramowanie, spyware/grayware oraz zagrożenia z sieci Web.
Usługa licencji	Dotyczy usługi ochrony przed wirusami, Usługi Usuwania Szkód Services, usługi Web Reputation oraz usługi ochrony przed oprogramowaniem spyware—wszystkie usługi są aktywowane podczas instalacji serwera OfficeScan.
Usługa OfficeScan Service	Usługi dostępne z poziomu konsoli Microsoft Management Console (MMC). Na przykład `ofcservice.exe` — główna usługa OfficeScan.
Program	Zawiera agenta OfficeScan i program Plug-in Manager.
Składniki	Odpowiedzialne za skanowanie, wykrywanie zagrożeń bezpieczeństwa oraz za wykonywanie operacji w przypadku ich wykrycia.

`Folder instalacji agenta`	Folder na punkcie końcowym, który zawiera pliki agenta OfficeScan. W przypadku zaakceptowania domyślnych ustawień podczas instalacji folder instalacji znajduje się w jednej z następujących lokalizacji:
	
	`C:\Program Files\Trend Micro\OfficeScan Client`
	
	`C:\Program Files (x86)\Trend Micro\OfficeScan Client`

TERMINOLOGIA	OPIS

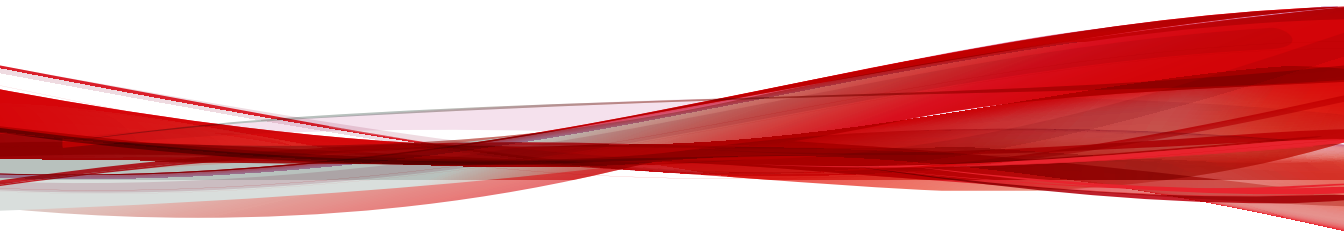
`Folder instalacji serwera`	Folder na punkcie końcowym, który zawiera pliki serwera OfficeScan. W przypadku zaakceptowania domyślnych ustawień podczas instalacji folder instalacji znajduje się w jednej z następujących lokalizacji:
	`C:\Program Files\Trend Micro\OfficeScan`
	`C:\Program Files (x86)\Trend Micro\OfficeScan`
	Jeśli na przykład plik znajduje się w folderze `\PCCSRV` umieszczonym w folderze instalacji serwera, pełna ścieżka dostępu do pliku to:
	`C:\Program Files\Trend Micro\OfficeScan\PCCSRV \<nazwa_pliku>`.

Agent Smart Scan	Dowolny Agent OfficeScan skonfigurowany do skanowania Smart Scan
Agent skanowania standardowego	Dowolny Agent OfficeScan skonfigurowany do skanowania standardowego
Dwa stosy	Obiekty, które mają zarówno adres IPv4, jak i adres IPv6. Na przykład: • Punkty końcowe, które mają zarówno adres IPv4, jak i adres IPv6 • Agenci OfficeScan zainstalowani na punktach końcowych z dwoma stosami punkty końcowe • Agenci aktualizacji, którzy rozsyłają aktualizacje do agentów • Serwer proxy z dwoma stosami, taki jak DeleGate, może wykonywać konwersję między adresami IPv4 i IPv6.
Obiekt wykorzystujący wyłącznie protokół IPv4	Obiekt, który ma tylko adres IPv4
Obiekt wykorzystujący wyłącznie protokół IPv6	Obiekt, który ma tylko adres IPv6

TERMINOLOGIA	OPIS
Rozwiązania dodatków	Natywne funkcje programu OfficeScan i programy dodatków dostarczane za pomocą programu Plug-in Manager

Część I

Wprowadzenie



Rozdział 1

Wprowadzenie do programu OfficeScan

Ten rozdział zawiera wprowadzenie do programu Trend Micro™OfficeScan™ oraz przegląd jego głównych funkcji i możliwości.

Rozdział składa się z następujących tematów:

Informacje o programie OfficeScan

Program Trend Micro™OfficeScan™ zabezpiecza sieci korporacyjne przed złośliwym oprogramowaniem, wirusami sieciowymi, zagrożeniami internetowymi, a także przed spyware i atakami ze strony zagrożeń mieszanych. Program OfficeScan jest zintegrowanym rozwiązaniem i składa się z programu agenta OfficeScan, który znajduje się na punkcie końcowym, oraz programu serwera, który zarządza wszystkimi agentami. Agent OfficeScan chroni punkt końcowy i wysyła informacje o stanie zabezpieczeń do serwera. Obsługiwany przez konsolę zarządzania opartą na sieci Web serwer ułatwia ustalenie skoordynowanych reguł bezpieczeństwa i wdrażanie aktualizacji każdego agenta.

Oprogramowanie OfficeScan działa na bazie rozwiązania Trend Micro Smart Protection Network™. Jest to nowoczesna infrastruktura zabezpieczeń zasobów klientów pracujących w chmurze oferująca lepsze bezpieczeństwo, niż standardowe rozwiązania. Wyjątkowa technologia pracy w chmurze i agent, który wymaga niewielkiej ilości zasobów, zmniejszają zależność od zwyczajnych sposobów pobierania sygnatur i usuwają opóźnienia, które z reguły występują w takich sytuacjach. W ten sposób firmy mogą korzystać ze zwiększonej przepustowości sieci, mniejszej wymaganej mocy obliczeniowej i wynikających z tego oszczędności. Użytkownicy zaś zyskują natychmiastowy dostęp do najnowszych standardów ochrony, niezależnie od tego, czy pracują z sieci firmowej, z domu czy są w podróży.

Nowości w programie OfficeScan XG

Ta wersja programu OfficeScan zawiera następujące nowe funkcje i ulepszenia:

FUNKCJA	OPIS
Rozszerzona ochrona przed oprogramowaniem typu ransomware	Ochrona przed atakami z użyciem oprogramowania typu ransomware została rozszerzona o funkcję odzyskiwania przez Agenci OfficeScan plików zaszyfrowanych przez zagrożenia typu ransomware, blokowania procesów skojarzonych z oprogramowaniem typu ransomware oraz zapobiegania zarażeniu sieci przez zaatakowane pliki wykonywalne. Aby uzyskać więcej informacji, patrz *Ochrona przed oprogramowaniem typu ransomware na stronie 9-3*.
Rozszerzona ochrona przed nowo napotkanymi programami	Aby ułatwić maksymalizację zasad ochrony przez oprogramowaniem typu ransomware na poszczególnych agentach, funkcja ochrony przed nowo napotkanymi programami została przeniesiona na ekran Ustawienia monitorowania zachowania. Aby uzyskać więcej informacji, patrz *Ochrona przed nowo napotkanymi programami na stronie 9-6*. Można także dostosować komunikat wyświetlany na punktach końcowych agentów, gdy użytkownik pobierze i uruchomi nowo napotkany program. Aby uzyskać więcej informacji, patrz *Zmiana treści powiadomień programu na stronie 9-18*.
Predykcyjne uczenie maszynowe	Silnik przewidującego uczenia maszynowego może chronić sieć przed niezidentyfikowanymi lub nieznanymi zagrożeniami dzięki zaawansowanym funkcjom analizy plików oraz monitorowania procesów za pomocą algorytmów heurystycznych. Predykcyjne uczenie maszynowe może potwierdzić prawdopodobieństwo występowania zagrożenia w pliku lub procesie oraz określić prawdopodobny typ zagrożenia, zapewniając ochronę przed nowymi atakami.

FUNKCJA	OPIS
Serwer Przekaźnika Krawędziowego OfficeScan	Program Serwer Przekaźnika Krawędziowego OfficeScan zapewnia lepszy wgląd do danych oraz lepszą ochronę punktów końcowych w warstwie brzegowej lokalnej sieci intranetowej dzięki następującym funkcjom: • Synchronizacja listy podejrzanych obiektów • Przesyłanie próbek • Przesyłanie dzienników • Przesyłanie informacji o stanie agentów, takich jak aktualna sygnatura i wersje składników Aby uzyskać więcej informacji, patrz *Serwer Przekaźnika Krawędziowego na stronie 16-2*.
Przesyłanie próbek podejrzanych plików	W celu rozszerzenia integracji z usługą Deep Discovery Virtual Analyzer Agenci OfficeScan mogą teraz wykrywać i przesyłać podejrzane pliki, które mogą zawierać wcześniej nieznane zagrożenia, bezpośrednio do usługi Virtual Analyzer w celu wykonania dalszej analizy. Po zweryfikowaniu występowania zagrożenia następuje natychmiastowa aktualizacja listy podejrzanych obiektów oraz jej synchronizacja ze wszystkimi agentami, co zapobiega rozprzestrzenianiu się zagrożenia w sieci. Aby uzyskać więcej informacji, patrz *Przesyłanie próbek na stronie 8-10*.
Ulepszenia interfejsu użytkownika pulpitu	Interfejs pulpitu został zmodyfikowany, aby zapewnić lepszy wgląd w stan ochrony sieci.
Rozszerzona integracja z programem Control Manager	Aby zapobiec nieautoryzowanej komunikacji między programem Control Manager a serwerami OfficeScan, rejestracja na serwerze Control Manager wymaga uwierzytelniania certyfikatem, a zarządzania regułami przez serwer Control Manager odbywa się przy użyciu szyfrowania kluczem publicznym. Aby uzyskać więcej informacji, patrz *Autoryzacja certyfikatu serwera Control Manager na stronie 14-30*.

FUNKCJA	OPIS
Ochrona przed programami wykorzystującymi luki	Skanowanie w czasie rzeczywistym umożliwia wykrywanie i blokowanie zagrożeń, które wykorzystują luki CVE (Common Vulnerabilities and Exposures). Aby uzyskać więcej informacji, patrz *Ustawienia skanowania na stronie 7-31*. Także monitorowanie zachowania może wykrywać nietypowe zachowanie programu, które jest typowe dla ataków wykorzystujących luki. Aby uzyskać więcej informacji, patrz *Ochrona przed programami wykorzystującymi luki na stronie 9-5*.
Ulepszenia funkcji Podejrzane połączenia	Teraz można skonfigurować funkcję Podejrzane połączenia w celu rejestrowania lub blokowania połączeń sieciowych wykrytych przez globalną listę adresów IP C&C i funkcję rejestrowania połączenia przy użyciu pakietu identyfikacyjnego złośliwej sieci. Aby uzyskać więcej informacji, patrz *Konfigurowanie ustawień podejrzanego połączenia na stronie 8-7*.
Ulepszenia zapory	Filtr aplikacji zapory programu OfficeScan obsługuje teraz system Windows 8 i nowsze wersje. Użytkownikom Agenci OfficeScan można przyznać uprawnienie do konfigurowania poziomu zabezpieczeń i listy wyjątków. Aby uzyskać więcej informacji, patrz *Dodawanie profilu zapory na stronie 13-21*.
Tryb niezależny	Tryb “mobilny” nosi teraz nazwę trybu “niezależnego”. Aby uzyskać więcej informacji, patrz *Stan połączenia agenta na stronie 2-46*.

FUNKCJA	OPIS
Obsługa platform i przeglądarek	Ta wersja programu OfficeScan obsługuje: • Microsoft™Windows™ Server 2016 **Uwaga** W tej wersji programu OfficeScan wycofano obsługę serwera Web Apache.

Kluczowe funkcje i korzyści

Program OfficeScan zawiera następujące funkcje i zapewnia następujące korzyści:

TABELA 1-1. Kluczowe funkcje i korzyści

FUNKCJA	KORZYŚCI
Ochrona przed oprogramowaniem typu ransomware	Rozszerzone funkcje skanowania mogą identyfikować i blokować programy ransomware atakujące dokumenty uruchamiane na punktach końcowych przez identyfikację typowych zachowań i blokowanie procesów typowo związanych z takimi programami.
Aktywna obrona przed zagrożeniami	Program OfficeScan można skonfigurować do subskrybowania list podejrzanych obiektów z serwera Control Manager. Za pomocą konsoli programu Control Manager można utworzyć niestandardowe operacje wykonywane na obiektach wykrytych na podstawie list podejrzanych obiektów w celu zapewnienia niestandardowej ochrony przed zagrożeniami zidentyfikowanymi przez punkty końcowe chronione przez produkty firmy Trend Micro właściwe dla danego środowiska. Możesz skonfigurować agentów OfficeScan w celu przesyłania obiektów plikowych, które mogą zawierać wcześniej niezidentyfikowane zagrożenia, do usługi Virtual Analyzer w celu przeprowadzenia dalszej analizy. Po dokonaniu oceny obiektów usługa Virtual Analyzer dodaje wszystkie obiekty z nieznanymi zagrożeniami do list podejrzanych obiektów usługi Virtual Analyzer, a następnie rozsyła te listy do innych agentów OfficeScan w sieci.

Funkcja	Korzyści
Program Plug-in Manager i rozwiązania dodatków	Program Plug-in Manager zapewnia instalację, wdrożenie i zarządzanie rozwiązaniami dodatków. Administratorzy mogą instalować dwa rodzaje rozwiązań dodatków: • Programy dodatków • Natywne funkcje programu OfficeScan
Scentralizowane zarządzanie	Oparta na sieci Web konsola zarządzania zapewnia administratorom przejrzysty dostęp do wszystkich agentów i serwerów w sieci. Konsola Web koordynuje automatyczną instalację reguł zabezpieczeń, plików sygnatur i aktualizacji oprogramowania na każdym agencie i serwerze. Dzięki usługom ochrony przed epidemią zamyka wektory infekcji i szybko wdraża dostosowane do ataku reguły zabezpieczeń, aby zapobiec wybuchowi epidemii lub ją izolować zanim będą dostępne pliki sygnatur. Program OfficeScan przeprowadza także monitorowanie w czasie rzeczywistym, udostępnia powiadomienia o zdarzeniach i dostarcza wszechstronne raporty. Administratorzy mogą prowadzić administrację zdalną, ustalać niestandardowe reguły dla poszczególnych komputerów lub grup i blokować ustawienia zabezpieczeń agenta.

Funkcja	Korzyści
Ochrona przed zagrożeniami bezpieczeństwa	W celu ochrony komputerów przed zagrożeniami program OfficeScan skanuje pliki i wykonuje określone czynności przy każdym wykrytym zagrożeniu bezpieczeństwa. Bardzo duża liczba zagrożeń bezpieczeństwa wykrytych w krótkim przedziale czasu sugeruje epidemię. Aby odizolować epidemię, program OfficeScan wdraża zasady ochrony przed epidemią i izoluje zarażone komputery tak długo, aż zagrożenia zostaną usunięte. W celu zwiększenia wydajności skanowania program OfficeScan używa technologii Smart Scan. Ta technologia działa w taki sposób, że przerzuca dużą ilość sygnatur zmagazynowanych wcześniej na lokalnym punkcie końcowym na źródła programu Smart Protection. Pozwala to znacząco zmniejszyć obciążenie komputerów i sieci przez stale rosnącą liczbę aktualizacji sygnatur. Informacje o rozwiązaniu Smart Scan i sposobach jego instalacji na agentach zawiera temat *Typy metod skanowania na stronie 7-9*.
Usługi Usuwania Szkód Services	Usługi Usuwania Szkód Services™ usuwają z komputerów wirusy oparte na plikach i wirusy sieciowe, a także pozostałości wirusów i robaków (trojany, wpisy w rejestrze, zainfekowane pliki) w ramach całkowicie zautomatyzowanego procesu. W celu usunięcia zagrożeń i niedogodności będących wynikiem obecności trojanów usługa Usuwania Szkód Services wykonuje następujące czynności: • Wykrywa i usuwa aktywne trojany • Przerywa procesy tworzone przez trojany • Naprawia pliki systemowe, zmodyfikowane przez trojany • Usuwa pliki i aplikacje pozostawione przez trojany Ponieważ Usługi Usuwania Szkód Services są automatycznie uruchamiane w tle, nie trzeba ich konfigurować. Użytkownicy nie zdają sobie nawet sprawy, że usługa jest uruchomiona. Program OfficeScan może jednak czasami powiadomić użytkownika o konieczności ponownego uruchomienia punktu końcowego w celu zakończenia procesu usuwania trojana.

Funkcja	Korzyści
Usługa Web Reputation	Usługa Web Reputation zapewnia agentom znajdującym się wewnątrz sieci korporacyjnej i poza nią ochronę zapobiegawczą przed złośliwymi i potencjalnie niebezpiecznymi stronami internetowymi. Dzięki przerwaniu łańcucha infekcji usługa Web Reputation zapobiega pobieraniu złośliwego kodu. Integracja programu OfficeScan z serwerem Smart Protection lub siecią Trend Micro Smart Protection Network pozwala sprawdzić wiarygodność stron i witryn internetowych.
Zapora programu OfficeScan	Zapora programu OfficeScan chroni agentów i serwery w sieci korzystając z kontroli stanowej — wysoce skutecznego skanowania wirusów sieciowych. Można tworzyć zasady filtrowania połączeń na podstawie aplikacji, adresu IP, numeru portu lub protokołu, a następnie zastosować te zasady do różnych grup użytkowników.
Zapobieganie utracie danych	Funkcja Zapobieganie utracie danych chroni zasoby cyfrowe organizacji przed przypadkowymi lub celowymi wyciekami. Funkcja Zapobieganie utracie danych umożliwia administratorom: • Identyfikację zasobów cyfrowych wymagających ochrony. • Tworzenie reguł ograniczających lub uniemożliwiających przesyłanie zasobów cyfrowych przez typowe kanały transmisji, takie jak wiadomości e-mail i urządzenia zewnętrzne. • Zapewnianie zgodności z określonymi standardami ochrony prywatności.
Kontrola urządzeń	Kontrola urządzeń zapewnia dostęp do zewnętrznych urządzeń pamięci masowej oraz do zasobów sieciowych połączonych z komputerami. Funkcja kontroli urządzeń ułatwia zapobieganie utracie i wyciekowi danych oraz, w połączeniu z funkcją skanowania plików, wzmacnia ochronę przed zagrożeniami bezpieczeństwa.
Monitorowanie zachowań	Funkcja monitorowania zachowań stale monitoruje agentów w poszukiwaniu nietypowych modyfikacji systemu operacyjnego i zainstalowanego oprogramowania.

Serwer OfficeScan

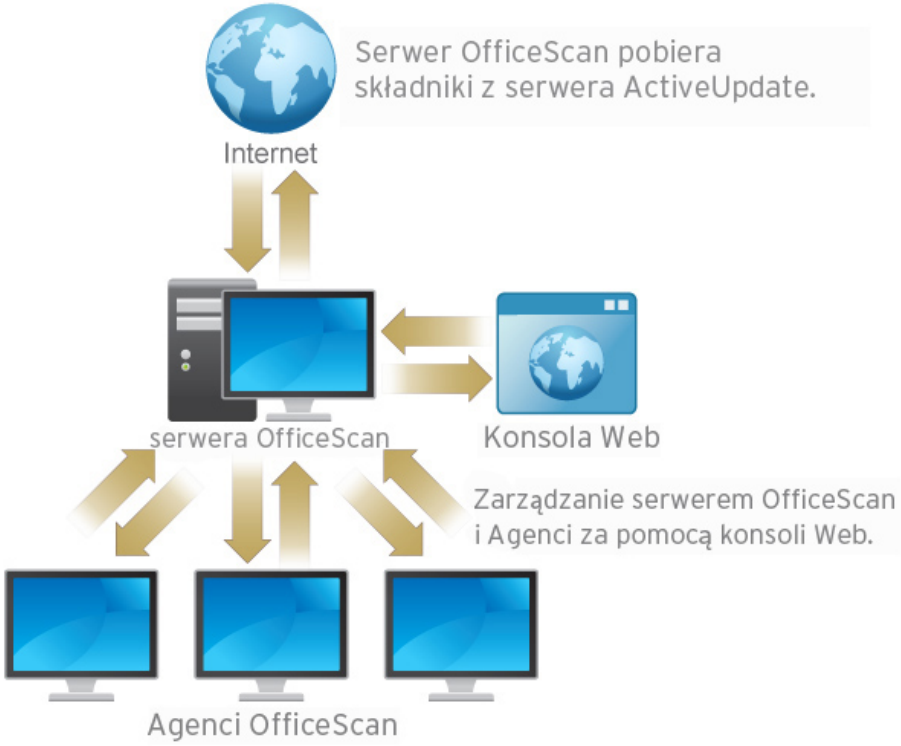
Serwer OfficeScan to centralny magazyn, w którym są przechowywane wszystkie dane konfiguracyjne agentów, dzienniki zagrożeń bezpieczeństwa i aktualizacje.

Serwer spełnia dwie istotne funkcje:

- Instaluje, monitoruje i zarządza agentami OfficeScan
- Pobiera większość składników wymaganych przez agentów Serwer OfficeScan pobiera składniki z serwera Trend Micro ActiveUpdate Server, a następnie rozsyła je do agentów.

Uwaga

Niektóre składniki są pobierane ze źródeł Smart Protection. Szczegółowe informacje można znaleźć w części *Źródła Smart Protection na stronie 4-6*.



ILUSTRACJA 1-1. Działanie serwera OfficeScan

Serwer OfficeScan zapewnia dwukierunkową komunikację w czasie rzeczywistym pomiędzy serwerem a agentami OfficeScan. Agentami można zarządzać za pomocą konsoli Web opartej na przeglądarce, umożliwiającej administratorom dostęp z dowolnego miejsca w sieci. Serwer komunikuje się z agentem (a agent z serwerem) za pomocą protokołu Hypertext Transfer Protocol (HTTP).

Agent OfficeScan

Komputery pracujące w systemie Windows należy chronić przed zagrożeniami bezpieczeństwa, instalując na każdym punkcie końcowym agenta OfficeScan.

Agent OfficeScan podlega serwerowi nadrzędnemu, z poziomu którego został zainstalowany. Aby agenci podlegali innemu serwerowi, należy ich odpowiednio skonfigurować za pomocą narzędzia Agent Mover. Agent przesyła do serwera informacje o zdarzeniach i stanie w czasie rzeczywistym. Przykłady zdarzeń to wykrycie wirusa/złośliwego oprogramowania, uruchomienie agenta, zamknięcie agenta, rozpoczęcie skanowania i zakończenie aktualizacji.

Integracja z produktami i usługami firmy Trend Micro

Program OfficeScan integruje się z produktami i usługami firmy Trend Micro wymienionymi w poniższej tabeli. Aby zapewnić płynną integrację, należy upewnić się, że produkty mają wymagane lub zalecane wersje.

TABELA 1-2. Produkty i usługi integrujące się z programem OfficeScan

PRODUKT/ USŁUGA	OPIS	WERSJA
Serwer ActiveUpdate	Zapewnia wszystkie składniki wymagane przez program Agent OfficeScan w celu ochrony punktów końcowych przed zagrożeniami bezpieczeństwa	Nie dotyczy
Smart Protection Network	Zapewnia usługi File Reputation Services i Web Reputation Services dla agentów. Sieć Smart Protection Network jest obsługiwana przez firmę Trend Micro.	Nie dotyczy

PRODUKT/ USŁUGA	OPIS	WERSJA
Oddzielny Serwer Smart Protection	Zapewnia analogiczne usługi File Reputation Services i Web Reputation Services jak sieć Smart Protection Network. Oddzielny Serwer Smart Protection umożliwia umieszczenie usług w sieci firmowej w celu zapewnienia optymalnej wydajności. **Uwaga** Zintegrowany Serwer Smart Protection jest instalowany wraz z serwerem OfficeScan. Zapewnia identyczne funkcje jak oddzielny serwer, ale ma ograniczoną pojemność.	• 3.0
Control Manager	Rozwiązanie do zarządzania oprogramowaniem, które umożliwia kontrolę nad programami antywirusowymi i służącymi do zabezpieczania zawartości z jednego miejsca — niezależnie od fizycznej lokalizacji czy platformy programu.	• Wersja 6.0 z dodatkiem SP3 i poprawką 2 (zalecane) • 6.0 z dodatkiem SP3 • 6.0 z dodatkiem SP2 • 6.0 z dodatkiem SP1
Deep Discovery Analyzer	Usługa Deep Discovery zapewnia monitorowanie całej sieci przy użyciu niestandardowych piaskownic i odpowiedniej inteligencji czasu rzeczywistego, aby umożliwić wczesne wykrywanie ataków, szybkie powstrzymywania i dostarczanie niestandardowych aktualizacji zabezpieczeń, które natychmiast ulepszają ochronę przed dalszymi atakami.	5.1 i nowszy

Rozdział 2

Wprowadzenie do programu OfficeScan

W tym rozdziale opisano, jak rozpocząć pracę z programem OfficeScan i wstępnymi ustawieniami konfiguracji.

Rozdział składa się z następujących tematów:

Konsola Web

Konsola sieci Web to centralny punkt monitorowania programu OfficeScan w całej sieci firmowej. Konsola jest wyposażona w zestaw domyślnych ustawień i wartości, które można konfigurować w oparciu o wymagania bezpieczeństwa oraz specyfikacje.
W konsoli Web zastosowano standardowe technologie internetowe, takie jak JavaScript, CGI, HTML i HTTPS.

Uwaga

W konsoli Web można skonfigurować ustawienia limitu czasu. Patrz sekcja *Ustawienia konsoli Web na stronie 14-62*.

Za pomocą konsoli Web można wykonywać następujące operacje:

- zarządzanie agentami zainstalowanymi na komputerach w sieci,
- grupowanie agentów w logiczne domeny w celu jednoczesnej konfiguracji i zarządzania,
- konfigurowanie ustawień skanowania i inicjowanie skanowania ręcznego na jednym lub wielu komputerach pracujących w sieci,
- konfigurowanie powiadomień dotyczących zagrożeń bezpieczeństwa w sieci oraz przeglądanie dzienników przysłanych przez agentów,
- konfigurowanie kryteriów i powiadomień dotyczących epidemii,
- przekazywanie zadań administracyjnych konsoli Web do innych administratorów programu OfficeScan za pomocą skonfigurowanych ról i kont użytkowników.
- Należy się upewnić, że agenci są zgodni z wytycznymi zabezpieczeń.

Uwaga

Konsola Web nie obsługuje systemu Windows 8, 8.1, 10 lub Windows Server 2012 w trybie interfejsu użytkownika systemu Windows.

Wymagania dotyczące otwierania programu Web Console

Konsolę Web można otworzyć z dowolnego punktu końcowego w sieci, który spełnia następujące wymagania:

- procesor Intel™Pentium™ 300MHz lub odpowiednik
- 128MB pamięci RAM
- Co najmniej 30 MB wolnego miejsca na dysku
- Monitor obsługujący rozdzielczość 1366 x 768 przy 256 kolorach lub lepszy
- Obsługa przeglądarek internetowych:
  - Microsoft Internet Explorer™ w wersji 10.0 lub nowszej
  - Microsoft Edge
  - Chrome

Uwaga

Program OfficeScan podczas wyświetlania konsoli Web obsługuje tylko ruch HTTPS.

W przeglądarce internetowej (w pasku adresu) należy wpisać jeden z następujących adresów, w zależności od rodzaju instalacji serwera programu OfficeScan:

TABELA 2-1. Adresy URL konsoli OfficeScan Web

TYP INSTALACJI	URL
Z protokołem SSL w witrynie domyślnej	`https://<Nazwa FQDN lub adres IP serwera OfficeScan>/OfficeScan`
Z protokołem SSL w witrynie wirtualnej	`https://<adres FDQN lub IP serwera OfficeScan>:<numer portu>/OfficeScan`

Uwaga

W przypadku uaktualnienia programu OfficeScan z poprzedniej wersji pliki pamięci podręcznej przeglądarki internetowej oraz serwera proxy mogą uniemożliwić prawidłowe załadowanie konsoli Web programu OfficeScan. Należy wyczyścić pamięć podręczną przeglądarki internetowej oraz pamięć podręczną wszystkich serwerów proxy znajdujących się między serwerem OfficeScan a punktem końcowym, na którym będzie uruchamiana konsola Web.

Konto logowania

Podczas instalacji serwera OfficeScan program instalacyjny tworzy konto główne i żąda wpisania hasła dla tego konta. Podczas pierwszego otwierania konsoli Web jako nazwę użytkownika należy wpisać „root" oraz wprowadzić ustalone wcześniej hasło. W przypadku zapomnienia hasła należy się skontaktować z pomocą techniczną w celu uzyskania pomocy dotyczącej ponownego ustawienia hasła.

Aby umożliwić użytkownikom dostęp do konsoli Web bez konieczności korzystania z konta głównego, należy zdefiniować role użytkowników i skonfigurować konta użytkowników. Logując się w konsoli, użytkownicy będą mogli korzystać z utworzonych dla nich kont. Aby uzyskać więcej informacji, patrz *Administracja oparta na rolach na stronie 14-3*.

Baner konsoli Web

Obszar banera konsoli Web zapewnia następujące opcje:

ILUSTRACJA 2-1. Obszar banera konsoli Web

- **<nazwa konta>**: By zmodyfikować szczegóły konta, takie jak hasło, kliknij nazwę konta (np. główny).
- **Wyloguj**: wylogowanie użytkownika z konsoli Web.

Uzyskiwanie pomocy

Menu **Pomoc** zapewnia dostęp do następujących informacji pomocy technicznej:

- **Materiały &i spis treści**: otwiera pomoc elektroniczną
- **Co nowego**: wyświetla informacje o niektórych nowych, ważnych funkcjach w tej wersji
- **Wsparcie**: wyświetla stronę internetową pomocy technicznej firmy Trend Micro, która umożliwia przesyłanie pytań i szukanie odpowiedzi na często zadawane pytania dotyczące produktów Trend Micro.
- **Encyklopedia zagrożeń**: wyświetla stronę internetową Encyklopedia zagrożeń, która stanowi repozytorium firmy Trend Micro zawierające informacje dotyczące złośliwego oprogramowania. Eksperci firmy Trend Micro od zagrożeń regularnie publikują informacje o wykrytym złośliwym oprogramowaniu, spamie, złośliwych adresach URL i lukach w zabezpieczeniach. Encyklopedia zagrożeń przedstawia także ataki internetowe na dużą skalę i powiązane informacje.
- **Kontakt z firmą Trend Micro**: Wyświetla stronę internetową **Skontaktuj się z nami**, która zawiera informacje o biurach firmy Trend Micro na całym świecie.
- **Informacje**: Udostępnia przegląd produktu, instrukcje sprawdzania szczegółów wersji składników oraz łącze do systemu Inteligentny system wspierający.

  Szczegółowe informacje zawiera sekcja *Inteligentny system wspierający na stronie 18-2*.

Pulpit

Ekran **Pulpit** pojawia się po otwarciu konsoli Web programu OfficeScan lub kliknięciu polecenia **Pulpit** w menu głównym.

Każde konto użytkownika konsoli Web ma całkowicie niezależny pulpit. Wszelkie zmiany dokonane w ustawieniach pulpitu dla danego konta użytkownika nie wpłyną na pulpity innych kont użytkowników.

Jeśli pulpit zawiera dane agenta OfficeScan, wyświetlane dane są zależne od uprawnień konta użytkownika do domeny agentów. Jeśli na przykład przyznano uprawnienia konta

użytkownika do zarządzania domenami A i B, pulpit konta użytkownika będzie wyświetlać tylko dane agentów należących do domen A i B.

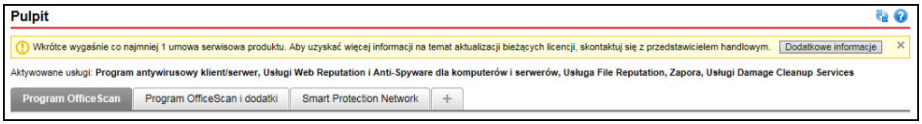
Szczegółowe informacje o kontach użytkowników zawiera temat *Administracja oparta na rolach na stronie 14-3*.

Ekran **Pulpit** zawiera następujące elementy:

- Sekcja Stan licencji produktu
- Element widget
- Karty

Sekcja Stan licencji produktu

Ta sekcja znajduje się na górze pulpitu i przedstawia stan licencji na produkt OfficeScan.



ILUSTRACJA 2-2. Sekcja Stan licencji produktu

Przypomnienia dotyczące stanu licencji są wyświetlane w następujących przypadkach:

- Jeśli użytkownik dysponuje licencją na pełną wersję:
  - 60 dni przed wygaśnięciem licencji
  - Podczas okresu próbnego korzystania z produktu. Czas trwania okresu próbnego różni się w zależności od regionu. Informacje na ten temat można uzyskać u przedstawiciela firmy Trend Micro.
  - Po wygaśnięciu licencji i upływie okresu próbnego. W tym okresie nie ma możliwości korzystania z pomocy technicznej ani dokonywania aktualizacji składników. Silniki skanowana będą jednak skanować komputery, używając nieaktualnych składników. Te nieaktualne składniki mogą nie zapewniać pełnej ochrony przed najnowszymi zagrożeniami bezpieczeństwa.

- Jeśli użytkownik dysponuje licencją na wersję próbną:
  - 14 dni przed wygaśnięciem licencji
  - Po wygaśnięciu licencji. W tym okresie program OfficeScan wyłącza aktualizację składników, skanowanie i wszystkie funkcje agenta.

Po otrzymaniu kodu aktywacyjnego odnów licencję, przechodząc do opcji **Administracja** > **Ustawienia** > **Licencja produktu**.

Paski informacji o produkcie

Program OfficeScan wyświetla na górze ekranu **Pulpit** różne komunikaty, które zawierają dodatkowe informacje dla administratorów.

Wyświetlane są m.in. następujące informacje:

- Najnowsze dodatki Service Pack lub poprawki dostępne dla programu OfficeScan

Uwaga

Kliknij polecenie **Więcej informacji**, aby pobrać poprawkę z Centrum pobierania firmy Trend Micro (http://downloadcenter.trendmicro.com/index.php?regs=PL).

- Dostępne nowe widgety
- Powiadomienia o umowie serwisowej, gdy zbliża się data wygaśnięcia umowy
- Powiadomienia trybu oceny
- Powiadomienia o autentyczności

Uwaga

W przypadku, gdy licencja programu OfficeScan nie jest oryginalna, pojawia się komunikat informacyjny. Jeśli nie uzyskasz oryginalnej licencji, program OfficeScan wyświetli ostrzeżenie i przerwie wykonywanie aktualizacji.

Karty i widgety

Widgety stanowią główne składniki pulpitu. Widgety dostarczają określonych informacji dotyczących różnych zdarzeń związanych z zabezpieczeniami. Niektóre widgety umożliwiają wykonywanie pewnych zadań, takich jak aktualizacja nieaktualnych składników.

Informacje wyświetlane przez widgety pochodzą z następujących źródeł:

- OfficeScan Serwer i agenci
- Rozwiązania dodatków i ich agenci
- Trend Micro Smart Protection Network

Uwaga

Aby wyświetlać dane z sieci Smart Protection Network, należy włączyć funkcję Smart Feedback. Szczegółowe informacje dotyczące funkcji Smart Feedback zawiera temat *Smart Feedback na stronie 14-67*.

Karty stanowią kontenery dla widgetów. Ekran **Pulpit** obsługuje do 30 kart.

Praca z kartami

Kartami można zarządzać poprzez dodawanie, zmienianie nazw, zmienianie układu, usuwanie i automatyczne przełączanie między widokami kart.

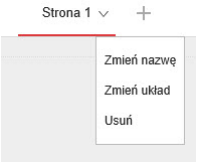
Procedura

1. Przejdź do pozycji **Pulpit**.
2. Aby dodać nową kartę:
   a. Kliknij ikonę dodawania.

b. Wpisz nazwę nowej karty.

3. Aby zmienić nazwę karty:

a. Umieść wskaźnik myszy na nazwie karty i kliknij strzałkę w dół.



b. Kliknij opcję **Zmień nazwę** i wpisz nową nazwę karty.

4. Aby zmienić układ widgetów na karcie:

a. Umieść wskaźnik myszy na nazwie karty i kliknij strzałkę w dół.

b. Kliknij opcję **Zmień układ**.

c. Wybierz nowy układ na wyświetlonym ekranie.

d. Kliknij przycisk **Zapisz**.

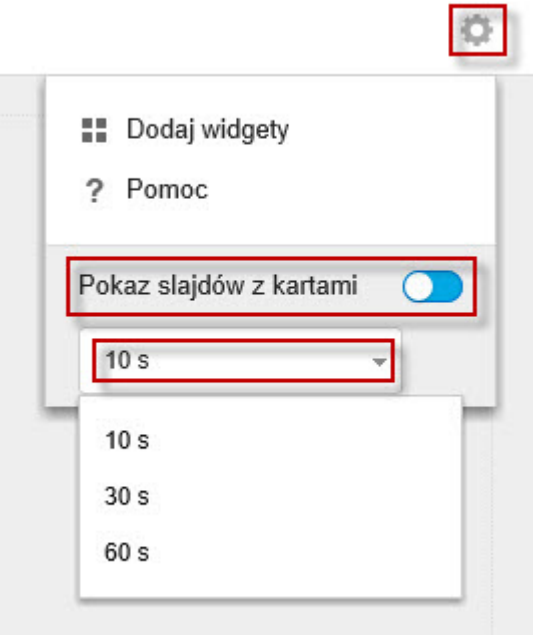
5. Aby usunąć kartę:

a. Umieść wskaźnik myszy na nazwie karty i kliknij strzałkę w dół.

b. Kliknij opcję **Usuń** i potwierdź.

6. Aby odtworzyć pokaz slajdów z kartami:

a. Kliknij przycisk **Ustawienia** po prawej stronie wyświetlanych kart.



b. Włącz opcję **Pokaz slajdów z kartami**.

c. Wybierz czas wyświetlania poszczególnych kart przed przełączeniem na następną kartę.

Praca z widgetami

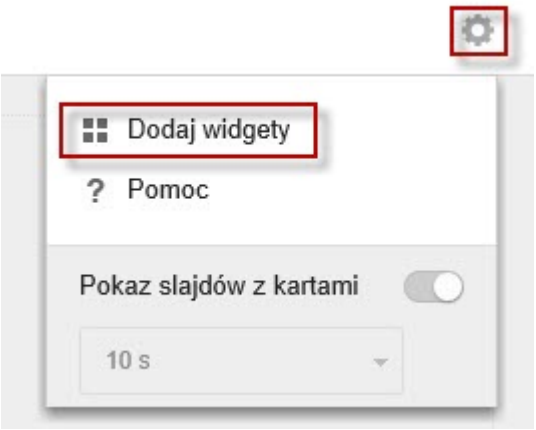
Widgetami można zarządzać poprzez dodawanie, przenoszenie, zmienianie rozmiaru, zmienianie nazw i usuwanie elementów.

Procedura

1. Przejdź do pozycji **Pulpit**.
2. Kliknij kartę.

3. Aby dodać widget:

   a. Kliknij przycisk **Ustawienia** po prawej stronie wyświetlanych kart.



   b. Kliknij opcję **Dodaj widgety**.

   c. Wybierz widgety do dodania.

      - Wybierz kategorię z listy rozwijanej nad widgetami, aby zawęzić dostępne opcje.
      - Użyj tekstowego pola wyszukiwania na górze ekranu, aby wyszukać określony widget.

   d. Kliknij przycisk **Dodaj**.

4. Aby przenieść widget w nowe miejsce na tej samej karcie, przeciągnij i upuść widget w nowe miejsce.

5. Rozmiar widgetów na karcie z wieloma kolumnami można zmienić, umieszczając kursor na prawą krawędzią widgetu, a następnie przesuwając kursor w lewo lub w prawo.

6. Aby zmienić nazwę widgetu:

   a. Kliknij ikonę ustawień (>).

b. Wpisz nowy tytuł.

Uwaga

W przypadku niektórych widgetów, takich jak widget **Informacje z programu OfficeScan i dodatków**, można zmodyfikować niektóre elementy związane z widgetem.

c. Kliknij przycisk **Zapisz**.

7. Aby usunąć widget, kliknij ikonę usuwania (>).

Widgety karty Podsumowanie

Karta **Podsumowanie** zawiera przegląd stanu zabezpieczeń wszystkich Agenci OfficeScan w sieci.

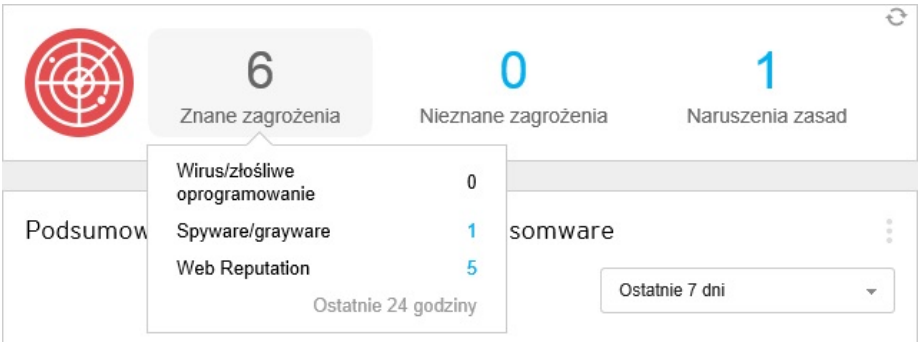
Uwaga

Nie można dodawać, usuwać ani modyfikować widgetów wyświetlanych na karcie **Podsumowanie**.

Dostępne widgety:

- *Widget Wykryte ogólne zagrożenia i naruszenia reguł na stronie 2-13*
- *Widget stan punktu końcowego na stronie 2-14*
- *Widget Wykryte zagrożenia bezpieczeństwa w czasie na stronie 2-20*

Widget Wykryte ogólne zagrożenia i naruszenia reguł



Ten widget zawiera przegląd wszystkich wykrytych zagrożeń i naruszeń reguł w całej sieci w ciągu ostatnich 24 godzin.

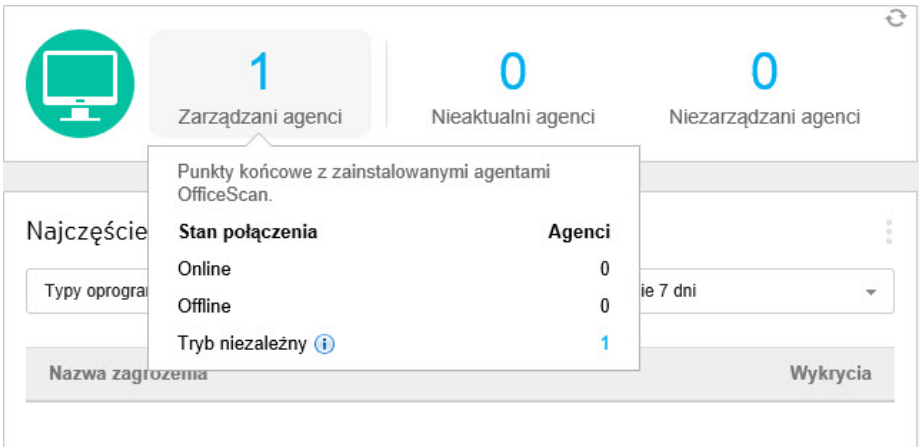
Przesuń wskaźnik myszy na liczbę zagrożeń lub naruszeń, aby wyświetlić podział określonych typów wykrytych zagrożeń, które wystąpiły w poszczególnych grupach. Aby wyświetlić dzienniki dla określonej funkcji, kliknij liczbę po prawej stronie.

TABELA 2-2. Kategorie wykrytych zagrożeń

KATEGORIA	OPIS
Znane zagrożenia	Wyświetla wszystkie funkcje, które wykrywają zagrożenia bezpieczeństwa potwierdzone przez firmę Trend Micro • Wirusy/złośliwe oprogramowanie • program szpiegujący/grayware • Usługa Web Reputation

KATEGORIA	OPIS
Nieznane zagrożenia	Wyświetla wszystkie funkcje, które wykrywają potencjalne zagrożenia przy użyciu zaawansowanej heurystyki, analizy lub modelowania funkcji • Predykcyjne uczenie maszynowe • Monitorowanie zachowania • Podejrzane połączenia • Podejrzane pliki/obiekty
Naruszenia zasad	Wyświetla wszystkie funkcje, które zawierają naruszenia reguł odnoszących się do firmowych standardów bezpieczeństwa • Zapora • Kontrola urządzeń • Zapobieganie utracie danych

Widget stan punktu końcowego



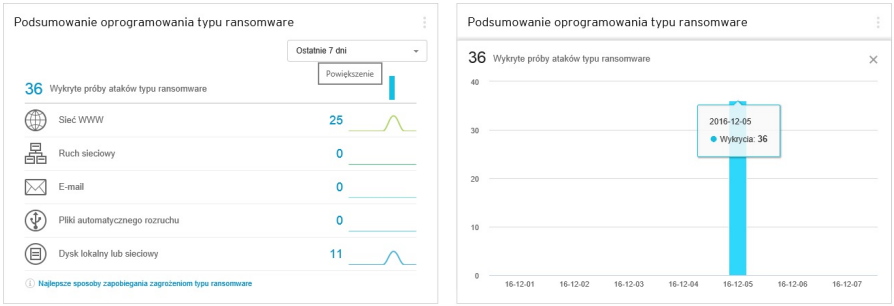
Ten widget zawiera przegląd stanu połączenia i aktualizacji Agenci OfficeScan w sieci, a także najnowszą liczbę zgodności z zabezpieczeniami dla niezarządzanych punktów końcowych, które nie podlegają serwerowi OfficeScan.

Przesuń wskaźnik myszy na liczbę, aby wyświetlić podział różnych stanów. Aby wyświetlić dzienniki dla określonego stanu, kliknij liczbę po prawej stronie.

TABELA 2-3. Grupy agentów/punktów końcowych

GRUPA	OPIS
Zarządzani agenci	Wyświetla ostatni zgłoszony stan połączenia Agenci OfficeScan w sieci • Online • Offline • Tryb niezależny
Nieaktualni agenci	Wyświetla listę kategorii składników i liczbę Agenci OfficeScan z nieaktualnym składnikiem w każdej kategorii
Niezarządzane punkty końcowe	Wyświetla listę wszystkich punktów końcowych, które program OfficeScan może wykryć, ale które nie mają zainstalowanego programu Agent OfficeScan lub które nie podlegają serwerowi OfficeScan **Uwaga** Aby upewnić się, że serwer OfficeScan regularnie aktualizuje liczbę niezarządzanych punktów końcowych: 1. Zdefiniuj zakres obiektów usługi Active Directory / adresów IP dla oceny. Aby uzyskać więcej informacji, patrz *Integracja usługi Active Directory na stronie 2-41*. 2. Skonfiguruj zaplanowaną ocenę. Aby uzyskać więcej informacji, patrz *Zgodność z zabezpieczeniami dla niezarządzanych punktów końcowych na stronie 15-74*.

Widget Podsumowanie oprogramowania typu ransomware



ILUSTRACJA 2-3. Domyślny widok przedstawiający wszystkie dane dotyczące oprogramowania typu ransomware oraz powiększony widok wykresu słupkowego "Wykryte próby ataków typu ransomware"

Ten widget zawiera przegląd wszystkich prób ataków z użyciem oprogramowania typu ransomware w określonym przedziale czasu.

Widok domyślny przedstawia podsumowanie wszystkich wykrytych zagrożeń typu ransomware i wykonuje ich dalszą kategoryzację na podstawie kanału zarażenia.

- Kliknij licznik wykrywania oprogramowania typu ransomware w widoku domyślnym, aby otworzyć ekran dzienników **Zagrożenia bezpieczeństwa — oprogramowanie typu ransomware** ze szczegółami wykrytych zagrożeń typu ransomware.

Kliknij dowolny wykres po prawej stronie widgetu, aby wyświetlić powiększony widok danych wykresu.

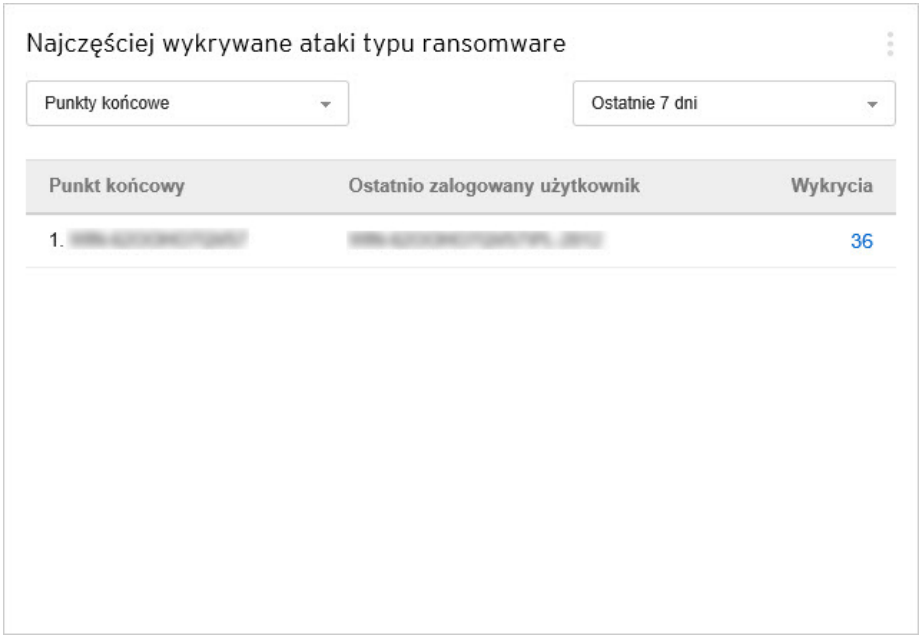
- Przesuń wskaźnik myszy na węzły dowolnego wybranego dnia, aby wyświetlić łączną liczbę wykrytych zagrożeń dla wyświetlanej kategorii wykrywania. Kliknij węzeł, aby przejść do ekranu dzienników **Zagrożenia bezpieczeństwa — oprogramowanie typu ransomware**, który przedstawia szczegóły wykrywania oprogramowania typu ransomware dla określonego dnia.

TABELA 2-4. Kanały wykrywania oprogramowania typu ransomware

KANAŁ	OPIS	WYKRYTO PRZEZ
Sieć Web	Pliki pobrane przy użyciu klienta sieci Web (takiego jak przeglądarka lub klient FTP)	• Usługa Web Reputation • Skanowanie w czasie rzeczywistym • Monitorowanie zachowania
Ruch sieciowy	Oprogramowanie typu ransomware wykryte przez funkcję Podejrzane połączenia	• Podejrzane połączenia
E-mail	Załączniki wiadomości e-mail otwarte przy użyciu programu Microsoft Outlook lub Windows Live Mail **Uwaga** Program OfficeScan klasyfikuje wszystkie załączniki otwarte przy użyciu innych aplikacji poczty e-mail do kanału **Dysk lokalny lub sieciowy**.	• Skanowanie w czasie rzeczywistym • Monitorowanie zachowania
Pliki automatycznego rozruchu	Programy znajdujące się na wymiennych urządzeniach pamięci masowej i uruchomione przy użyciu pliku autorun **Uwaga** Program OfficeScan klasyfikuje wszystkie inne pliki/programy, które nie zostały uruchomione przy użyciu programu autorun na wymiennych urządzeniach pamięci masowej, do kanału **Dysk lokalny lub sieciowy**.	• Skanowanie w czasie rzeczywistym • Monitorowanie zachowania

Kanał	Opis	Wykryto przez
Dysk lokalny lub sieciowy	Oprogramowanie typu ransomware wykryte na dyskach lokalnych lub sieciowych, w tym: • Załączniki wiadomości e-mail otwarte przy użyciu klientów e-mail innych niż Microsoft Outlook lub Windows Live Mail • Pliki na wymiennych urządzeniach pamięci masowej, które nie zostały uruchomione przez program autorun	• Skanowanie w czasie rzeczywistym • Skanowanie ręczne • Skanowanie zaplanowane • Skanuj teraz • Monitorowanie zachowania

Widget Najczęściej wykrywane ataki typu ransomware

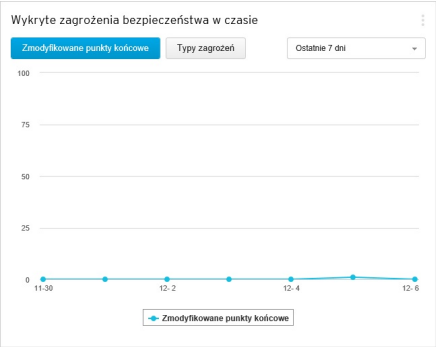


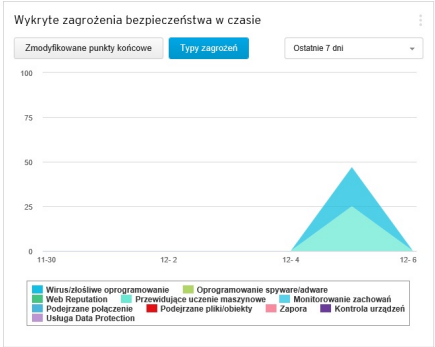
Ten widget zawiera przegląd najczęściej wykrywanych ataków z użyciem oprogramowania typu ransomware w określonym przedziale czasu.

Użyj menu rozwijanego, aby wybrać typ wyświetlanych danych dotyczących oprogramowania typu ransomware.

Wyświetl	Opis
Punkty końcowe	Przedstawia punkty końcowe z największą liczbą wykryć oprogramowania typu ransomware w sieci Kliknij licznik wykrywania oprogramowania typu ransomware, aby otworzyć ekran dzienników **Zagrożenia bezpieczeństwa — oprogramowanie typu ransomware** ze szczegółami wykrytych zagrożeń typu ransomware.
Typy oprogramowania ransomware	Przedstawia typy oprogramowania ransomware z największą liczbą wykryć w sieci Kliknij łącze **Nazwa zagrożenia**, aby otworzyć Encyklopedię zagrożeń firmy Trend Micro w celu uzyskania dalszych informacji dotyczących określonego typu zagrożenia.
Domeny	Przedstawia domeny oprogramowania ransomware z największą liczbą wykryć w sieci Kliknij łącze **Nazwa zagrożenia**, aby otworzyć Encyklopedię zagrożeń firmy Trend Micro w celu uzyskania dalszych informacji dotyczących określonej domeny.

Widget Wykryte zagrożenia bezpieczeństwa w czasie





Ten widget zawiera przegląd punktów końcowych w sieci wraz z danymi dotyczącymi wykrywania i typów zagrożeń mających wpływ na sieć w określonym przedziale czasu.

Kliknij przycisk **Zmodyfikowane punkty końcowe** lub **Typy zagrożeń**, aby przełączać się między różnymi widokami.

Wyświetl	Opis
Zmodyfikowane punkty końcowe	Przedstawia liczbę punktów końcowych z wykrytymi zagrożeniami lub naruszeniami reguł w określonym przedziale czasu Kliknij węzeł dowolnego wybranego dnia, aby przejść do ekranu **Zarządzanie agentami**, który wyświetla w drzewie agentów wszystkie zmodyfikowane punkty końcowe dla tego dnia.
Typy zagrożeń	Wyświetla wykres przedstawiający liczbę zagrożeń i naruszeń reguł, które zostały zarejestrowane w określonym przedziale czasu. • Kliknij nazwy typów zagrożeń na dole wykresu, aby wyświetlić/ukryć informacje o wykryciu na wykresie. • Przesuń wskaźnik myszy na węzły dowolnego wybranego dnia, aby wyświetlić łączną liczbę wykrytych zagrożeń dla wyświetlanych typów zagrożeń. Kliknij węzeł, aby przejść do ekranu dzienników dla typu zagrożenia wyróżnionego na liście.

Porada

Ten widget można dodać wielokrotnie, aby wyświetlić oba widoki. Podczas dodawania widgetów do innych kart można znaleźć ten widget w grupie widgetów typu **OfficeScan**.

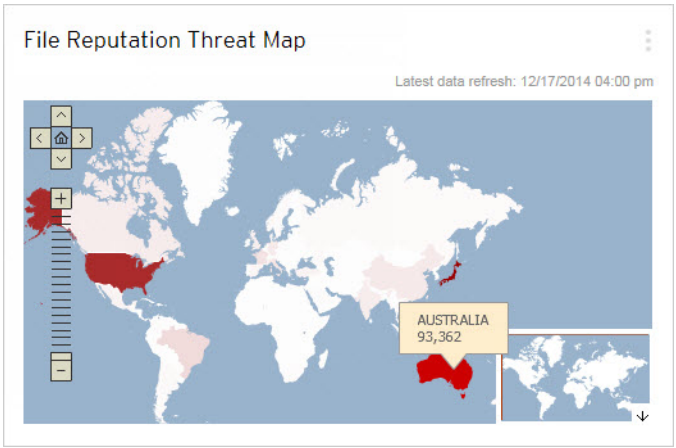
Widgety Smart Protection Network

Program OfficeScan zapewnia domyślną kartę zawierającą informacje pochodzące z sieci Trend Micro Smart Protection Network, która zapewnia usługi File Reputation Services i Web Reputation Services dla Agenci OfficeScan.

Dostępne widgety:

- *Widget Najczęstsze źródła zagrożeń usługi Web Reputation na stronie 2-23*
- *Widget Najbardziej zagrożeni użytkownicy usługi Web Reputation na stronie 2-22*
- *Widget Mapa zagrożeń usługi File Reputation na stronie 2-21*

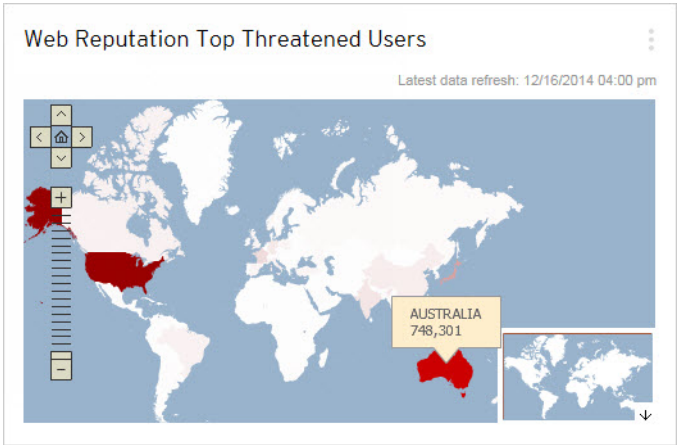
Widget Mapa zagrożeń usługi File Reputation



Ten widget wyświetla łączną liczbę zagrożeń bezpieczeństwa wykrytych przez usługi File Reputation Services. Informacje są wyświetlane na mapie świata według lokalizacji geograficznej.

Aby zobaczyć całkowitą liczbę zagrożeń bezpieczeństwa wykrytych w określonych regionach, umieść wskaźnik myszy na różnych regionach na mapie.

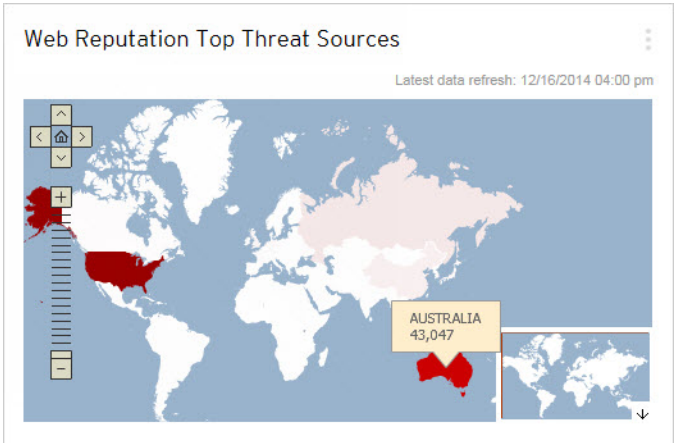
Widget Najbardziej zagrożeni użytkownicy usługi Web Reputation



Ten widget wyświetla liczbę użytkowników, na których wpłynęły złośliwe adresy URL wykryte przez usługi Web Reputation Services. Informacje są wyświetlane na mapie świata według lokalizacji geograficznej.

Aby zobaczyć całkowitą liczbę zaatakowanych użytkowników w danym regionie, umieść na nim wskaźnik myszy.

Widget Najczęstsze źródła zagrożeń usługi Web Reputation



Ten widget wyświetla łączną liczbę zagrożeń bezpieczeństwa wykrytych przez usługi Web Reputation Services. Informacje są wyświetlane na mapie świata według lokalizacji geograficznej.

Aby zobaczyć całkowitą liczbę zagrożeń bezpieczeństwa wykrytych w określonych regionach, umieść wskaźnik myszy na różnych regionach na mapie.

Widgety Ochrona danych

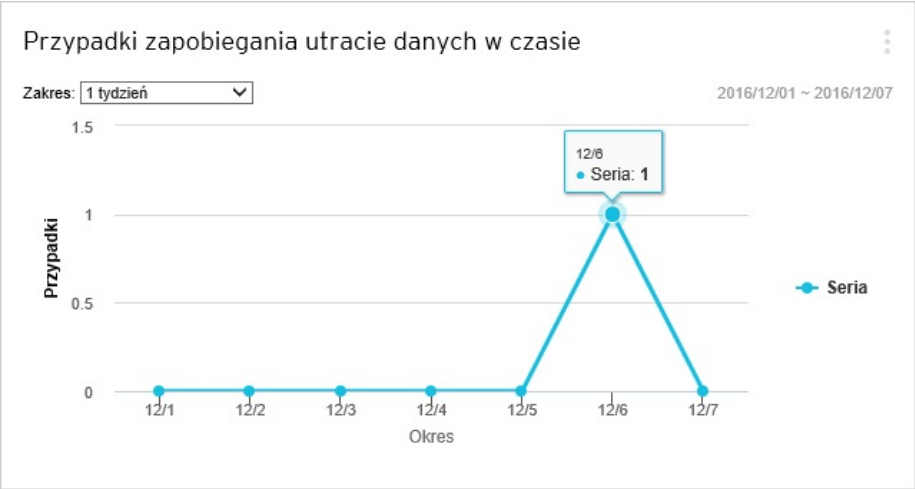
Uwaga

Widgety Ochrona danych są dostępne po aktywowaniu usługi Ochrona danych OfficeScan.

Dostępne widgety:

- *Widget Przypadki Zapobieganie utracie danych w czasie na stronie 2-24*
- *Widget Najważniejsze zdarzenia Zapobieganie utracie danych na stronie 2-25*

Widget Przypadki Zapobieganie utracie danych w czasie



Ten widget wyświetla ogólną liczbę zdarzeń Zapobieganie utracie danych w określonym przedziale czasu.

Uwaga

Liczba wykryć obejmuje wszystkie zdarzenia Zapobieganie utracie danych niezależnie od podjętego działania ("Zablokuj" lub "Zezwól").

Widget Najważniejsze zdarzenia Zapobieganie utracie danych

Ten widget przedstawia najczęstszych użytkowników, kanały, szablony lub punkty końcowe, które spowodowały zdarzenia Zapobieganie utracie danych w określonym przedziale czasu.

Uwaga

- Ten widget wyświetla maksymalnie 10 użytkowników, kanałów, szablonów lub punktów końcowych.
- Liczba wykryć obejmuje wszystkie zdarzenia Zapobieganie utracie danych niezależnie od podjętego działania ("Zablokuj" lub "Zezwól").

Wybierz typ danych funkcji Zapobieganie utracie danych do wyświetlenia przy użyciu menu rozwijanego **Wyświetl według**.

TABELA 2-5. Widoki Zapobieganie utracie danych

WYŚWIETL	OPIS
Użytkownik	Użytkownicy, którzy przesłali największą liczbę zasobów cyfrowych • Kliknij nazwy użytkowników na dole wykresu, aby wyświetlić/ukryć informacje o wykryciu na wykresie. • Przesuń wskaźnik myszy na paski wykrywania, aby wyświetlić nazwę użytkownika i liczbę zdarzeń Zapobieganie utracie danych dla tego użytkownika.
Kanał	najczęściej używane kanały do transmisji zasobów cyfrowych • Kliknij nazwy kanałów na dole wykresu, aby wyświetlić/ukryć informacje o wykryciu na wykresie. • Przesuń wskaźnik myszy na paski wykrywania, aby wyświetlić nazwę kanału i liczbę zdarzeń Zapobieganie utracie danych dla tego kanału.
Szablon	szablony zasobów cyfrowych, które spowodowały wykrycie największej liczby elementów • Kliknij nazwy szablonów na dole wykresu, aby wyświetlić/ukryć informacje o wykryciu na wykresie. • Przesuń wskaźnik myszy na paski wykrywania, aby wyświetlić nazwę szablonu i liczbę zdarzeń Zapobieganie utracie danych dla tego szablonu.
Punkty końcowe	Punkty końcowe, które przesłały największą liczbę zasobów cyfrowych • Kliknij nazwy punktów końcowych na dole wykresu, aby wyświetlić/ukryć informacje o wykryciu na wykresie. • Przesuń wskaźnik myszy na paski wykrywania, aby wyświetlić nazwę punktu końcowego i liczbę zdarzeń Zapobieganie utracie danych dla tego punktu końcowego.

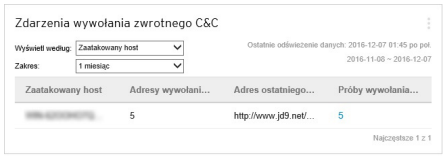
Widgety programu OfficeScan

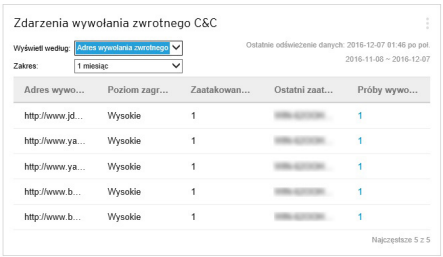
Widgety OfficeScan zapewniają szybki przegląd stanu zabezpieczeń i wykrytych zagrożeń Agent OfficeScan, informacje o dodatkach oraz informacje o występujących epidemiach.

Dostępne widgety:

- *Widget Zdarzenia wywołania zwrotnego C&C na stronie 2-27*
- *Widget Wykryte zagrożenia bezpieczeństwa na stronie 2-29*
- *Widget Informacje z programu OfficeScan i dodatków na stronie 2-30*
- *Widget Łączność agenta antywirusowego na stronie 2-31*
- *Widget Agenci połączeni z serwerem Przekaźnika Krawędziowego na stronie 2-33*
- *Widget Epidemie na stronie 2-34*
- *Widget Aktualizacje agenta na stronie 2-36*

Widget Zdarzenia wywołania zwrotnego C&C





Ten widget wyświetla wszystkie informacje o zdarzeniu wywołania zwrotnego C&C, w tym cel ataku i źródłowy adres wywołania zwrotnego.

Możesz wybrać wyświetlanie informacji o wywołaniu zwrotnym C&C z określonej listy serwerów C&C. Aby wybrać źródło listy (Global Intelligence, Virtual Analyzer), kliknij ikonę edycji (>) i wybierz listę z menu rozwijanego **Lista źródeł C&C**.

Użyj menu rozwijanego **Wyświetl według**, aby wybrać typ wyświetlanych danych wywołania zwrotnego C&C:

- **Zaatakowany host**: wyświetla najnowsze informacje C&C dla docelowego punktu końcowego

TABELA 2-6. Informacje o zaatakowanym hoście

KOLUMNA	OPIS
Zaatakowany host	Nazwa punktu końcowego będącego celem ataku C&C
Adresy wywołania zwrotnego	Liczba adresów wywołania zwrotnego, z którymi punkt końcowy próbował nawiązać kontakt
Adres ostatniego wywołania	Ostatni adres wywołania zwrotnego, z którym punkt końcowy próbował nawiązać kontakt
Próby wywołania zwrotnego	Liczba prób kontaktu docelowego punktu końcowego z adresem wywołania zwrotnego **Uwaga** Kliknij hiperłącze, aby otworzyć ekran **Dzienniki wywołania zwrotnego C&C** i wyświetlić bardziej szczegółowej informacje.

- **Adres wywołania zwrotnego**: wyświetla najnowsze informacje C&C dla adresu wywołania zwrotnego C&C

TABELA 2-7. Informacje o adresie C&C

KOLUMNA	OPIS
Adres wywołania zwrotnego	Adres wywołań zwrotnych C&C pochodzących z sieci
Poziom ryzyka C&C	Poziom zagrożenia adresu wywołania zwrotnego określony przez listę Global Intelligence lub Virtual Analyzer
Zaatakowane hosty	Liczba punktów końcowych, których celem był adres wywołania zwrotnego

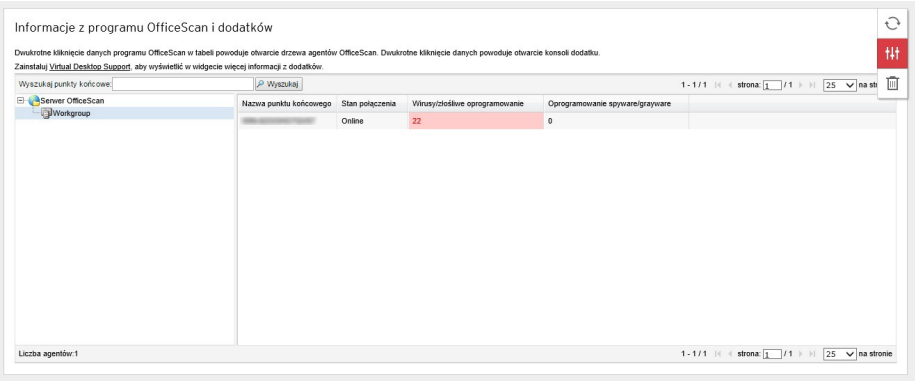
Kolumna	Opis
Ostatni zaatakowany host	Nazwa punktu końcowego, który jako ostatni próbował skontaktować się z adresem wywołania zwrotnego C&C
Próby wywołania zwrotnego	Liczba wykonanych prób wywołania zwrotnego wykonanych dla adresu z sieci **Uwaga** Kliknij hiperłącze, aby otworzyć ekran **Dzienniki wywołania zwrotnego C&C** i wyświetlić bardziej szczegółowej informacje.

Widget Wykryte zagrożenia bezpieczeństwa

Ten widget pokazuje liczbę wykrytych zagrożeń bezpieczeństwa i liczbę zmodyfikowanych punktów końcowych

Kliknij liczbę punktów końcowych, aby otworzyć ekran **Zarządzanie agentami** z listą zmodyfikowanych Agenci OfficeScan w drzewie agentów.

Widget Informacje z programu OfficeScan i dodatków



Ten widget łączy dane z Agenci OfficeScan i zainstalowanych programów dodatków, a następnie wyświetla je w drzewie agentów. Ten widget pomaga szybko ocenić stan ochrony na agentach i zmniejszyć nakłady związane z zarządzaniem poszczególnymi programami dodatków.

Ten widget przedstawia dane z następujących programów dodatków:

- Trend Micro Virtual Desktop Support

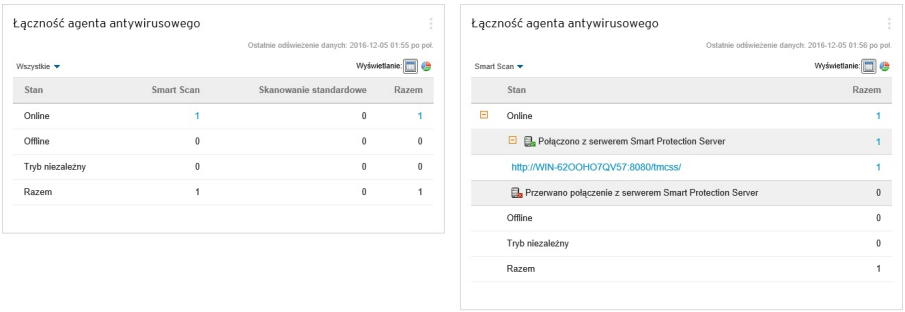
Ważne

Zanim widget Mashup wyświetli powiązane dane, należy aktywować obsługiwany program dodatku. Należy uaktualnić programy dodatków, jeśli dostępne są nowsze wersje.

Aby wybrać kolumny wyświetlane w drzewie agentów, kliknij przycisk **Więcej opcji** w prawym górnym rogu widgetu i kliknij przycisk **Ustawienia**.

Kliknij dane w dowolnej kolumnie, aby otworzyć konsolę odpowiedniego programu dodatku lub ekran **Zarządzanie agentami** OfficeScan. Wyświetlony ekran będzie zależny od typu kliknięty danych.

Widget Łączność agenta antywirusowego



ILUSTRACJA 2-4. Widok domyślny wyświetla wszystkich agentów Smart Scan i agentów skanowania standardowego oraz rozwinięty widok agentów Smart Scan z serwerami Smart Protection

Ten widget wyświetla stan połączenia Agenci OfficeScan z serwerem OfficeScan w odniesieniu do skonfigurowanej metody skanowania (skanowanie Smart Scan i standardowe).

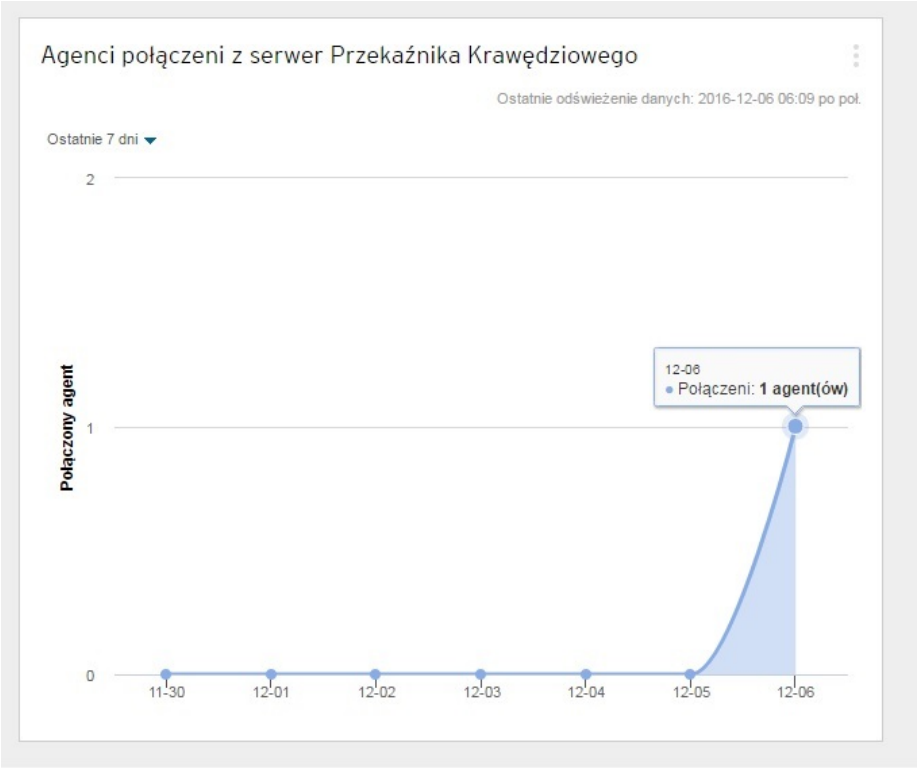
Dane można wyświetlać w tabeli lub na wykresie kołowym, klikając ikony wyświetlania ().

Użyj listy rozwijanej powyżej tabeli/wykresu, aby zmienić typ wyświetlanych danych. Kliknij liczbę dla dowolnego stanu, aby otworzyć ekran **Zarządzanie agentami** z listą powiązanych Agenci OfficeScan w drzewie agentów.

WYŚWIETL	OPIS
Wszystkie	Wyświetla stan połączenia wszystkich Agenci OfficeScan dla obu metod skanowania
Skanowanie standardowe	Wyświetla stan połączenia wszystkich Agenci OfficeScan, którzy używają metody skanowania standardowego.

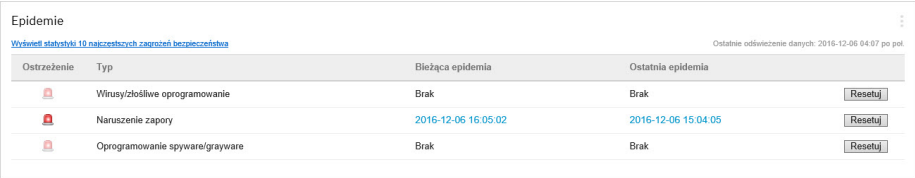
WYŚWIETL	OPIS
Smart Scan	Wyświetla stan połączenia wszystkich Agenci OfficeScan, którzy używają metody skanowania Smart Scan Podczas wyświetlania stanu połączenia agenta w tabeli: • Rozwiń informacje o agentach “online”, aby wyświetlić stan połączenia agentów z serwerem Smart Protection. • Kliknij adres URL, aby otworzyć konsolę zarządzania serwera Smart Protection.  **Uwaga** Tylko agenci online (podlegający serwerowi OfficeScan) mogą wysłać raport o stanie połączenia z serwerami Smart Protection. Aby przywrócić połączenie agenta offline z serwerem Smart Protection, patrz *Rozwiązywanie problemów wskazywanych przez ikony agentów OfficeScan na stronie 15-42*.

Widget Agenci połączeni z serwerem Przekaźnika Krawędziowego



Ten widget wyświetla liczbę Agenci OfficeScan połączonych z serwerem Przekaźnika Krawędziowego OfficeScan w określonym przedziale czasu.

Widget Epidemie

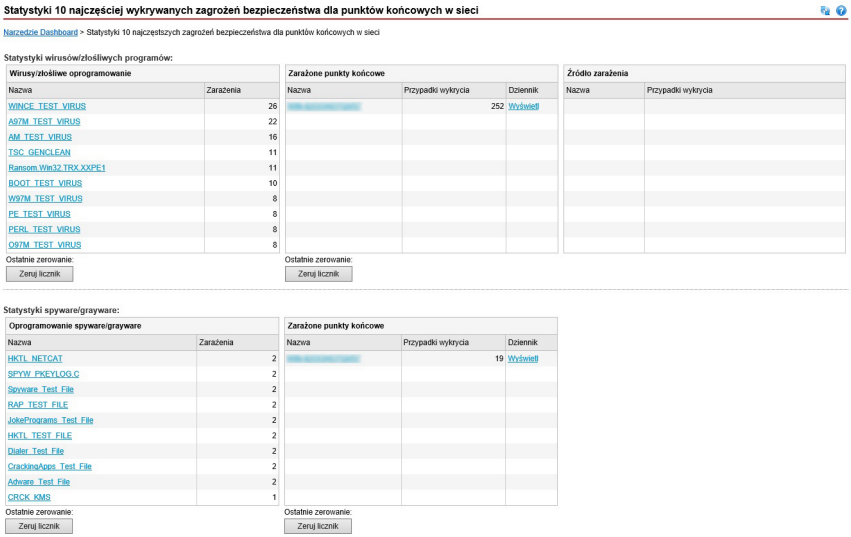


Widget **Epidemie** zawiera informacje o stanie bieżących epidemii zagrożeń bezpieczeństwa oraz ostatnie ostrzeżenie o epidemii.

- Kliknij łącze daty/godziny alarmu, aby wyświetlić więcej szczegółów dotyczących epidemii.
- Gry program OfficeScan wykryje epidemię można **zresetować** stan informacji ostrzeżenia o epidemii i natychmiast wprowadzić środki zapobiegające epidemii.

  Szczegółowe informacje dotyczące korzystania z funkcji zapobiegania epidemii zawiera temat *Reguły ochrony przed epidemią na stronie 7-124*.

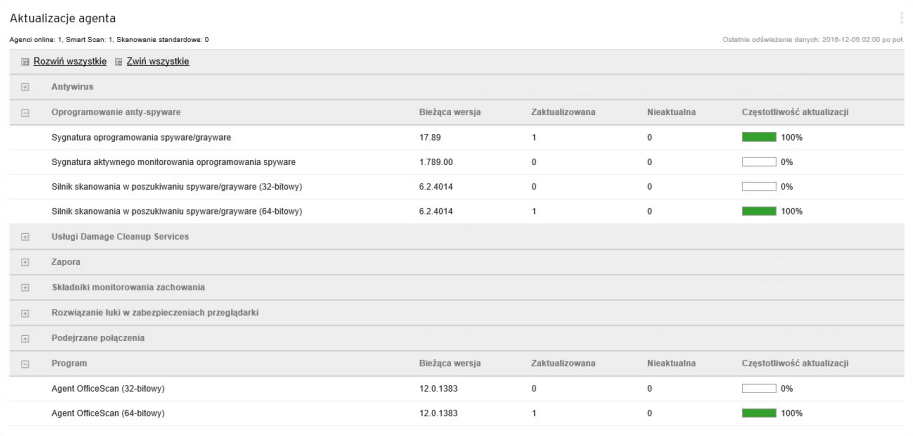
- Kliknij opcję **Wyświetl statystyki 10 najczęstszych zagrożeń bezpieczeństwa**, aby wyświetlić najczęściej występujące zagrożenia bezpieczeństwa, punkty końcowe z największą liczbą zagrożeń bezpieczeństwa oraz najczęstsze źródła zarażenia.



Na ekranie **Statystyki 10 najczęstszych zagrożeń bezpieczeństwa** można:

- Przeglądać szczegółowe informacje dotyczące zagrożeń dla bezpieczeństwa poprzez kliknięcie nazwy zagrożenia dla bezpieczeństwa.
- Przeglądać status ogólny danego punktu końcowego poprzez kliknięcie jego nazwy.
- Przeglądać dzienniki zagrożeń bezpieczeństwa dla tego punktu końcowego poprzez kliknięcie polecenia **Widok** odpowiadającego nazwie punktu końcowego.
- Skasować statystyki w każdej tabeli poprzez kliknięcie polecenia **Zeruj licznik**.

Widget Aktualizacje agenta



Ten widget wyświetla składniki i programy, które chronią Agenci OfficeScan przed zagrożeniami bezpieczeństwa.

Kliknij liczbę "Nieaktualni", aby otworzyć ekran **Zarządzanie agenta** z listą Agenci OfficeScan w drzewie agentów, które wymagają aktualizacji.

Widget Zarządzanie

Widget Zarządzanie wyświetla stan połączenia Agenci OfficeScan z serwerem OfficeScan.

Dostępne widgety:

- *Widget Łączność klient-serwer na stronie 2-37*

Widget Łączność klient-serwer

Ten widget przedstawia stan połączenia wszystkich agentów z serwerem OfficeScan.

Można przełączać się między tabelą a wykresem kołowym, klikając ikony wyświetlania ( ).

Kliknij liczbę dla dowolnego stanu, aby otworzyć ekran **Zarządzanie agentami** z listą powiązanych Agenci OfficeScan w drzewie agentów.

Narzędzie Server Migration Tool

Program OfficeScan zapewnia narzędzie Server Migration Tool, które umożliwia administratorom kopiowanie ustawień z wcześniejszej wersji programu OfficeScan do bieżącej wersji. Narzędzie Server Migration Tool migruje następujące ustawienia:

FUNKCJA	MIGROWANE USTAWIENIA
Zarządzanie agentami	• Ustawienia skanowania ręcznego* • Ustawienia skanowania zaplanowanego* • Ustawienia skanowania w czasie rzeczywistym* • Ustawienia funkcji Skanuj teraz* • Ustawienia usługi Web Reputation* • Ustawienia monitorowania zachowań* • Ustawienia kontroli urządzeń* • Ustawienia Zapobieganie utracie danych* • Uprawnienia i inne ustawienia* • Dodatkowe ustawienia usługi* • Lista dozwolonych spyware/grayware* **Uwaga** • Narzędzie Server Migration nie dokonuje migracji katalogów kopii zapasowych dla funkcji skanowania ręcznego, skanowania zaplanowanego, skanowania w czasie rzeczywistym i Skanuj teraz. • Ustawienia zachowują konfiguracje zarówno na poziomie administratora, jak i na poziomie domeny.
Grupowanie agentów	Wszystkie ustawienia **Uwaga** Po dokonaniu synchronizacji z usługą Active Directory po raz pierwszy wyświetlana jest struktura domen Active Directory.
Ustawienia agenta globalnego	Wszystkie ustawienia

FUNKCJA	MIGROWANE USTAWIENIA
Lokalizacja punktu końcowego	• Ustawienia rozpoznawania lokalizacji • Listy adresów IP bramy i adresów MAC
Zapobieganie utracie danych	• Identyfikatory danych • Szablony
Zapora	• Reguły • Profile
Obsługa dziennika	Wszystkie ustawienia
Źródła aktualizacji agenta	• Źródło aktualizacji agenta • Lista niestandardowych źródeł aktualizacji
Źródła Smart Protection	Lista niestandardowych źródeł programu Smart Protection
Powiadomienia	• Ogólne ustawienia powiadamiania • Ustawienia powiadamiania administratorów • Ustawienia powiadamiania o epidemiach • Ustawienia powiadamiania agentów
Serwer proxy	Wszystkie ustawienia
Nieaktywni agenci	Wszystkie ustawienia
Menedżer kwarantanny	Wszystkie ustawienia
Konsola Web	Wszystkie ustawienia
Ustawienia w pliku `ofcscan.ini`	• [INI_CLIENT_INSTALLPATH_SECTION] WinNT_InstallPath • [INI_REESTABLISH_COMMUNICATION_SECTION]: wszystkie ustawienia
Ustawienia w pliku `ofcserver.ini`	[INI_SERVER_DISK_THRESHOLD]: wszystkie ustawienia

Uwaga

- Narzędzie nie tworzy kopii zapasowej list agentów OfficeScan z serwera OfficeScan, a jedynie struktury domen.
- Agent OfficeScan migruje tylko funkcje dostępne w starszej wersji serwera agentów OfficeScan. W przypadku funkcji, które nie były dostępne na starym serwerze, Agent OfficeScan stosuje ustawienia domyślne.

Użycie narzędzia Server Migration Tool

Uwaga

Ta wersja programu OfficeScan obsługuje migrację z programuOfficeScan 10.6 SP3 lub nowszego.

Starsze wersje programu OfficeScan mogą nie zawierać wszystkich ustawień dostępnych w najnowszej wersji. Program OfficeScan automatycznie stosuje ustawienia domyślne dla wszystkich funkcji, które nie zostały zmigrowane z poprzedniej wersji serwera OfficeScan.

Procedura

1. Na komputerze serwera OfficeScan XG przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\ServerMigrationTool`.
2. Skopiuj narzędzie Server Migration Tool na źródłowy komputer serwera OfficeScan.

   Ważne

   Aby mieć pewność, że wszystkie dane są poprawnie sformatowane dla nowego serwera docelowego, należy użyć narzędzia Server Migration programu OfficeScan XG na źródłowym serwerze OfficeScan. Program OfficeScan XG nie jest zgodny ze starszymi wersjami narzędzia Server Migration.

3. Kliknij dwukrotnie plik `ServerMigrationTool.exe`, aby uruchomić narzędzie Server Migration Tool.

   Zostanie otwarte narzędzie Server Migration Tool.

4. Aby wyeksportować ustawienia ze źródłowego serwera OfficeScan:

   a. Określ folder docelowy przy użyciu przycisku **Przeglądaj**.

   Uwaga

   Domyślna nazwa pakietu eksportu to `OsceMigrate.zip`.

   b. Kliknij **Eksportuj**.

      Zostanie wyświetlona prośba o potwierdzenie.

   c. Skopiuj pakiet eksportu na docelowy serwer OfficeScan.

5. Aby zaimportować ustawienia na docelowy serwer OfficeScan:

   a. Znajdź pakiet eksportu przy użyciu przycisku **Przeglądaj**.

   b. Kliknij przycisk **Importuj**.

      Zostanie wyświetlony komunikat ostrzegawczy.

   c. Kliknij przycisk **Tak**, aby kontynuować.

      Zostanie wyświetlona prośba o potwierdzenie.

6. Upewnij się, że serwer zawiera wszystkie ustawienia z poprzedniej wersji programu OfficeScan.

7. Przenieś starych agentów OfficeScan na nowy serwer.

   Szczegółowe informacje o przenoszeniu agentów OfficeScan zawiera sekcja *Przenoszenie agenta OfficeScan do innej domeny lub serwera OfficeScan na stronie 2-69* lub *Agent Mover na stronie 15-23*.

Integracja usługi Active Directory

Integracja programu OfficeScan ze strukturą Microsoft™ Active Directory™ pozwala na wydajniejsze zarządzanie Agenci OfficeScan, przypisywanie uprawnień dostępu do konsoli internetowej za pomocą kont usługi Active Directory oraz określanie, na których

agentach nie zostało zainstalowane oprogramowanie zabezpieczające Wszyscy użytkownicy w domenie sieciowej mogą mieć bezpieczny dostęp do konsoli OfficeScan. Możliwe jest także ograniczenie dostępu do określonych użytkowników, również z innej domeny. Weryfikacja poświadczeń użytkowników jest realizowana za pomocą mechanizmu uwierzytelniania i klucza szyfrowania.

Integracja usługi Active Directory zapewnia możliwość korzystania z zalet następujących funkcji:

- **Niestandardowe grupy agentów**: Wykorzystanie usługi Active Directory lub adresów IP do ręcznego grupowania agentów i przypisania ich do domen w drzewie agentów OfficeScan.

  Szczegółowe informacje zawiera sekcja *Automatyczne grupowanie Agentów na stronie 2-62*.

- **Niezarządzane punkty końcowe**: Zapewnienie zgodności punktów końcowych w sieci, które nie są zarządzane przez serwer OfficeScan, z wytycznymi bezpieczeństwa obowiązującymi w firmie.

  Szczegółowe informacje zawiera sekcja *Zgodność z zabezpieczeniami dla niezarządzanych punktów końcowych na stronie 15-74*.

Strukturę usługi Active Directory można synchronizować z serwerem OfficeScan ręcznie lub okresowo w celu zapewnienia spójności danych.

Szczegółowe informacje zawiera sekcja *Synchronizacja danych z domenami Active Directory na stronie 2-44*.

Integrowanie usługi Active Directory z programem OfficeScan

Procedura

1. Przejdź do opcji **Administracja** > **Active Directory** > **Integracja usługi Active Directory**.
2. W obszarze **Domeny usługi Active Directory** wprowadź nazwę domeny usługi Active Directory.

3. Określ poświadczenia, które będą używane przez serwer OfficeScan podczas synchronizowania danych z określoną domeną Active Directory. Poświadczenia są wymagane, gdy serwer nie jest częścią określonej domeny. W przeciwnym razie poświadczenia są opcjonalne. Upewnij się, że poświadczenia domeny nie są przeterminowane i że serwer będzie miał możliwość zsynchronizowania danych.

   a. Kliknij polecenie **Wprowadź poświadczenia domeny**.

   b. W oknie podręcznym, które się otworzy, należy wpisać nazwę użytkownika i hasło. Nazwa użytkownika można określić przy użyciu jednego z następujących formatów:

      - `domena\nazwa_użytkownika`
      - `nazwa_uzytkownika@domena`

   c. Kliknij przycisk **Zapisz**.

4. Kliknij przycisk (+), aby dodać więcej domen. W razie potrzeby określ poświadczenia odpowiedniej z dodanych domen.

5. Kliknij przycisk (-), aby usunąć domeny.

6. Określ ustawienia szyfrowania, jeśli określono poświadczenia domeny. W ramach bezpieczeństwa wprowadzone poświadczenia domeny są szyfrowane przez serwer OfficeScan przed zapisaniem ich w bazie danych. Podczas synchronizowania danych między serwerem OfficeScan a jakąkolwiek określoną domeną, do odszyfrowania poświadczeń domeny jest używany klucz szyfrowania.

   a. Przejdź do sekcji **Ustawienia szyfrowania dotyczące poświadczeń domeny**.

   b. Wprowadź klucz szyfrowania, który nie jest dłuższy niż 128 znaków.

   c. Określ plik, w którym należy zapisać klucz szyfrowania. Można wybrać popularny format plików, taki jak `.txt`. Wpisz pełną ścieżkę do pliku i nazwę, np. `C:\AD_Encryption\EncryptionKey.txt`.

OSTRZEŻENIE!

w przypadku usunięcia pliku lub zmiany jego nazwy synchronizacja danych między programem OfficeScan a wszystkimi określonymi domenami nie jest możliwa.

7. Kliknij jedną z poniższych opcji:

   - **Zapisze**: tylko zapisz ustawienia. Synchronizacja danych może zużywać zasoby sieciowe, dlatego też można zapisać tylko ustawienia, a synchronizację wykonać później, np. podczas mniej istotnych godzin pracy.
   - **Zapisz i synchronizuj**: zapisz ustawienia i synchronizuj dane z domenami Active Directory.

8. Zaplanuj okresową synchronizację. Szczegółowe informacje zawiera sekcja *Synchronizacja danych z domenami Active Directory na stronie 2-44*.

Synchronizacja danych z domenami Active Directory

Regularna synchronizacja danych z domenami Active Directory zapewnia zachowanie aktualności struktury drzewa agentów OfficeScan i wykonywanie zapytań o niezarządzanych agentów.

Ręczna synchronizacja danych z domenami usługi Active Directory

Procedura

1. Przejdź do opcji **Administracja** > **Active Directory** > **Integracja usługi Active Directory**.
2. Upewnij się, że poświadczenia domeny i ustawienia szyfrowania nie uległy zmianie.
3. Kliknij polecenie **Zapisz i zsynchronizuj**.

Automatyczna synchronizacja danych z domenami usługi Active Directory

Procedura

1. Przejdź do opcji **Administracja** > **Active Directory** > **Synchronizacja zaplanowana**.
2. Wybierz opcję **Włącz zaplanowaną synchronizację usługi Active Directory**.
3. Określ harmonogram synchronizacji.

   Uwaga

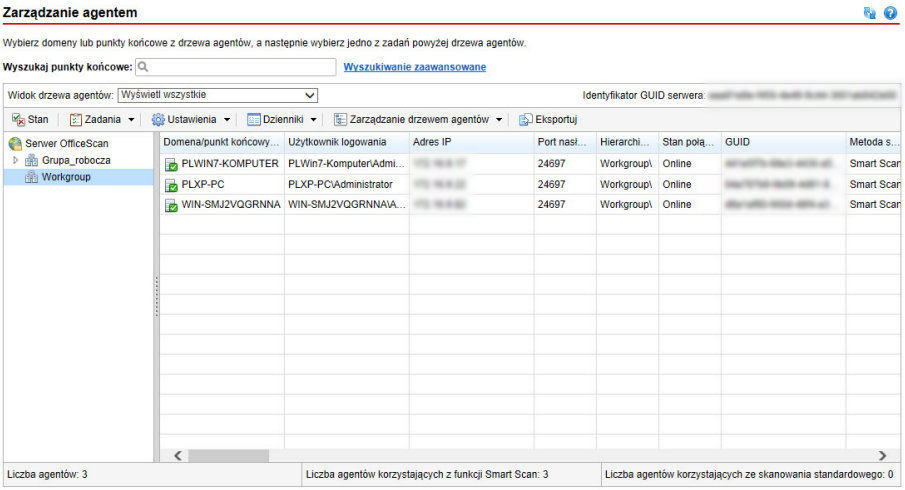
   W przypadku aktualizacji dziennych, tygodniowych i miesięcznych, przedział czasu to liczba godzin, w czasie których program OfficeScan synchronizuje usługę Active Directory z serwerem OfficeScan.

4. Kliknij przycisk **Zapisz**.

Drzewo agentów Program OfficeScan

Drzewo agentów Program OfficeScan przedstawia wszystkich agentów pogrupowanych w domeny, którymi serwer obecnie zarządza. Agentów można grupować w domeny,

zapewniając możliwość jednoczesnego konfigurowania wszystkich członków domeny, zarządzania konfiguracją i jej stosowania.



ILUSTRACJA 2-5. Drzewo agentów Program OfficeScan

Stan połączenia agenta

Stan połączenia Agent OfficeScan jest zależny od sposobu, w jaki serwer OfficeScan komunikuje się z Agent OfficeScan. Poniższa tabela przedstawia różne stany połączenia dostępne dla Agent OfficeScan.

TABELA 2-8. Stan połączenia agenta Office

STAN	OPIS
Online	Agent OfficeScan może połączyć się z serwerem OfficeScan w celu dwukierunkowej komunikacji następujących elementów: • Ustawienia reguł • Aktualizacje • Polecenia skanowania • Synchronizacja listy podejrzanych obiektów • Przesyłanie próbek • Przesyłanie dzienników
Offline	Agent OfficeScan nie ma funkcjonalnego połączenia z serwerem OfficeScan ani z serwerem Przekaźnika Krawędziowego.
Tryb niezależny	Agent OfficeScan może nawiązać połączenie z serwerem OfficeScan, ale komunikacja jest ograniczona. W trybie niezależnym: • Agent OfficeScan nie akceptuje ustawień reguł z serwera. • Agent OfficeScan nie inicjuje poleceń skanowania z serwera. • Agent OfficeScan nie wysyła dzienników na serwer. Agentów w trybie niezależnym można skonfigurować przy użyciu uprawnień blokowania lub zezwalania na aktualizacje składników, jeśli dostępne jest funkcjonalne połączenie z serwerem OfficeScan. Użytkownicy końcowi mogą ręcznie inicjować skanowanie i aktualizowanie agentów w trybie niezależnym.
Zdalny	Agent OfficeScan znajduje się poza siecią firmową i nie może nawiązać bezpośrednio połączenia z serwerem OfficeScan. Agent OfficeScan może jednak nawiązać połączenie z serwerem Przekaźnika Krawędziowego na potrzeby następujących zadań: • Synchronizacja listy podejrzanych obiektów • Przesyłanie próbek • Przesyłanie dzienników

Ikony drzewa agentów

Ikony drzewa agentów OfficeScan oferują wizualne informacje o typie punktu końcowego i stanie agentów OfficeScan zarządzanych przez program OfficeScan.

TABELA 2-9. OfficeScan Ikony drzewa agentów

IKONA	OPIS
	Domena
	Katalog główny
	Agent aktualizacji
	Agent skanowania standardowego
	Dostępny Agent OfficeScan Smart Scan
	Niedostępny Agent OfficeScan Smart Scan
	Skanowanie Smart Scan dostępne — agent aktualizacji
	Skanowanie Smart Scan niedostępne — agent aktualizacji

Ogólne zadania dostępne w drzewie agentów

Poniżej przedstawiono ogólne zadania, jakie można wykonywać po wyświetleniu drzewa agentów:

Procedura

- Kliknij ikonę domeny głównej  , aby wybrać wszystkie domeny i agentów. Po kolejnym wybraniu ikony domeny głównej i czynności powyżej drzewa agentów zostanie wyświetlony ekran służący do konfigurowania ustawień. Na tym ekranie można korzystać z następujących opcji ogólnych:
  - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
  - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.
- Aby wybrać kilka sąsiednich domen lub agentów:
  - W prawym panelu wybierz pierwszą domenę, przytrzymaj wciśnięty klawisz SHIFT, a następnie kliknij ostatnią domenę lub agenta z tego zakresu.
- Aby wybrać zakres domen lub agentów nie znajdujących się w sąsiedztwie, przytrzymaj wciśnięty klawisz CTRL i kliknij domeny lub agentów w celu wybrania.
- Wyszukaj dowolnego agenta do zarządzania, podając nazwę agenta w polu tekstowym **Wyszukaj punkty końcowe**.

  W drzewie agentów zostanie wyświetlona lista wyników. Aby wyświetlić więcej opcji wyszukiwania, kliknij opcję **Szukanie zaawansowane**.

  Uwaga

  Podczas wyszukiwania określonych agentów nie można określić adresów IPv6 lub IPv4. Aby wyszukiwać według adresu IPv4 lub IPv6, należy użyć wyszukiwania zaawansowanego. Szczegółowe informacje zawiera sekcja *Zaawansowane opcje wyszukiwania na stronie 2-50*.
- Po wybraniu domeny tabela drzewa agentów zostanie rozwinięta w celu przedstawienia agentów należących do domeny oraz wszystkich kolumn zawierających odpowiednie informacje dla każdego agenta. Aby przeglądnąć jedynie zestaw odpowiednich kolumn, wybierz element w widoku drzewa agentów.

- **Pokaz wszystkie**: Pokazuje wszystkie kolumny
- **Widok aktualizacji**: Pokazuje wszystkie składniki i programy
- **Widok narzędzi antywirusowych**: Pokazuje składniki antywirusowe
- **Widok oprogramowania anty-spyware**: Pokazuje składniki anty-spyware
- **Widok Ochrona danych**: Pokazuje stan modułu Ochrona danych na agentach
- **Widok zapory**: Pokazuje składniki zapory
- **Widok Smart Protection**: Pokazuje metody skanowania używane przez agentów (skanowanie standardowe lub Smart Scan) oraz składniki Smart Protection
- **Widok agenta aktualizacji**: Pokazuje informacje o wszystkich agentach aktualizacji zarządzanych przez serwer OfficeScan
- **Widok agenta zdalnego**: Pokazuje informacje o wszystkich agentach podlegających serwerowi Serwer Przekaźnika Krawędziowego

- Agentów można posortować na podstawie informacji w kolumnach, klikając nazwę kolumny.
- Odśwież drzewo agentów, klikając polecenie ikonę odświeżania ( ).
- Poniżej drzewa agentów można wyświetlić jego statystyki, takie jak łączna liczba agentów, liczba agentów Smart Scan oraz liczba agentów skanowania standardowego.

Zaawansowane opcje wyszukiwania

agenci można wyszukiwać, korzystając z następujących kryteriów:

Procedura

- **Podstawowe kryteria**: Podstawowe kryteria: Umożliwia wyszukiwanie według podstawowych informacji o komputerach, takich jak adres IP, system operacyjny, domena, adres MAC, metoda skanowania i stan usługi Web Reputation.

- Szukanie według segmentu IPv4 wymaga podania części adresu IP, począwszy od pierwszego oktetu. Wynikiem wyszukiwania będą wszystkie punkty końcowe z adresem IP zawierającym ten wpis. Na przykład, po wpisaniu 10.5 wynikiem wyszukiwania będą wszystkie komputery z adresami IP od 10.5.0.0 do 10.5.255.255.
- Wyszukiwanie według adresu IPv6 wymaga prefiksu i długości.
- Wyszukiwanie według adresu MAC wymaga podania zakresu adresów MAC w notacji szesnastkowej, na przykład 000A1B123C12.

- **Wersje składników**: Zaznacz pole wyboru umieszczone obok nazwy składnika, zawęź kryteria, wybierając polecenie **Wcześniej niż** lub **równy lub starszy niż** i wpisz numer wersji. Domyślnie wyświetlany jest numer bieżącej wersji.
- **Stan**: Zawiera ustawienia agent
- Po określeniu kryteriów wyszukiwania kliknij polecenie **Szukaj**. W drzewie agent zostanie wyświetlona lista punkt końcowy spełniających kryteria.

Zaawansowane zadania dostępne w drzewie agentów

Drzewo agentów jest wyświetlane podczas uzyskiwania dostępu do określonych ekranów konsoli Web. Powyżej drzewa agentów są widoczne elementy menu charakterystyczne dla otwartego ekranu. Te elementy menu umożliwiają wykonywania określonych zadań, takich jak konfigurowanie ustawień agentów czy inicjowanie zadań agentów. Aby wykonać jedno z tych zadań, należy najpierw wybrać element docelowy, a następnie wybrać polecenie menu.

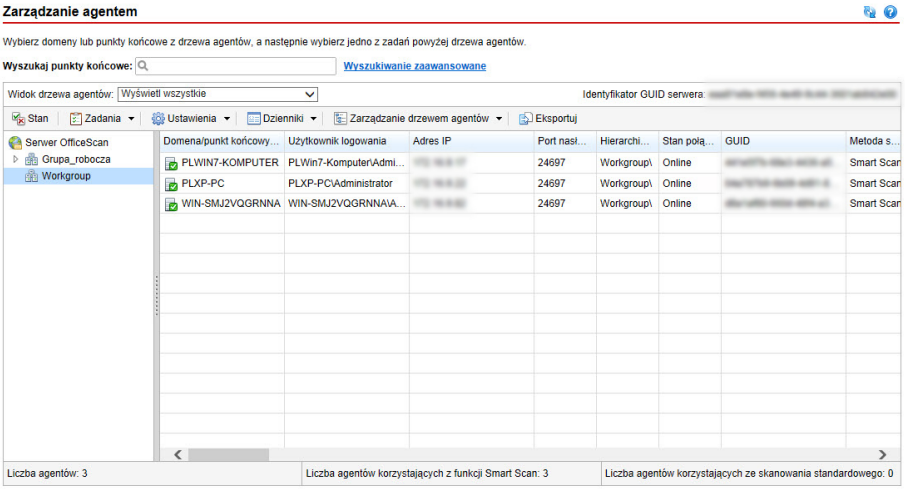
Drzewo agentów jest wyświetlane na następujących ekranach:

- *Ekran Zarządzanie agentami na stronie 2-52*
- *Ekran Ochrona przed epidemią na stronie 2-56*
- *Ekran Wybór agenta na stronie 2-57*
- *Ekran Wycofywanie na stronie 2-57*
- *Ekran Dzienniki zagrożeń bezpieczeństwa na stronie 2-58*

Ekran Zarządzanie agentami

Aby wyświetlić ten ekran, przejdź do opcji **Agenci** > **Zarządzanie agentami**.

Na ekranie **Zarządzanie agentami** można zarządzać ogólnymi ustawieniami agentów i wyświetlać informacje o stanie określonych agentów (takie jak **użytkownik logowania**, **adres IP** i **stan połączenia**).



ILUSTRACJA 2-6. Ekran Zarządzanie agentami

Poniższa tabela przedstawia zadania, które można wykonać:

TABELA 2-10. Zadania Zarządzanie agentami

PRZYCISK MENU	ZADANIE
Stan	Wyświetlenie szczegółowych informacji o agencie. Szczegółowe informacje zawiera sekcja *Wyświetlanie informacji o agencie OfficeScan na stronie 15-58*.

PRZYCISK MENU	ZADANIE
Zadania	• Uruchomienie funkcji Skanuj teraz na punktach końcowych agentów. Szczegółowe informacje zawiera sekcja *Uruchamianie Skanuj teraz na stronie 7-28*. • Dezinstalacja agenta. Szczegółowe informacje zawiera sekcja *Dezinstalacja agenta OfficeScan z poziomu konsoli Web na stronie 5-80*. • Przywracanie podejrzanych plików, które zostały wykryte. Szczegółowe informacje zawiera sekcja *Przywracanie plików poddanych kwarantannie na stronie 7-50*. • Przywrócenie składników oprogramowania spyware/grayware. Szczegółowe informacje zawiera sekcja *Przywracanie spyware/grayware na stronie 7-59*.

Przycisk menu	Zadanie

Ustawienia	• Konfigurowanie ustawień skanowania. Aby uzyskać szczegółowe informacje, zobacz następujące tematy:
	  • *Typy metod skanowania na stronie 7-9*
	  • *Skanowanie ręczne na stronie 7-19*
	  • *Skanowanie w czasie rzeczywistym na stronie 7-16*
	  • *Skanowanie zaplanowane na stronie 7-22*
	  • *Skanuj teraz na stronie 7-25*
	• Konfigurowanie ustawień usługi Web Reputation. Szczegółowe informacje zawiera sekcja *Reguły Web Reputation na stronie 12-5*.
	• Konfigurowanie ustawień przewidującego uczenia maszynowego. Szczegółowe informacje zawiera sekcja *Konfigurowanie ustawień przewidującego uczenia maszynowego na stronie 8-3*.
	• Konfigurowanie ustawień podejrzanego połączenia. Szczegółowe informacje zawiera sekcja *Konfigurowanie ustawień podejrzanego połączenia na stronie 8-7*.
	• Konfigurowanie ustawień monitorowania zachowań. Szczegółowe informacje zawiera sekcja *Monitorowanie zachowań na stronie 9-2*.
	• Konfigurowanie ustawień kontroli urządzeń. Szczegółowe informacje zawiera sekcja *Kontrola urządzeń na stronie 10-2*.
	• Konfigurowanie reguł Zapobieganie utracie danych. Szczegółowe informacje zawiera sekcja *Konfiguracja reguł Zapobieganie utracie danych na stronie 11-50*.
	• Przydzielanie agentów jako agentów aktualizacji. Szczegółowe informacje zawiera sekcja *Konfiguracja Agenta aktualizacji na stronie 6-58*.
	• Konfigurowanie uprawnień agenta i innych ustawień. Szczegółowe informacje zawiera sekcja *Konfigurowanie uprawnień agenta i innych ustawień na stronie 15-96*.
	• Włączenie lub wyłączenie usług agenta OfficeScan. Szczegółowe informacje zawiera sekcja *Usługi agenta OfficeScan na stronie 15-7*.
	• Konfigurowanie listy dozwolonego oprogramowania spyware/grayware. Szczegółowe informacje zawiera sekcja *Lista dozwolonych spyware/grayware na stronie 7-57*.
	• Konfigurowanie listy zaufanych programów. Szczegółowe informacje zawiera sekcja *Konfigurowanie listy zaufanych programów na stronie 7-61*.

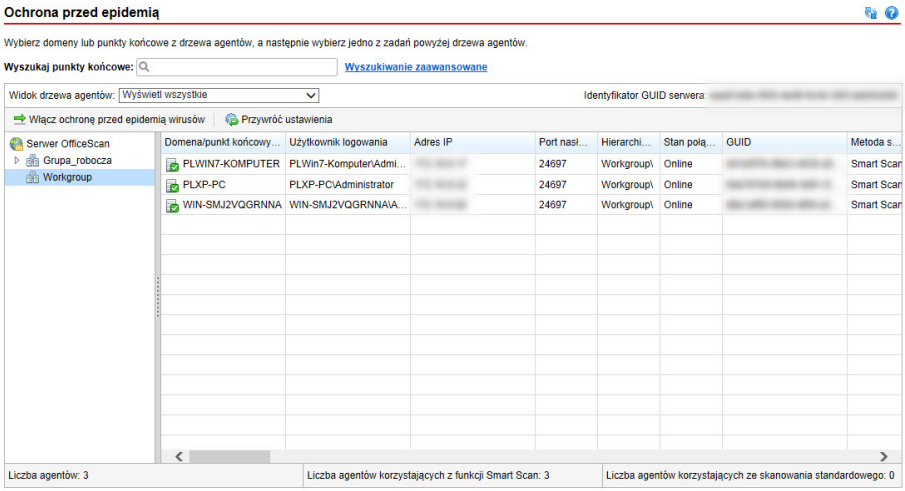
PRZYCISK MENU	ZADANIE
Dzienniki	Wyświetlanie następujących dzienników: • Dzienniki wirusów/złośliwych programów (aby uzyskać szczegółowe informacje, patrz *Wyświetlanie dzienników wirusów/złośliwego oprogramowania na stronie 7-102*) • Dzienniki oprogramowania spyware/grayware (aby uzyskać szczegółowe informacje, patrz *Wyświetlanie dzienników oprogramowania spyware/grayware na stronie 7-111*) • Dzienniki zapory (aby uzyskać szczegółowe informacje, patrz *Dzienniki zapory na stronie 13-30*) • Dzienniki usługi Web Reputation (aby uzyskać szczegółowe informacje, patrz *Dzienniki zagrożenia internetowego na stronie 12-22*) • Dzienniki podejrzanego połączenia (aby uzyskać szczegółowe informacje, patrz *Przeglądanie dzienników podejrzanego połączenia na stronie 8-15*) • Dzienniki podejrzanych plików (aby uzyskać szczegółowe informacje, patrz *Wyświetlanie dzienników podejrzanych plików na stronie 7-115*). • Dzienniki wywołań zwrotnych C&C (aby uzyskać szczegółowe informacje, patrz *Wyświetlanie dzienników wywołań zwrotnych C&C na stronie 12-24*). • Dzienniki monitorowania zachowań (aby uzyskać szczegółowe informacje, patrz *Dzienniki monitorowania zachowań na stronie 9-19*) • Dzienniki przewidującego uczenia maszynowego (aby uzyskać szczegółowe informacje, patrz *Wyświetlanie dzienników przewidującego uczenia maszynowego na stronie 8-11*) • Dzienniki kontroli urządzeń (aby uzyskać szczegółowe informacje, patrz *Dzienniki kontroli urządzeń na stronie 10-19*) • Dzienniki DLP (aby uzyskać szczegółowe informacje, patrz *Dzienniki Zapobieganie utracie danych na stronie 11-60*) • Dzienniki operacji skanowania (aby uzyskać szczegółowe informacje, patrz *Wyświetlanie dzienników operacji skanowania: na stronie 7-116*). Usuwanie dzienników. Szczegółowe informacje zawiera sekcja *Zarządzanie dziennikiem na stronie 14-41*.

PRZYCISK MENU	ZADANIE
Zarządzanie drzewem agentów	Zarządzanie drzewem agentów. Szczegółowe informacje zawiera sekcja *Zadania grupowania agentów OfficeScan na stronie 2-66*.
Eksportuj	Eksportowanie listy agentów do pliku rozdzielanego przecinkami (`.csv`).

Ekran Ochrona przed epidemią

Aby wyświetlić ten ekran, przejdź do opcji **Agenci** > **Ochrona przed epidemią**.

Na ekranie **Ochrona przed epidemią** można określić i aktywować ustawienia ochrony przed epidemią. Szczegółowe informacje zawiera sekcja *Konfigurowanie zapobiegania epidemiom zagrożeń bezpieczeństwa na stronie 7-122*.

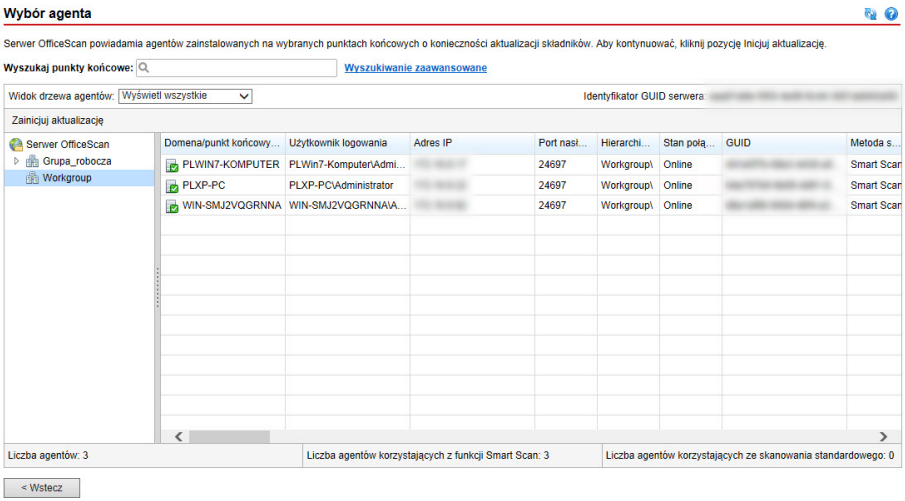


ILUSTRACJA 2-7. Ekran Ochrona przed epidemią

Ekran Wybór agenta

Aby wyświetlić ten ekran, przejdź do opcji **Aktualizacje** > **Agenci** > **Aktualizacja ręczna**. Wybierz pozycję **Wybierz agentów ręcznie**, a następnie kliknij polecenie **Wybierz**.

Zainicjuj aktualizację ręczną na ekranie **Wybór agenta**. Szczegółowe informacje zawiera sekcja *Aktualizacja ręczna agentów OfficeScan na stronie 6-47*.

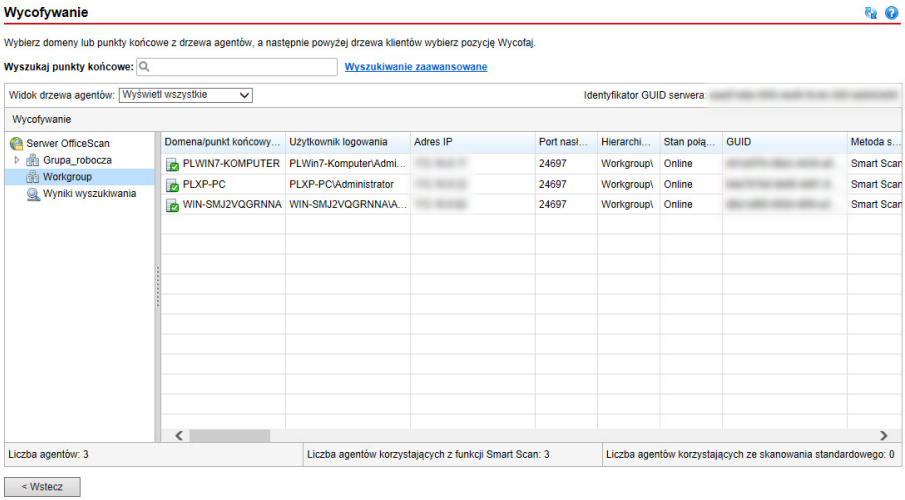


ILUSTRACJA 2-8. Ekran Wybór agenta

Ekran Wycofywanie

Aby wyświetlić ten ekran, przejdź do opcji **Aktualizacje** > **Wycofywanie**. Kliknij przycisk **Synchronizuj z serwerem**.

Na ekranie **Wycofywanie** można wycofać składniki agenta. Szczegółowe informacje zawiera sekcja *Wycofywanie składników agentów OfficeScan na stronie 6-55*.

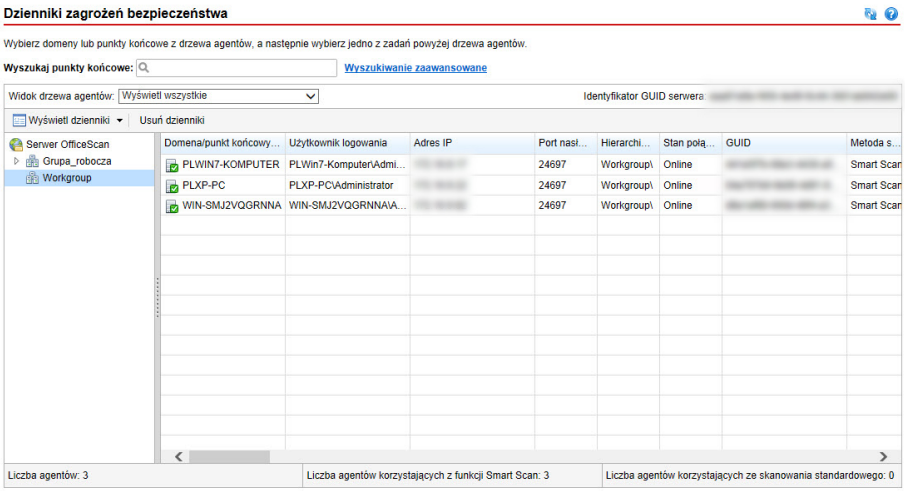


ILUSTRACJA 2-9. Ekran Wycofywanie

Ekran Dzienniki zagrożeń bezpieczeństwa

Aby wyświetlić ten ekran, przejdź do opcji **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa**.

Na ekranie **Dzienniki zagrożeń bezpieczeństwa** można wyświetlać dzienniki i zarządzać nimi.



ILUSTRACJA 2-10. Ekran Dzienniki zagrożeń bezpieczeństwa

Wykonaj następujące czynności:

1. Wyświetl dzienniki wysyłane przez agentów na serwer. Szczegółowe informacje zawiera sekcja:

   - *Wyświetlanie dzienników wirusów/złośliwego oprogramowania na stronie 7-102*
   - *Wyświetlanie dzienników oprogramowania spyware/grayware na stronie 7-111*
   - *Wyświetlanie dzienników zapory na stronie 13-30*
   - *Wyświetlanie dzienników usługi Web Reputation na stronie 12-23*
   - *Przeglądanie dzienników podejrzanego połączenia na stronie 8-15*
   - *Wyświetlanie dzienników podejrzanych plików na stronie 7-115*
   - *Wyświetlanie dzienników wywołań zwrotnych C&C na stronie 12-24*

- *Wyświetlanie dzienników monitorowania zachowań na stronie 9-19*
- *Wyświetlanie dzienników kontroli urządzeń na stronie 10-19*
- *Wyświetlanie dzienników Zapobieganie utracie danych na stronie 11-61*

2. Usuwanie dzienników. Szczegółowe informacje zawiera sekcja *Zarządzanie dziennikiem na stronie 14-41*.

Domeny programu OfficeScan

Domena w programie OfficeScan to grupa agentów korzystających z tej samej konfiguracji i wykonujących te same zadania. Grupując agentów w domeny, można stosować taką samą konfigurację dla wszystkich członków domeny, zarządzać nią i ją wdrażać. Dodatkowe informacje na temat grupowania agentów znajdują się w temacie *Grupowanie agentów na stronie 2-60*.

Grupowanie agentów

Funkcja grupowania agentów służy do ręcznego lub automatycznego tworzenia domen i zarządzania nimi w drzewie agentów programu OfficeScan.

Istnieją dwie metody grupowania agentów w domeny.

TABELA 2-11. Metody grupowania agentów

METODA	GRUPOWANIE AGENTÓW	OPISY
Ręczne	• domena NetBIOS • domena Active Directory • domena DNS	Ręczne grupowanie agentów definiuje domenę, do której powinien należeć nowo zainstalowany agent. Kiedy agent pojawi się w drzewie agentów, można go przenieść do innej domeny lub na inny serwer OfficeScan. Ręczne grupowanie agentów umożliwia także tworzenie i usuwanie domen w drzewie agentów. Szczegółowe informacje zawiera sekcja *Ręczne grupowanie agentów na stronie 2-61*.

METODA	GRUPOWANIE AGENTÓW	OPISY
Automatyczna	Niestandardowe grupy agentów	Automatyczne grupowanie agentów używa reguł w celu sortowania agentów w drzewie agentów. Po zdefiniowaniu reguł można uzyskać dostęp do drzewa agentów, aby ręcznie posortować agentów albo umożliwić programowi OfficeScan ich automatyczne sortowanie po wystąpieniu określonych zdarzeń lub zgodnie z zaplanowanym przedziałem czasu. Szczegółowe informacje zawiera sekcja *Automatyczne grupowanie Agentów na stronie 2-62*.

Ręczne grupowanie agentów

Program OfficeScan korzysta z tego ustawienia tylko podczas nowej instalacji agenta. Program instalacyjny sprawdza domenę sieciową, do której należy docelowy punkt końcowy. Jeśli nazwa domeny istnieje już w drzewie agentów, program OfficeScan zgrupuje agenta na docelowym punkcie końcowym w tej domenie i zastosuje do niego ustawienia skonfigurowane dla tej domeny. Jeśli nazwa domeny nie istnieje, program OfficeScan dodaje domenę do drzewa agentów, grupuje agenta w ramach tej domeny, a następnie stosuje ustawienia główne do domeny i agenta.

Konfigurowanie automatycznego grupowania agentów

Procedura

1. Przejdź do opcji **Agenci** > **Grupowanie agentów**.
2. Wybierz metodę grupowania agentów:
   - domena NetBIOS
   - domena Active Directory
   - domena DNS

3. Kliknij przycisk **Zapisz**.

Co dalej

Domenami i zgrupowanymi w nich agentami można zarządzać, wykonując następujące zadania:

- Dodaj domenę
- Usuwanie domeny lub agenta
- Zmień nazwę domeny
- Przenieś pojedynczego agenta do innej domeny

Szczegółowe informacje zawiera sekcja *Zadania grupowania agentów OfficeScan na stronie 2-66*.

Automatyczne grupowanie Agentów

Automatyczne grupowanie agentów używa reguł zdefiniowanych przez adresy IP lub domeny Active Directory. Jeśli zasada definiuje adres IP lub zakres adresów IP, serwer OfficeScan zgrupuje agentów ze zgodnym adresem IP do określonej domeny w drzewie agentów. Analogicznie, jeśli zasada definiuje jedną lub więcej domen Active Directory, serwer OfficeScan zgrupuje agentów należących do określonej domeny Active Directory w konkretnej domenie w drzewie agentów.

Agenci stosują jednocześnie tylko jedną zasadę. Należy określić priorytety zasad tak, aby dla agenta pasującego do więcej niż jednej reguły była stosowana reguła o najwyższym priorytecie.

Konfigurowanie automatycznego grupowania agentów

Procedura

1. Przejdź do opcji **Agenci** > **Grupowanie agentów**
2. Przejdź do sekcji **Grupowanie agentów** i wybierz opcję **Utwórz osobiste grupy istniejących agentów OfficeScan**.

3. Przejdź do sekcji **Automatyczne grupowanie agentów**.

4. Aby rozpocząć tworzenie reguł, kliknij przycisk **Dodaj**, a następnie wybierz opcję **Active Directory** lub **Adres IP**.

   - Jeśli wybrano opcję **Active Directory**, zapoznaj się z instrukcjami konfiguracji w temacie *Definiowanie reguł grupowania agentów według domen Active Directory na stronie 2-64*.

   - Jeśli wybrano opcję **Adres IP**, zapoznaj się z instrukcjami konfiguracji w temacie *Definiowanie reguł grupowania agentów według adresów IP na stronie 2-65*.

5. Jeśli utworzono więcej niż jedną regułę, określ priorytety reguł, wykonując następujące czynności:

   a. Wybierz regułę.

   b. Kliknij strzałkę poniżej kolumny **Priorytet grupy**, aby przenieść regułę w górę lub w dół listy. Numer identyfikacyjny reguły zostaje zmieniony zgodnie z nową pozycją.

6. Aby użyć reguł podczas sortowania agentów:

   a. Zaznacz pola wyboru odpowiadające regułom, których chcesz używać.

   b. Włącz reguły, przełączając element sterujący **Stan** do pozycji **Wł**.

Uwaga

Jeśli pole wyboru odpowiadające regule nie zostanie zaznaczone lub jeśli reguła zostanie wyłączona, ta reguła nie będzie używana podczas sortowania agentów w drzewie agentów. Jeśli na przykład reguła nakazuje przeniesienie agenta do nowej domeny, agent nie zostanie przeniesiony i pozostanie w bieżącej domenie.

7. Określ harmonogram sortowania w sekcji **Zaplanowane tworzenie domeny**.

   a. Wybierz opcję **Włącz zaplanowane tworzenie domeny**.

   b. Określ harmonogram w sekcji **Zaplanowane tworzenie domeny**.

8. Wybierz jedną z następujących opcji:

   - **Zapisz i utwórz domenę teraz**: Wybierz tę opcję, jeśli określono nowe domeny w procedurze *Definiowanie reguł grupowania agentów według adresów IP na*

stronie 2-65 krok 7 lub *Definiowanie reguł grupowania agentów według domen Active Directory na stronie 2-64* krok 7.

- **Zapisz**: Wybierz tę opcję, jeśli nie określono nowych domen lub chcesz utworzyć nowe domeny dopiero po uruchomieniu sortowania agentów.

Uwaga

Sortowanie agentów nie zostanie rozpoczęte po wykonaniu tego kroku.

Definiowanie reguł grupowania agentów według domen Active Directory

Przed wykonaniem poniższej procedury należy upewnić się, że skonfigurowano ustawienia integracji usługi Active Directory. Szczegółowe informacje zawiera sekcja *Integracja usługi Active Directory na stronie 2-41*.

Procedura

1. Przejdź do opcji **Agenci** > **Grupowanie agentów**
2. Przejdź do sekcji **Grupowanie agentów** i wybierz opcję **Utwórz osobiste grupy istniejących agentów OfficeScan**.
3. Przejdź do sekcji **Automatyczne grupowanie agentów**.
4. Kliknij przycisk **Dodaj**, a następnie wybierz opcję **Active Directory**.

   Zostanie wyświetlony nowy ekran.
5. Wybierz opcję **Włącz grupowanie**.
6. Podaj nazwę reguły.
7. W obszarze **Źródło domeny Active Directory** wybierz domeny lub poddomeny usługi Active Directory.
8. W obszarze **Drzewo agentów** wybierz istniejącą domenę OfficeScan, na którą są mapowane domeny usługi Active Directory. Jeśli żądana domena programu OfficeScan nie istnieje, wykonaj następujące czynności:

a. Najedź myszą na określoną domenę OfficeScan i kliknij ikonę dodawania domeny (➕).

b. Wpisz nazwę domeny w polu tekstowym.

c. Kliknij znacznik wyboru obok pola tekstowego. Nowa domena została utworzona i automatycznie wybrana.

9. (Opcjonalnie) Wybierz opcję **Duplikuj strukturę usługi Active Directory w drzewie agentów OfficeScan**. Ta opcja powoduje zduplikowanie hierarchii wybranych domen usługi Active Directory do wybranej domeny programu OfficeScan.

10. Kliknij przycisk **Zapisz**.

Definiowanie reguł grupowania agentów według adresów IP

Używając adresów IP, utwórz niestandardowe grupy komputerów, aby posortować klientów w produkcie OfficeScan w drzewie komputerów. Ta funkcja ułatwia administratorom organizowanie struktury drzewa agentów OfficeScan zanim agent zarejestruje się na serwerze OfficeScan.

Procedura

1. Przejdź do opcji **Agenci** > **Grupowanie agentów**.
2. Przejdź do sekcji **Grupowanie agentów** i wybierz opcję **Utwórz osobiste grupy istniejących agentów OfficeScan**.
3. Przejdź do sekcji **Automatyczne grupowanie agentów**.
4. Kliknij przycisk **Dodaj,** a następnie wybierz opcję **Adres IP**.

   Zostanie wyświetlony nowy ekran.
5. Wybierz opcję **Włącz grupowanie**.
6. Podaj nazwę grupowania.
7. Określ jedną z następujących wartości:

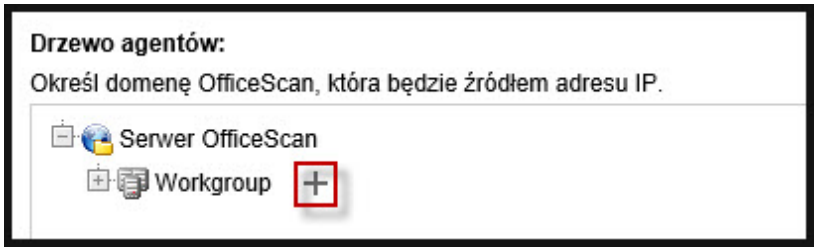
- Pojedynczy adres IPv4 lub IPv6
- Zakres adresów IPv4
- Prefiks IPv6 i długość

Uwaga

Jeśli adresy IPv4 i IPv6 agenta z dwoma stosami należą do dwóch oddzielnych grup agentów, agent zostanie umieszczony w grupie IPv6. Jeśli protokół IPv6 został wyłączony na hoście agenta, agent zostanie przeniesiony do grupy IPv4.

8. Wybierz domenę OfficeScan, do której zostanie przypisany adres lub zakres adresów IP. Jeżeli domena nie istnieje, wykonaj następujące czynności:

   a. Najedź myszą na drzewo agentów i kliknij ikonę dodawania domeny.



ILUSTRACJA 2-11. Ikona dodawania domeny

   b. Wpisz domenę w polu tekstowym.

   c. Kliknij znacznik wyboru obok pola tekstowego. Nowa domena została utworzona i automatycznie wybrana.

9. Kliknij przycisk **Zapisz**.

Zadania grupowania agentów OfficeScan

Podczas grupowania agentów w domenach można wykonać następujące zadania:

- Dodawanie domeny. Szczegółowe informacje można znaleźć w części *Dodawanie domeny na stronie 2-67*.

- Usuwanie domeny lub agenta. Szczegółowe informacje można znaleźć w części *Usuwanie domeny lub agenta na stronie 2-67*.
- Zmiana nazwy domeny. Szczegółowe informacje można znaleźć w części *Zmiana nazwy domeny na stronie 2-68*.
- Przeniesienie pojedynczego agenta do innej domeny lub na inny serwer OfficeScan. Szczegółowe informacje można znaleźć w części *Przenoszenie agenta OfficeScan do innej domeny lub serwera OfficeScan na stronie 2-69*.

Dodawanie domeny

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. Kliknij kolejno opcje **Zarządzanie drzewem agentów** > **Dodaj domenę**.
3. Wpisz nazwę domeny, którą chcesz dodać.
4. Kliknij przycisk **Dodaj**.

   Nowa domena zostanie wyświetlona w drzewie agentów.
5. (Opcjonalnie) Utwórz poddomeny.
   a. Wybierz domenę nadrzędną.
   b. Kliknij kolejno opcje **Zarządzanie drzewem agentów** > **Dodaj domenę**.
   c. Wpisz nazwę poddomeny.

Usuwanie domeny lub agenta

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów wybierz:

- Jedną lub kilka domen
- Jednego, kilku lub wszystkich agentów należących do domeny

3. Kliknij kolejno opcje **Zarządzanie drzewem agentów** > **Usuń domenę/agenta**.
4. Aby usunąć pustą domenę, kliknij opcję **Usuń domenę/agenta**. Jeśli domena zawiera agentów i kliknięto opcję **Usuń domenę/agenta**, serwer OfficeScan ponownie utworzy domenę i zgrupuje w niej wszystkich agentów, kiedy agenci następnym razem połączą się z serwerem OfficeScan. Przed usunięciem domeny można wykonać następujące zadania:
   a. Przenieś agentów do innych domen. Agentów można przenieść do domeny docelowej metodą przeciągania i upuszczania.
   b. Usuń wszystkich agentów.
5. Aby usunąć pojedynczego agenta, kliknij opcję **Usuń domenę/agenta**.

Uwaga

Usunięcie agenta z drzewa agentów nie powoduje usunięcia agenta OfficeScan z punktu końcowego agenta. Agent OfficeScan może nadal wykonywać zadania niezależne od serwera, na przykład aktualizować składniki. Na serwerze nie ma jednak informacji o istnieniu agenta, dlatego serwer nie będzie wysyłać do agenta konfiguracji ani powiadomień.

Zmiana nazwy domeny

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. Wybierz domenę w drzewie agentów.
3. Kliknij kolejno opcje **Zarządzanie drzewem agentów** > **Zmień nazwę domeny**.
4. Wpisz nową nazwę domeny.
5. Kliknij przycisk **Zmień nazwę**.

Nowa domena zostanie wyświetlona w drzewie agentów.

Przenoszenie agenta OfficeScan do innej domeny lub serwera OfficeScan

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów wybierz jednego, kilka lub wszystkich agentów.
3. Kliknij kolejno opcje **Zarządzanie drzewem agentów** > **Przenieś agenta**.
4. Aby przenieść agentów do innej domeny:
   - Wybierz opcję **Przenieś wybranych agentów do innej domeny**.
   - Wybierz domenę.
   - (Opcjonalnie) Zastosuj ustawienia nowej domeny do agentów.

   Porada

   Innym sposobem jest przeciągnięcie i upuszczenie agentów do innej domeny w drzewie agentów.
5. Aby przenieść agentów na inny serwer OfficeScan:
   - Wybierz opcję **Przenieś wybranych agentów do innego serwera OfficeScan**.
   - Wpisz nazwę serwera lub adres IPv4/IPv6 i numer portu HTTP.
6. Kliknij opcję **Przenieś**.

Rozdział 3

Wprowadzenie do modułu Ochrona danych

W tym rozdziale przedstawiono sposób instalacji i aktywacji modułu Ochrona danych.

Rozdział składa się z następujących tematów:

Instalacja modułu Ochrona danych

Moduł Ochrona danych zawiera następujące funkcje:

- **Zapobieganie utracie danych (DLP)**: Uniemożliwia nieautoryzowaną transmisję zasobów cyfrowych
- **Kontrola urządzeń**: Sterowanie dostępem do urządzeń zewnętrznych

Uwaga

Natychmiast po zainstalowaniu program OfficeScan zapewnia funkcję kontroli urządzeń, która reguluje dostęp do powszechnie używanych urządzeń, takich jak urządzenia pamięci masowej USB. Funkcja kontroli urządzeń, która stanowi część modułu Ochrona danych, rozszerza zakres monitorowanych urządzeń. Listę monitorowanych urządzeń zawiera temat *Kontrola urządzeń na stronie 10-2*.

Kontrola zasobów cyfrowych i kontrola urządzeń to natywne funkcje programu OfficeScan, ale są licencjonowane oddzielnie. Po zainstalowaniu serwera OfficeScan funkcje te są dostępne, ale nie działają i nie można ich zainstalować na agentach. Instalacja modułu Ochrona danych oznacza pobranie pliku z serwera ActiveUpdate lub niestandardowego źródła aktualizacji, jeśli zostało skonfigurowane. Po umieszczeniu pliku na serwerze OfficeScan można aktywować funkcję licencję Ochrona danych, aby włączyć jej pełną funkcjonalność. Instalacja i aktywacja są wykonywane za pomocą programu **Plug-in Manager**.

Ważne

Nie jest konieczne instalowanie modułu Ochrona danych, jeśli oprogramowanie Zapobieganie utracie danych firmy Trend Micro jest już zainstalowane i uruchomione na punktach końcowych.

Instalacja modułu Ochrona danych

Procedura

1. Otwórz konsolę Web programu OfficeScan i kliknij polecenie **Dodatki** w menu głównym.

2. Na ekranie **Plug-in Manager** przejdź do sekcji **Usługa Ochrona danych OfficeScan** i kliknij przycisk **Pobieranie**.

   Rozmiar pliku do pobrania zostanie wyświetlony obok przycisku **Pobierz**.

   Program Plug-In Manager zapisuje pobrany plik w lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Download\Product`.

   Uwaga

   Jeśli program Plug-in Manager nie może pobrać pliku, wznowi automatycznie pobieranie po 24 godzinach. Aby ręcznie uruchomić pobieranie pliku przez program Plug-in Manager, uruchom ponownie usługę OfficeScan Plug-in Manager z poziomu konsoli Microsoft Management Console.

3. Monitoruj postęp pobierania.

   Można opuścić ten ekran podczas pobierania.

   W przypadku wystąpienia problemów podczas pobierania pliku należy sprawdzić dzienniki aktualizacji serwera w konsoli Web programu OfficeScan. W menu głównym kliknij opcję **Dzienniki** > **Aktualizacje serwera**.

   Po pobraniu pliku przez program Plug-in Manager zostanie wyświetlony nowy ekran z modułem Ochrona danych OfficeScan.

   Uwaga

   Jeśli ekran modułu Ochrona danych OfficeScan nie zostanie wyświetlony, sprawdź przyczyny i sposoby rozwiązania problemu w temacie *Rozwiązywanie problemów z programem Plug-in Manager na stronie 17-13*.

4. Aby od razu zainstalować program Usługa Ochrona danych OfficeScan, kliknij polecenie **Instaluj teraz**. Jeśli chcesz wykonać instalację później, wykonaj następujące czynności:

   a. Kliknij przycisk **Instaluj później**.

   b. Zostanie wyświetlony ekran **Plug-in Manager**.

   c. Przejdź do sekcji **Ochrona danych OfficeScan** i kliknij przycisk **Instaluj**.

5. Przeczytaj umowę licencyjną i zaakceptuj jej warunki, klikając przycisk **Akceptuję**.

   Rozpocznie się instalacja.

6. Monitoruj postęp instalacji. Po zakończeniu instalacji wyświetlona zostanie wersja modułu Ochrona danych OfficeScan.

Licencja Ochrona danych

Korzystając z programu Plug-in Manager, można wyświetlać, aktywować i odnawiać licencję Ochrona danych.

Kod aktywacyjny należy uzyskać z firmy Trend Micro, a następnie użyć go w celu aktywacji licencji.

Aktywowanie licencji dodatku Program dodatku

Procedura

1. Otwórz konsolę Web programu Program OfficeScan i kliknij polecenie **Dodatki** w menu głównym.
2. Na ekranie **Plug-in Manager** przejdź do sekcji dodatku i kliknij polecenie **Zarządzaj programem**.

   Zostanie wyświetlony ekran **Nowy kod aktywacyjny licencji produktu**.

3. Wpisz kod aktywacyjny lub skopiuj i wklej go do pól tekstowych.
4. Kliknij przycisk **Zapisz**.

   Zostanie wyświetlona konsola dodatku.

Wyświetlanie i odnawianie informacji o licencji

Procedura

1. Otwórz konsolę Web programu Program OfficeScan i kliknij polecenie **Dodatki** w menu głównym.
2. Na ekranie **Plug-in Manager** przejdź do sekcji dodatku i kliknij polecenie **Zarządzaj programem**.
3. Kliknij opcję **Wyświetl informacje o licencji**, aby wyświetlić informacje o aktualnej licencji w witrynie internetowej firmy Trend Micro.
4. Zapoznaj się ze następującymi szczegółami licencjami na wyświetlonym ekranie.

Opcja	Opis
Stan	Wyświetlana jest wartość „Aktywowane”, „Nieaktywowane” lub „Wygasłe”.
Wersja	Wyświetlana jest wartość „Pełna” lub „Próbna”. **Uwaga** Po aktywacji wersji pełnej i próbnej wyświetlana jest wersja „Pełna”.
Stanowiska	Wyświetla liczbę punktów końcowych, którymi może zarządzać program dodatku.
Licencja utraci ważność	Jeśli program dodatku ma przypisanych wiele licencji, jest wyświetlana najpóźniejsza data wygaśnięcia. Na przykład, jeśli licencje wygasają w dniach 31-12-2011 i 30-06-2011, wyświetlana jest data 31-12-2011.
Kod aktywacyjny	wyświetla kod aktywacyjny.
Przypomnienia	W zależności od bieżącej wersji licencji dodatek wyświetla przypomnienie o dacie utraty ważności licencji w ciągu okresu wstępnego (tylko w pełnej wersji) lub po utracie ważności licencji.

Uwaga

Czas trwania okresu próbnego różni się w zależności od regionu. Okres wstępny dodatku można sprawdzić u przedstawiciela firmy Trend Micro.

5. Aby zaktualizować zawartość ekranu na podstawie najnowszych informacji o licencji, kliknij opcję **Aktualizuj informacje**.

6. Kliknij polecenie **Nowy kod aktywacyjny**, aby otworzyć ekran **Nowy kod aktywacyjny licencji produktu**.

   Szczegółowe informacje zawiera sekcja *Aktywowanie licencji dodatku Program dodatku na stronie 3-4*.

Instalowanie modułu Ochrona danych na agentach OfficeScan

Moduł Ochrona danych należy zainstalować na agentach OfficeScan po aktywowaniu jego licencji. Po zakończeniu instalacji agenci OfficeScan rozpoczną użycie funkcji Zapobieganie utracie danych i kontroli urządzeń.

Ważne

- Moduł jest domyślnie wyłączony w systemach Windows Server 2003, Windows Server 2008 i Windows Server 2012, aby nie obniżać wydajności hosta. Po włączeniu modułu należy stale monitorować wydajność systemu i podjąć odpowiednie działanie w przypadku spadku wydajności.

  Moduł można włączyć lub wyłączyć z poziomu konsoli Web. Szczegółowe informacje zawiera sekcja *Usługi agenta OfficeScan na stronie 15-7*.

- Jeśli na punkcie końcowym zostało już zainstalowane oprogramowanie Zapobieganie utracie danych firmy Trend Micro, program OfficeScan nie zastąpi go modułem Ochrona danych.

- Agenci online instalują moduł Ochrona danych natychmiast. Agenci offline i w trybie niezależnym instalują moduł po ponownym nawiązaniu połączenia z serwerem OfficeScan.

- Użytkownicy muszą uruchomić ponownie swoje komputery, aby zakończyć instalację sterowników funkcji Zapobieganie utracie danych. Należy wcześniej poinformować użytkowników o konieczności ponownego uruchomienia komputerów.

- Firma Trend Micro zaleca włączenie funkcji rejestracji diagnostyki, które pomoże w rozwiązywaniu problemów z instalacją. Szczegółowe informacje zawiera sekcja *Włączanie rejestracji w dzienniku diagnostycznym w module Ochrona danych na stronie 11-67*.

Wdrożenie modułu Ochrona danych na agentach OfficeScan

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów można:

   - Kliknąć ikonę domeny głównej (), aby zainstalować moduł na wszystkich istniejących i przyszłych agentach.

   - Wybrać określoną domenę, aby zainstalować moduł na wszystkich istniejących i przyszłych agentach w domenie.

- Wybrać określonego agenta, aby zainstalować moduł tylko na tym agencie.

3. Zainstaluj moduł na jeden z dwóch sposobów:
   - Kliknij polecenie **Ustawienia** > **Ustawienia DLP**.
   - Kliknij polecenie **Ustawienia** > **Ustawienia kontroli urządzeń**.

Uwaga

Jeśli instalacja jest wykonywana na ekranie **Ustawienia** > **Ustawienia DLP**, a moduł Ochrona danych został zainstalowany pomyślnie, zostaną zainstalowane sterowniki kontroli zasobów cyfrowych. Po pomyślnym zainstalowaniu sterowników zostanie wyświetlony komunikat informujący użytkowników o konieczności ponownego uruchomienia punktów końcowych w celu zakończenia instalacji sterowników.

Jeśli komunikat ten nie został wyświetlony, mógł wystąpić problem z instalacją sterowników. Jeśli włączono funkcję rejestracji diagnostyki, można sprawdzić dzienniki diagnostyczne w celu uzyskania szczegółowych informacji dotyczących problemów z instalacją sterowników.

4. Zostanie wyświetlony komunikat wskazujący liczbę agentów, na których nie zainstalowano modułu. Kliknij przycisk **Tak**, aby rozpocząć instalację.

Uwaga

Po kliknięciu przycisku **Nie** (lub jeśli z jakiegoś powodu moduł nie został zainstalowany na co najmniej jednym agencie) ten sam komunikat zostanie wyświetlony po ponownym kliknięciu opcji **Ustawienia** > **Ustawienia DLP** lub **Ustawienia** > **Ustawienia kontroli urządzeń**.

Agenci OfficeScan rozpoczną pobieranie modułu z serwera.

5. Sprawdź, czy moduł został zainstalowany na agentach.
   a. Wybierz domenę w drzewie agentów.
   b. W widoku drzewa agentów wybierz opcję **Widok Ochrona danych** lub **Wyświetl wszystkie**.
   c. Sprawdź kolumnę **Stan Ochrona danych**. Możliwe stany instalacji są następujące:

- **Uruchomiono**: Moduł został zainstalowany pomyślnie, a jego funkcje są włączone.
- **Wymaga ponownego uruchomienia**: Sterowniki Zapobieganie utracie danych nie zostały zainstalowane, ponieważ użytkownicy nie uruchomili ponownie swoich komputerów. Jeśli sterowniki nie zostaną zainstalowane, Zapobieganie utracie danych nie będzie działać.
- **Zatrzymano**: Usługa modułu nie została uruchomiona lub docelowy punkt końcowy nie został prawidłowo wyłączony. Aby uruchomić Ochrona danych, przejdź do opcji **Agenci** > **Zarządzanie agentami** > **Ustawienia** > **Ustawienia dodatkowej usługi** i włącz Ochrona danych.
- **Nie można zainstalować**: Wystąpił problem podczas instalowania modułu na agencie. Konieczne będzie ponowne zainstalowanie modułu z poziomu drzewa agentów.
- **Nie można zainstalować (funkcja Zapobieganie utracie danych już działa)**: Jeśli na punkcie końcowym zostało już zainstalowane oprogramowanie Zapobieganie utracie danych firmy Trend Micro, program OfficeScan nie zastąpi go modułem Ochrona danych.
- **Niezainstalowany**: Moduł nie został zainstalowany na agencie. Ten stan jest wyświetlany, jeśli nie wybrano instalacji modułu na agencie, a także jeśli agent jest w stanie offline lub w trybie niezależnym podczas instalacji.

Folder ekspertyzy i baza danych DLP

Po wystąpieniu zdarzenia Zapobieganie utracie danych program OfficeScan zapisuje szczegóły zdarzenia w specjalnej bazie danych ekspertyzy. Program OfficeScan tworzy także zaszyfrowany plik zawierający kopię poufnych danych, które wyzwoliły zdarzenie, oraz generuje wartość hash na potrzeby weryfikacji i w celu zapewnienia integralności poufnych danych. Program OfficeScan tworzy zaszyfrowane pliki ekspertyzy na komputerze agenta, a następnie przesyła je do określonej lokalizacji na serwerze.

Ważne

- Zaszyfrowane pliki ekspertyzy zawierają bardzo poufne dane. Administratorzy powinny zachować ostrożność, przyznając dostęp do tych plików.
- Program OfficeScan integruje się z programem Control Manager, aby zapewnić użytkownikom programu Control Manager z rolami kontrolera zdarzeń DLP lub specjalisty ds. zgodności DLP możliwość dostępu do danych w zaszyfrowanych plikach. Szczegółowe informacje dotyczące ról DLP i dostępu do danych plików ekspertyzy w programie Control Manager zawiera *Podręcznik administratora programu Control Manager 6.0 poprawka 2* lub nowszego.

Modyfikowanie ustawień folderu i bazy danych ekspertyzy

Administratorzy mogą zmieniać lokalizację i harmonogram usuwania folderu ekspertyzy, a także maksymalny rozmiar plików przesyłanych przez agentów, modyfikując pliki INI programu OfficeScan.

OSTRZEŻENIE!

Zmiana lokalizacji folderu ekspertyzy po zarejestrowaniu przypadków Zapobieganie utracie danych może spowodować rozłączenie danych bazy danych i lokalizacji istniejących plików ekspertyzy. Firma Trend Micro.

Poniższa tabela przedstawia przegląd ustawień serwera dostępnych w pliku <*Folder instalacyjny serwera*>`\PCCSRV\Private\ofcserver.ini` na serwerze OfficeScan.

TABELA 3-1. Ustawienia folderu ekspertyzy na serwerze w pliku `PCCSRV\Private\ofcserver.ini`

CEL	USTAWIENIE INI	WARTOŚCI
Włączenie zdefiniowanej przez użytkownika lokalizacji folderu ekspertyzy	[INI_IDLP_SECTION] `EnableUserDefinedUploadFolder`	0: wyłącz (wartość domyślna) 1: włącz

CEL	USTAWIENIE INI	WARTOŚCI
Konfigurowanie zdefiniowanej przez użytkownika lokalizacji folderu ekspertyzy	[INI_IDLP_SECTION] `UserDefinedUploadFolder` **Uwaga** • Administratorzy muszą włączyć ustawienie `EnableUserDefinedUploadFolder`, zanim funkcja Zapobieganie utracie danych zastosuje to ustawienie. • Domyślna lokalizacja folderu ekspertyzy to: <*Folder instalacji serwera*>`\PCCSRV\Private\DLPForensicData` • Zdefiniowana przez użytkownika lokalizacja folderu ekspertyzy musi być dyskiem fizycznym (wewnętrznym lub zewnętrznym) na komputerze serwera. Program OfficeScan nie obsługuje mapowania lokalizacji dysku sieciowego.	Wartość domyślna: <Zastąp tę wartość zdefiniowaną przez klienta ścieżką do folderu. Przykład: C:\VolumeData\OfficeScanDlpForensicData> Wartość zdefiniowana przez użytkownika: musi stanowić fizyczną lokalizację dysku na komputerze serwera
Włączenie czyszczenia plików danych ekspertyzy	[INI_IDLP_SECTION] `ForensicDataPurgeEnable`	0: wyłącz 1: włącz (wartość domyślna)

CEL	USTAWIENIE INI	WARTOŚCI
Konfigurowanie częstotliwości kontroli czyszczenia plików danych ekspertyzy	[INI_IDLP_SECTION] `ForensicDataPurgeCheckFrequency` **Uwaga** • Administratorzy muszą włączyć ustawienie `ForensicDataPurgeEnable`, zanim program OfficeScan zastosuje to ustawienie. • Program OfficeScan usuwa pliki danych dopiero po przekroczeniu daty wygaśnięcia określonej w ustawieniu `ForensicDataExpiredPeriodInDays`.	1: co miesiąc, w pierwszym dniu miesiąca o godzinie 00:00 2: co tydzień (wartość domyślnie), w każdą niedzielę o godzinie 00:00 3: codziennie, o godzinie 00:00 4: co godzinę HH: 00
Konfigurowanie czasu przechowywania plików danych ekspertyzy na serwerze	[INI_IDLP_SECTION] `ForensicDataExpiredPeriodInDays`	Wartość domyślna (w dniach): 180 Wartość minimalna: 1 Wartość maksymalna: 3650
Konfigurowanie częstotliwości kontroli miejsca na dysku dla plików ekspertyzy	[INI_SERVER_DISK_THRESHOLD] `MonitorFrequencyInSecond` **Uwaga** Jeśli dostępna ilość miejsca w folderze danych ekspertyzy jest mniejsza niż wartość skonfigurowana w ustawieniu `InformUploadOnDiskFreeSpaceInGb`, program OfficeScan zapisuje dziennik zdarzeń w konsoli Web.	Wartość domyślna (w sekundach): 5

CEL	USTAWIENIE INI	WARTOŚCI
Konfigurowanie częstotliwości przesyłania dla kontroli miejsca na dysku dla plików ekspertyzy	[INI_SERVER_DISK_THRESHOLD] `IsapiCheckCountInRequest` **Uwaga** Jeśli dostępna ilość miejsca w folderze danych ekspertyzy jest mniejsza niż wartość skonfigurowana w ustawieniu `InformUploadOnDiskFreeSpaceInGb`, program OfficeScan zapisuje dziennik zdarzeń w konsoli Web.	Wartość domyślna (liczba plików): 200
Konfigurowanie minimalnej ilości miejsca na dysku, która powoduje wyzwolenie powiadomienia o ograniczonym miejscu na dysku	[INI_SERVER_DISK_THRESHOLD] `InformUploadOnDiskFreeSpaceInGb` **Uwaga** Jeśli dostępna ilość miejsca w folderze danych ekspertyzy jest mniejsza niż skonfigurowana wartość, program OfficeScan zapisuje dziennik zdarzeń w konsoli Web.	Wartość domyślna (w GB): 10
Konfigurowanie minimalnej ilości miejsca dostępnej na potrzeby przesyłania plików danych ekspertyzy z agentów	[INI_SERVER_DISK_THRESHOLD] `RejectUploadOnDiskFreeSpaceInGb` **Uwaga** Jeśli dostępna ilość miejsca w folderze danych ekspertyzy jest mniejsza niż skonfigurowana wartość, agenci OfficeScan nie przesyłają plików danych ekspertyzy na serwer, a program OfficeScan zapisuje dziennik zdarzeń w konsoli Web.	Wartość domyślna (w GB): 1

W poniższej tabeli przedstawiono przegląd ustawień agenta OfficeScan dostępnych w pliku <*Folder instalacji serwera*>`\PCCSRV\ofcscan.ini` na serwerze OfficeScan.

TABELA 3-2. Ustawienia plików ekspertyzy dla Agentów w pliku `PCCSRV\ofcscan.ini`

CEL	USTAWIENIE INI	WARTOŚCI
Włączenie przesyłania plików danych ekspertyzy na serwer	`UploadForensicDataEnable`	0: wyłącz 1: włącz (wartość domyślna)
Konfigurowanie maksymalnego rozmiaru plików przesyłanych przez agenta OfficeScan na serwer	`UploadForensicDataSizeLimitInMb` **Uwaga** Agent OfficeScan wysyła na serwer pliki o rozmiarze mniejszym niż ta wartość.	Wartość domyślna (w MB): 10 Wartość minimalna: 1 Wartość maksymalna: 2048
Konfigurowanie czasu przechowywania plików danych ekspertyzy na agencie OfficeScan	`ForensicDataKeepDays` **Uwaga** Agent OfficeScan usuwa pliki danych ekspertyzy, które przekroczyły datę wygaśnięcia, codziennie o godzinie 11:00.	Wartość domyślna (w dniach): 180 Wartość minimalna: 1 Wartość maksymalna: 3650
Konfigurowanie częstotliwości, z jaką Agent OfficeScan sprawdza połączenie z serwerem	`ForensicDataDelayUploadFrequenceInMinutes` **Uwaga** Agenci OfficeScan, którzy nie mogą przesłać plików ekspertyzy na serwer, automatycznie ponawiają próbę wysłania plików zgodnie z określonym interwałem.	Wartość domyślna (w minutach): 5 Wartość minimalna: 5 Wartość maksymalna: 60

Tworzenie kopii zapasowej danych ekspertyzy

W zależności od zasad bezpieczeństwa firmy, czas przechowywania danych ekspertyzy może się znacząco różnić. Aby zwolnić miejsce na dysku serwera, firma Trend Micro

zaleca ręczne tworzenie kopii zapasowej danych w folderze ekspertyzy i bazy danych ekspertyzy.

Procedura

1. Przejdź do lokalizacji folderu danych ekspertyzy na serwerze.
   - Lokalizacja domyślna: < *Folder instalacji serwera*>`\PCCSRV\Private \DLPForensicData`
   - Aby znaleźć dostosowaną lokalizację folderu ekspertyzy, patrz sekcja *Konfigurowanie zdefiniowanej przez użytkownika lokalizacji folderu ekspertyzy na stronie 3-11*.
2. Skopiuj folder do nowej lokalizacji.
3. Aby ręcznie utworzyć kopię zapasową bazy danych ekspertyzy, przejdź do folderu <*Folder instalacji serwera*>`\PCCSRV\Private`.
4. Skopiuj plik `DLPForensicDataTracker.db` do nowej lokalizacji.

Dezinstalacja modułu Ochrona danych

Jeśli moduł Ochrona danych zostanie zdezinstalowany z programu Plug-in Manager:

- Wszystkie parametry konfiguracyjne, ustawienia i dzienniki funkcji Zapobieganie utracie danych zostaną usunięte z serwera OfficeScan.
- Wszystkie konfiguracje i ustawienia kontroli urządzeń, które są zapewniane przez moduł Ochrona danych, zostaną usunięte z serwera.
- Moduł Ochrona danych zostanie usunięty z agentów. W celu pełnego usunięcia Ochrona danych należy ponownie uruchomić punkty końcowe agentów.
- Reguły Zapobieganie utracie danych nie będą już egzekwowane na agentach.
- Kontrola urządzeń nie będzie już monitorować dostępu do następujących urządzeń:

- Adaptery Bluetooth
- Porty COM i LPT
- Interfejs IEEE 1394
- Urządzenia do przetwarzania obrazu
- Urządzenia na podczerwień
- Modemy
- Karty PCMCIA
- Klawisz Print Screen
- Karty sieci bezprzewodowej

W dowolnym momencie możesz ponownie zainstalować moduł Ochrona danych. Po ponownym zainstalowaniu należy aktywować licencję przy użyciu prawidłowego kodu aktywacyjnego.

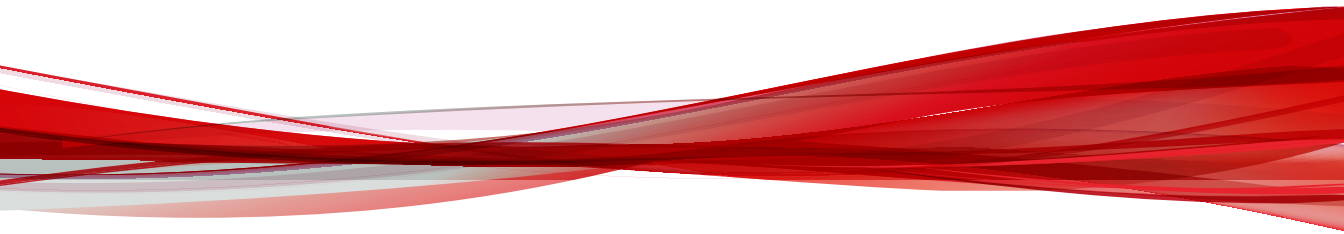
Dezinstalacja modułu Ochrona danych z programu Plug-in Manager

Procedura

1. Otwórz konsolę Web programu OfficeScan i kliknij polecenie **Dodatki** w menu głównym.
2. Na ekranie **Plug-in Manager** przejdź do sekcji **Usługa Ochrona danych OfficeScan** i kliknij przycisk **Odinstalujl**.
3. Monitoruj postęp odinstalowywania. Można opuścić ten ekran podczas dezinstalacji.
4. Odśwież ekran **Plug-in Manager** po zakończeniu dezinstalacji. Moduł Ochrona danych OfficeScan będzie ponownie dostępny w celu instalacji.

Część II

Ochrona agentów OfficeScan



Rozdział 4

Korzystanie z usługi Trend Micro Smart Protection

W tym rozdziale opisano rozwiązania Trend Micro Smart Protection oraz sposób, w jaki należy skonfigurować środowisko wymagane do korzystania z tych rozwiązań.

Rozdział składa się z następujących tematów:

Informacje o usłudze Trend Micro Smart Protection

Usługa Smart Protection firmy Trend Micro™ to nowoczesna infrastruktura zabezpieczeń zasobów klientów pracujących w chmurze zaprojektowana w celu ochrony klientów przed zagrożeniami bezpieczeństwa i zagrożeniami internetowymi. Współpracuje zarówno z rozwiązaniami lokalnymi, jak i zarządzanymi, zapewniając użytkownikom ochronę niezależnie od tego, czy znajdują się w sieci, w domu czy w podróży. Wykorzystuje niewielkich agentów, którzy uzyskują dostęp do unikatowych, zlokalizowanych w chmurze wiadomości e-mail, technologii Web Reputation i File Reputation oraz do baz danych dotyczących zagrożeń. Ochrona klientów jest automatycznie aktualizowana i wzmacniania w miarę zwiększania się liczby produktów, usług i użytkowników w sieci, tworzących usługę ochrony w czasie rzeczywistym dla swoich użytkowników.

Dzięki połączeniu technologii oceny reputacji, skanowania i korelacji w chmurze rozwiązanie Smart Protection firmy Trend Micro ogranicza konieczność pobierania konwencjonalnych plików sygnatur i eliminuje opóźnienia związane zwykle z pobieraniem aktualizacji.

Potrzeba nowego rozwiązania

W stosowanym obecnie podejściu do obsługi zagrożeń związanych z plikami, sygnatury (bądź definicje) wymagane do ochrony punktów końcowych są, w większości przypadków, dostarczane zgodnie z harmonogramem. Sygnatury są dostarczane do agentów w postaci pakietów wydawanych przez firmę Trend Micro. Po otrzymaniu nowej aktualizacji, oprogramowanie ochrony przed wirusami/złośliwym oprogramowaniem zainstalowane na agencie wczytuje ten pakiet sygnatur i definicji nowych wirusów/złośliwego oprogramowania do pamięci. W przypadku pojawienia się nowego zagrożenia związanego z wirusami/złośliwym oprogramowaniem plik sygnatur musi być ponownie — częściowo lub w całości — zaktualizowany i wczytany do pamięci agenta w celu zapewnienia ciągłości ochrony.

Z czasem wolumen pojawiających się unikatowych zagrożeń uległ znaczącemu zwiększeniu. Przewiduje się, że w najbliższych latach wolumen zagrożeń będzie wzrastał w postępie prawie wykładniczym. Równa się to stopie wzrostu, która w znaczącym stopniu przewyższa wolumen obecnie znanych zagrożeń bezpieczeństwa. W przyszłości

wolumen zagrożeń bezpieczeństwa stanie się nowym typem zagrożenia bezpieczeństwa. Wolumen zagrożeń bezpieczeństwa może wywierać wpływ na wydajność serwera i stacji roboczej, zużycie przepustowości sieci oraz całkowity czas potrzebny na zapewnienie wysokiej jakości ochrony - lub „czas na zapewnienie ochrony".

Firma Trend Micro jest pionierem nowego podejścia do obsługi dużej ilości zagrożeń. Celem firmy Trend Micro jest uodpornienie swoich klientów na zagrożenia ze strony wirusów/złośliwego oprogramowania. Technologia i architektura zastosowana w tym pionierskim rozwiązaniu wykorzystuje technologię, która pozwala przechowywać sygnatury i definicje wirusów/złośliwego oprogramowania w chmurze. Przechowywanie sygnatur i definicji wirusów/złośliwego oprogramowania w chmurze pozwala firmie Trend Micro lepiej chronić klientów przed wzrostem wolumenu pojawiających się zagrożeń bezpieczeństwa.

Usługi Smart Protection

Usługi Smart Protection zawierają usługi, które dostarczają sygnatury złośliwego oprogramowania, informacje dotyczące usługi Web Reputation oraz bazy danych zagrożeń, które są zapisane w chmurze.

Dostępne są następujące usługi Smart Protection:

- **Usługi File Reputation Services**: usługi File Reputation Services umożliwiają przeniesienie dużej liczby sygnatur złośliwego oprogramowania, które wcześniej były przechowywane na komputerach agentów, na źródła programu Smart Protection.

  Szczegółowe informacje zawiera sekcja *Usługi File Reputation Services na stronie 4-4*.

- **Usługi Web Reputation Services**: usługi Web Reputation Services umożliwiają obsługę przez lokalne źródła programu Smart Protection danych reputacji adresów URL, które wcześniej były obsługiwane wyłącznie przez firmę Trend Micro. Obie technologie zapewniają niższe zużycie przepustowości sieci podczas aktualizacji sygnatur lub sprawdzania adresów URL.

  Szczegółowe informacje zawiera sekcja *Usługi Web Reputation Services na stronie 4-4*.

- **Smart Feedback**: firma Trend Micro aktywnie rozpoznaje nowe zagrożenia, gromadząc anonimowe informacje przesyłane przez jej produkty z całego świata.

Szczegółowe informacje zawiera sekcja *Smart Feedback na stronie 4-5*.

Usługi File Reputation Services

Usługi File Reputation Services sprawdzają reputację każdego pliku, porównując ją ze zlokalizowaną w chmurze bazą danych. Ponieważ informacje na temat złośliwego oprogramowania znajdują się wewnątrz chmury, są one bezpośrednio dostępne dla wszystkich użytkowników. Podczas procesu weryfikacji minimalny czas opóźnienia gwarantują wysokowydajne sieci dostarczające treści oraz lokalne serwery rekursywne. Architektura agenta chmury zapewnia natychmiastową ochronę i eliminuje obciążenie związane z obsługą sygnatur, oszczędzając jednocześnie miejsce na dysku agenta.

Agenci muszą działać w trybie Smart Scan, aby możliwe było użycie usług File Reputation Services. Tacy agenci są określani w niniejszym dokumencie jako agenci Smart Scan. Agenci, którzy nie działają w trybie Smart Scan, nie używają usług File Reputation Services i są nazywani agentami skanowania standardowego. Administratorzy programu OfficeScan mogą skonfigurować wszystkich lub niektórych agentów do działania w trybie Smart Scan.agenciagenci

Usługi Web Reputation Services

Technologia Web Reputation firmy Trend Micro, wyposażona w jedną z największych baz danych reputacji domen na świecie, śledzi informacje na temat wiarygodności domen sieci Web, przypisując im ocenę reputacji na podstawie takich czynników, jak czas działania witryny w sieci Web, historyczne zmiany jej lokalizacji oraz symptomy podejrzanych działań wykryte za pomocą mechanizmów analizy zachowania złośliwego oprogramowania. Usługa Web Reputation następnie skanuje witryny i blokuje użytkownikom dostęp do zarażonych. Funkcje usługi Web Reputation pozwalają upewnić się, że strony otwierane przez użytkowników są bezpieczne i wolne od zagrożeń, takich jak złośliwe oprogramowanie, spyware i wyłudzanie informacji (tzw. phishing), tj. oszustwa mające na celu uzyskanie danych osobowych użytkownika. Aby zwiększyć dokładność i zmniejszyć liczbę fałszywych alarmów, technologia Web Reputation firmy Trend Micro nie klasyfikuje ani nie blokuje całych witryn, lecz przypisuje oceny reputacji poszczególnym stronom i osadzonym w nich łączom. Jest to lepsze rozwiązanie, ponieważ zdarza się, że atakom ulegają jedynie części wiarygodnych witryn, a reputacja może się dynamicznie zmieniać w czasie.

Agenci OfficeScan używający usług Web Reputation Services podlegają regułom Web Reputation. Administratorzy programu OfficeScan mogą zastosować reguły usług Web Reputation Services do wszystkich lub wybranych agentów.

Smart Feedback

Funkcja Trend Micro Smart Feedback zapewnia stałą komunikację między produktami firmy Trend Micro a działającymi przez całą dobę, siedem dni w tygodniu, centrami i technologiami analizy zagrożeń. Każde nowe zagrożenie rozpoznane za pomocą pojedynczego rutynowego sprawdzania oceny reputacji po stronie klienta automatycznie aktualizuje wszystkie bazy zagrożeń firmy Trend Micro, zapobiegając wyrządzeniu szkody przez to zagrożenie kolejnym klientom.

Dzięki ciągłemu przetwarzaniu informacji o zagrożeniach zbieranych w rozległej sieci klientów i partnerów firma Trend Micro zapewnia automatyczną ochronę w czasie rzeczywistym przed najnowszymi zagrożeniami oraz bezpieczeństwo w stylu „razem lepiej", podobnie do systemu straży sąsiedzkiej, który w celu ochrony innych angażuje członków społeczności. Poufność osobistych i biznesowych danych klienta jest zawsze chroniona, ponieważ gromadzenie informacji o zagrożeniach odbywa się na podstawie oceny reputacji źródła komunikacji, a nie zawartości określonej komunikacji.

Przykładowe informacje przesyłane do firmy Trend Micro:

- Sumy kontrolne plików
- Wyświetlane witryny internetowe
- Informacje o plikach, w tym rozmiary i ścieżki dostępu
- Nazwy plików wykonywalnych

Z uczestnictwa w programie można w dowolnej chwili zrezygnować z poziomu konsoli Web.

Porada

W celu zapewnienia ochrony punktów końcowych nie jest wymagany udział w programie Smart Feedback. Uczestnictwo jest opcjonalne i można się z niego w każdej chwili wycofać. Firma Trend Micro zaleca wzięcie udziału w programie Smart Feedback. Pozwoli to zapewnić wyższy poziom ochrony dla wszystkich klientów Trend Micro.

Więcej informacji na temat infrastruktury Smart Protection Network można uzyskać w witrynie internetowej:

http://www.trendmicro.pl/technology-innovation/our-tech/smart-protection-network/index.html

Źródła Smart Protection

Firma Trend Micro zapewnia usługi File Reputation Services i Web Reputation Services dla programu OfficeScan i źródeł Smart Protection.

Źródła programu Smart Protection zapewniają usługi File Reputation Services, udostępniając większość definicji sygnatur wirusów/złośliwego oprogramowania. Pozostałe definicje znajdują się na agentach OfficeScan. Agent wysyła żądania skanowania do źródeł programu Smart Protection, jeśli własne definicje sygnatur nie umożliwiają określenia ryzyka związanego z plikiem. Źródła Smart Protection określają ryzyko przy użyciu informacji identyfikacyjnych.

Źródła Smart Protection zapewniają usługi Web Reputation Services, udostępniając dane usługi Web Reputation, które wcześniej były dostępne tylko na serwerach obsługiwanych przez firmę Trend Micro. Agent wysyła zapytania usługi Web Reputation do źródeł programu Smart Protection w celu sprawdzenia reputacji witryn internetowych, do których użytkownik próbuje uzyskać dostęp. Agent dopasowuje reputację witryny internetowej do określonej reguły Web Reputation, która jest egzekwowana na punkcie końcowym w celu określenia, czy dostęp do witryny zostanie zablokowany, czy dozwolony.

To, z którym źródłem programu Smart Protection agent łączy się, zależy od jego lokalizacji. Agencimogą łączyć się z siecią Trend Micro Smart Protection Network lub serwerem Smart Protection.

Trend Micro™ Smart Protection Network™

Trend Micro™ Smart Protection Network™ to nowoczesna infrastruktura zabezpieczeń zasobów klientów pracujących w chmurze zaprojektowana w celu ochrony klientów przed zagrożeniami bezpieczeństwa i zagrożeniami internetowymi. Sieć zwiększa wydajność lokalnych i obsługiwanych przez firmę Trend Micro rozwiązań w celu

ochrony użytkowników niezależnie od tego, czy są podłączeni do sieci, pracują w domu czy w podróży. Sieć Smart Protection Network za pomocą prostszych agentów daje dostęp do unikatowej, zlokalizowanej w chmurze kombinacji technologii poczty e-mail, sieci Web i usługi File Reputation oraz baz danych zagrożeń. Ochrona klientów jest automatycznie aktualizowana i wzmacniania w miarę zwiększania się liczby produktów, usług i użytkowników w sieci, tworzących usługę ochrony w czasie rzeczywistym dla swoich użytkowników.

Więcej informacji na temat infrastruktury Smart Protection Network można uzyskać w witrynie internetowej:

http://www.trendmicro.pl/technology-innovation/our-tech/smart-protection-network/index.html

Serwer Smart Protection

serwery Smart Protection są przeznaczone dla użytkowników z bezpośrednim dostępem do lokalnej sieci firmowej. Usługi Smart Protection services realizowane są w sieci firmowej w celu zapewnienia optymalnej wydajności.

Istnieją dwa rodzaje serwerów Smart Protections:

- **Zintegrowany Serwer Smart Protection**: program instalacyjny OfficeScan Setup zawiera zintegrowany Serwer Smart Protection, który jest instalowany na tym samym punkcie końcowym co serwer OfficeScan. Po instalacji ustawieniami tego serwera można zarządzać z poziomu konsoli Web programu OfficeScan. Serwer zintegrowany jest przeznaczony dla instalacji programu OfficeScan na małą skalę. W przypadku większych instalacji wymagany jest samodzielny Serwer Smart Protection.
- **Samodzielny Serwer Smart Protection**: samodzielny Serwer Smart Protection jest instalowany na serwerze VMware lub Hyper-V. Serwer samodzielny ma oddzielną konsolę zarządzania i jest obsługiwany z poziomu konsoli Web programu OfficeScan.

Porównanie źródeł Smart Protection

Poniższa tabela zawiera podsumowanie różnic między siecią Smart Protection Network a serwerem Smart Protection.

TABELA 4-1. Porównanie źródeł Smart Protection

PODSTAWA PORÓWNANIA	SERWER SMART PROTECTION	TREND MICRO SMART PROTECTION NETWORK
Dostępność	Dostępne dla agentów wewnętrznych, czyli agentów spełniających kryteria lokalizacji określone w konsoli Web programu OfficeScan.	Dostępne głównie dla agentów zewnętrznych, czyli agentów niespełniających kryteriów lokalizacji określonych w konsoli Web programu OfficeScan.
Przeznaczenie	Przeznaczony do optymalizacji wydajności przez realizację usług Smart Protection w sieci korporacyjnej	Globalnie skalowana infrastruktura internetowa udostępniająca usługi Smart Protection agentom, którzy nie posiadają bezpośredniego dostępu do swojej sieci firmowej
Administracja	Administratorzy OfficeScan mogą instalować te źródła Smart Protection i zarządzać nimi	To źródło jest obsługiwane przez firmę Trend Micro
Źródło aktualizacji sygnatury	Trend Micro ActiveUpdate Server	Trend Micro ActiveUpdate Server
Protokoły połączenia Agenta	HTTP i HTTPS	HTTPS

Pliki sygnatur Smart Protection

Pliki sygnatur Smart Protection są używane przez usługi File Reputation Services i Web Reputation Services. Firma Trend Micro udostępnia te pliki sygnatur za pośrednictwem serwera Trend Micro ActiveUpdate Server.

Sygnatura Agenta Smart Scan

Sygnatura Agenta Smart Scan jest aktualizowana codziennie i pobierana przez źródło aktualizacji agentów OfficeScan (serwer OfficeScan lub niestandardowe źródło aktualizacji). Źródło aktualizacji wdraża następnie sygnaturę na agentach Smart Scan.

Uwaga

Agenci Smart Scan to Agenci OfficeScan skonfigurowani przez administratorów do korzystania z usług File Reputation Services. Agenci, którzy nie korzystają z usług File Reputation Services, są nazywani agentami skanowania standardowego.

Agenci Smart Scan używają sygnatura Agenta Smart Scan podczas skanowania w poszukiwaniu zagrożeń bezpieczeństwa. Jeśli ta sygnatura nie umożliwia określenia zagrożenia związanego z plikiem, używana jest inna sygnatura o nazwie Sygnatury Smart Scan.

Sygnatury Smart Scan

Sygnatury Smart Scan jest aktualizowana co godzinę i pobierana przez źródła Smart Protection. Agenci Smart Scan nie pobierają tej sygnatury. Agenci weryfikują potencjalne zagrożenia względem sygnatury Smart Scan, wysyłając żądania skanowania do źródeł programu Smart Protection.

Lista blokowania Web

Lista blokowania sieci jest pobierana przez źródła programu Smart Protection. Agenci OfficeScan, którzy podlegają regułom usługi Web Reputation, nie pobierają listy blokowania sieci.

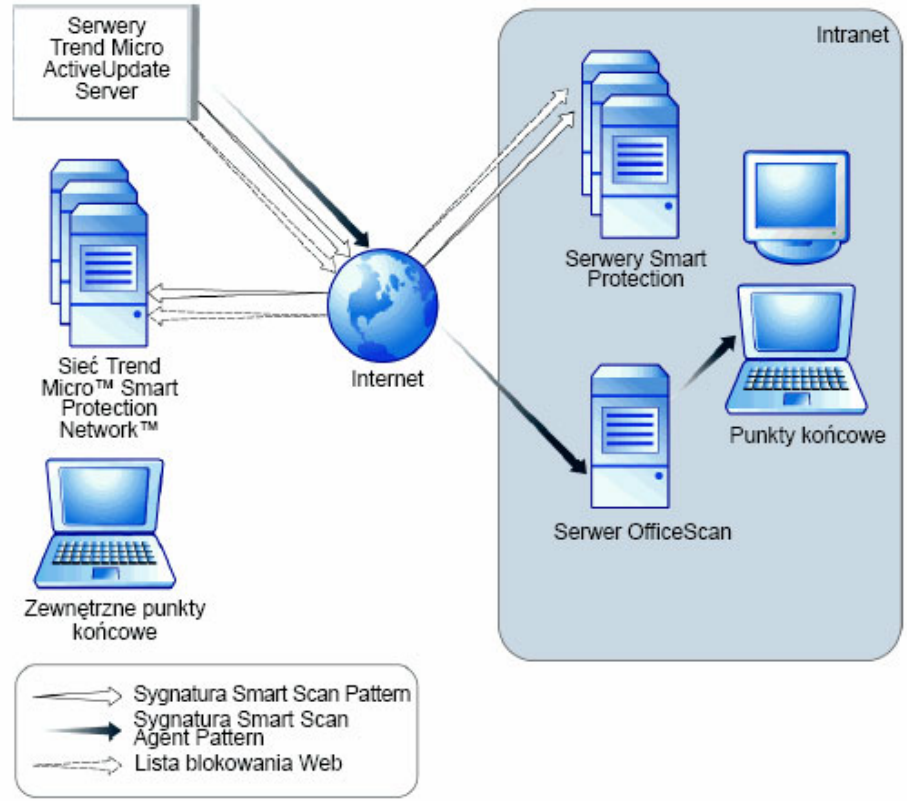
Uwaga

Administratorzy mogą zastosować reguły usługi Web Reputation do wszystkich lub wybranych agentów.

Agenci objęci regułami usługi Web Reputation weryfikują reputację witryny internetowej względem listy blokowania sieci, wysyłając zapytania usługi Web Reputation do źródła programu Smart Protection. Agent dopasowuje dane reputacji otrzymane ze źródła programu Smart Protection do reguły Web Reputation egzekwowanej na punkcie końcowym. W zależności od reguły agent blokuje lub zezwala na dostęp do witryny internetowej.

Proces aktualizacji sygnatury programu Smart Protection

Aktualizacje sygnatur Smart Protection Pattern są odbierane z serwera Trend Micro ActiveUpdate Server.



ILUSTRACJA 4-1. Proces aktualizacji sygnatur

Korzystanie z sygnatur programu Smart Protection

Agent OfficeScan używa sygnatura Agenta Smart Scan do skanowania w poszukiwaniu zagrożeń bezpieczeństwa i sprawdza sygnatury Smart Scan tylko w przypadku, gdy

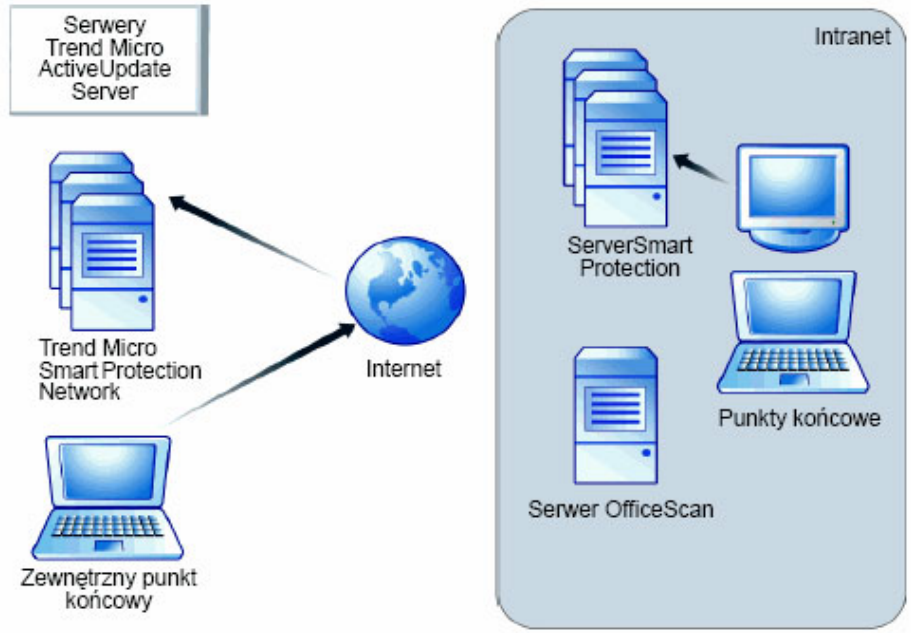
sygnatura Agenta Smart Scan nie może określić ryzyka związanego z plikiem. Agent sprawdza listę blokowania sieci, kiedy użytkownik próbuje uzyskać dostęp do witryny internetowej. Technologia filtrowania zaawansowanego pozwala agentowi „buforować" wyniki zapytania. Eliminuje to konieczność wielokrotnego wysyłania tego samego zapytania.

Agenci znajdujący się w sieci intranet mogą nawiązać połączenie z serwerem Smart Protection, aby sprawdzić sygnatury Smart Scan lub listę blokowania sieci. W celu połączenia z serwerem Smart Protection wymagane jest połączenie sieciowe. Jeśli skonfigurowano więcej niż jeden Serwer Smart Protection, administratorzy mogą określić priorytet połączenia.

Porada

Zaleca się zainstalowanie wielu serwerów Smart Protection, aby zapewnić ciągłość ochrony w razie utraty połączenia z serwerem Smart Protection.

Agenci, którzy nie są w sieci intranet, mogą łączyć się z siecią Trend Micro Smart Protection Network do wykonywania zapytań. W celu połączenia z serwerem Smart Protection Network wymagane jest połączenie internetowe.



ILUSTRACJA 4-2. Proces przeszukiwania

Agenci bez dostępu do sieci lub Internetu mogą skorzystać z ochrony zapewnianej przez sygnatura Agenta Smart Scan i pamięć podręczną zawierającą wyniki wcześniejszych zapytań. Poziom ochrony zostaje obniżony tylko w przypadku, gdy wymagane jest nowe zapytanie, a agent po wykonaniu wielu prób nie może nawiązać połączenia z żadnym źródłem programu Smart Protection. W takiej sytuacji agent oznacza flagą plik do weryfikacji i tymczasowo zezwala na dostęp do niego. Po przywróceniu połączenia ze źródłem Smart Protection wszystkie pliki oznaczone flagami są ponownie skanowane. Po czym wykonywane są odpowiednie czynności na plikach, które zostaną określone jako zagrożone.

Poniższa tabela zawiera podsumowanie poziomu ochrony zapewnianego na podstawie lokalizacji agenta.

TABELA 4-2. Zachowania ochrony oparte na lokalizacji

LOKALIZACJA	PLIK SYGNATURY I ZAPYTAŃA ZACHOWANIA
Uzyskanie dostępu do sieci intranet	• **Plik sygnatur**: agenci pobierają plik sygnatura Agenta Smart Scan z serwera OfficeScan lub niestandardowego źródła aktualizacji. • **zapytania do pliku i usługi Web Reputation**: agenci łączą się z serwerem Smart Protection w celu wykonywania zapytań.
Bez dostępu do sieci intranet, ale z połączeniem do sieci Smart Protection Network	• **Plik sygnatur**: agenci nie pobierają najnowszego pliku sygnatura Agenta Smart Scan, jeśli nie jest dostępne połączenie z serwerem OfficeScan lub niestandardowym źródłem aktualizacji. • **zapytania do pliku i usługi Web Reputation**: agenci łączą się z siecią Smart Protection Network w celu wykonywania zapytań.
Bez dostępu do sieci intranet i bez połączenia z siecią Smart Protection Network	• **Plik sygnatur**: agenci nie pobierają najnowszego pliku sygnatura Agenta Smart Scan, jeśli nie jest dostępne połączenie z serwerem OfficeScan lub niestandardowym źródłem aktualizacji. • **zapytania do pliku i usługi Web Reputation**: agenci nie otrzymują wyników zapytań i muszą korzystać wyłącznie z pliku sygnatura Agenta Smart Scan oraz pamięci podręcznej zawierającej wyniki wcześniejszych zapytań.

Konfigurowanie usług Smart Protection

Zanim agenci będą mogli korzystać z usług File Reputation Services i Web Reputation Services, należy upewnić się, że środowisko Smart Scan zostało skonfigurowane prawidłowo. Sprawdź następujące elementy:

- *Instalacja serwera Smart Protection na stronie 4-14*
- *Zarządzanie zintegrowanym serwerem Smart Protection na stronie 4-19*
- *Lista źródeł Smart Protection na stronie 4-23*

- *Ustawienia proxy dla połączenia agenta na stronie 4-32*
- *Instalacja usługi Trend Micro Network VirusWall na stronie 4-32*

Instalacja serwera Smart Protection

Jeśli liczba agentów nie przekracza 1000, można zainstalować zintegrowany lub samodzielny Serwer Smart Protection. Samodzielny Serwer Smart Protection należy zainstalować, jeśli liczba agentów przekracza 1000.

Firma Trend Micro zaleca zainstalowanie kilku serwerów Smart Protection na potrzeby awaryjnego przekazywania zadań. Agenci, którzy nie mogą się połączyć z określonym serwerem, będą próbować nawiązać połączenie z innymi skonfigurowanymi serwerami.

Ponieważ serwer zintegrowany i serwer OfficeScan są uruchomione na tym samym punkcie końcowym, jego wydajność może się znacznie pogorszyć podczas największego obciążenia obu serwerów. Należy rozważyć korzystanie z samodzielnego serwera Smart Protection jako głównego źródła programu Smart Protection i z serwera zintegrowanego jako źródła zapasowego.

Instalacja samodzielnego serwera Smart Protection

Instrukcje instalacji samodzielnego serwera Smart Protection i zarządzania nim zawiera *Podręcznik instalacji oraz uaktualniania serwera Smart Protection*.

Instalacja zintegrowanego serwera Smart Protection

Jeśli podczas instalacji serwera OfficeScan zainstalowano serwer zintegrowany:

- Włącz serwer zintegrowany i skonfiguruj jego ustawienia. Szczegółowe informacje zawiera sekcja *Zarządzanie zintegrowanym serwerem Smart Protection na stronie 4-19*.
- Jeśli serwer zintegrowany i Agent OfficeScan istnieją na tym samym komputerze serwera, rozważ wyłączenie zapory programu OfficeScan. Zapora programu OfficeScan jest przeznaczona do użytku przez punkt końcowy agenta, jego włączenie może wpływać na wydajność serwerów. Instrukcje dotyczące wyłączania zapory zawiera temat *Włączanie lub wyłączanie zapory programu OfficeScan na stronie 13-6*.

Uwaga

Należy rozważyć skutki wyłączenia zapory i upewnić się, że jest to zgodne z programami zabezpieczeń.

Porada

Zainstaluj zintegrowany Serwer Smart Protection po zakończeniu instalacji programu OfficeScan, wykorzystując do tego celu *Narzędzie zintegrowanego serwera Smart Protection na stronie 4-15*.

Narzędzie zintegrowanego serwera Smart Protection

Narzędzie Trend Micro OfficeScan Integrated Smart Protection ułatwia administratorom instalowanie i odinstalowywanie zintegrowanego serwera Smart Protection po zakończeniu instalacji serwera OfficeScan. Aktualna wersja programu OfficeScan nie pozwala administratorom na instalowanie/usuwanie zintegrowanego serwera Smart Protection po zakończeniu instalacji programu OfficeScan. Narzędzie to zwiększa elastyczność funkcji instalacji z poprzednich wersji programu OfficeScan.

Procedura

1. Otwórz wiersz polecenia i przejdź do katalogu <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\ISPSInstaller`, w którym znajduje się plik `ISPSInstaller.exe`.

2. Uruchom plik `ISPSInstaller.exe` za pomocą jednego z następujących poleceń:

TABELA 4-3. Opcje instalatora

POLECENIE	OPIS
`ISPSInstaller.exe /i`	Instaluje zintegrowany Serwer Smart Protection przy użyciu domyślnych ustawień portów. Szczegółowe informacje dotyczące domyślnych ustawień portów przedstawiono w poniższej tabeli.

POLECENIE	OPIS
`ISPSInstaller.exe /i /f:[numer portu] /s:[numer portu] /w:[numer portu]`	Instaluje zintegrowany serwer Serwer Smart Protection z użyciem określonych portów. **Uwaga** Porty można skonfigurować tylko przy korzystaniu z serwera sieci Web Apache. Gdzie: • `/f:[numer portu]` reprezentuje port HTTP usługi File Reputation • `/s:[numer portu]` reprezentuje port HTTPS usługi File Reputation • `/w:[numer portu]` reprezentuje port usługi Web Reputation **Uwaga** Nieokreślonemu portowi jest automatycznie przypisywana wartość domyślna.
`ISPSInstaller.exe /u`	Odinstalowuje zintegrowany serwer Serwer Smart Protection

TABELA 4-4. Porty usług Reputation Services zintegrowanego serwera Smart Protection

SERWER WEB I USTAWIENIA	PORTY USŁUG FILE REPUTATION SERVICES		PORT HTTP DLA USŁUG WEB REPUTATION SERVICES
	HTTP	HTTPS (SSL)	
Domyślna witryna internetowa programu IIS z włączonym protokołem SSL	80	443 (brak możliwości konfiguracji)	80 (brak możliwości konfiguracji)

Serwer Web i ustawienia	Porty usług File Reputation Services		Port HTTP dla usług Web Reputation Services
	HTTP	HTTPS (SSL)	
Domyślna witryna internetowa programu IIS z wyłączonym protokołem SSL	80	443 (brak możliwości konfiguracji)	80 (brak możliwości konfiguracji)
Wirtualna witryna internetowa programu IIS z włączonym protokołem SSL	8080	4343 (możliwość konfiguracji)	8080 (możliwość konfiguracji)
Wirtualna witryna internetowa programu IIS z wyłączonym protokołem SSL	8080	4343 (możliwość konfiguracji)	8080 (możliwość konfiguracji)

3. Po zakończeniu instalacji otwórz konsolę Web programu OfficeScan i wykonaj następujące sprawdzenia:

   - Otwórz program **Microsoft Management Console** (wpisując `services.msc` w menu **Początek**) i sprawdź, czy usługi Trend Micro Local Web Classification Server oraz Trend Micro Smart Scan Server mają stan „Uruchomiono".
   - Otwórz **Menedżera zadań systemu Windows**. Na karcie **Procesy** sprawdź, czy uruchomione są procesy `iCRCService.exe` i `LWCSService.exe`.
   - W konsoli Web programu OfficeScan sprawdź, czy wyświetlana jest pozycja menu **Administracja** > **Smart Protection** > **Zintegrowany serwer**.

Sprawdzone metody dotyczące serwera Smart Protection

Wykonanie poniższych czynności umożliwia optymalizację wydajności serwerów Smart Protection:

- Unikaj wykonywania jednocześnie skanowania ręcznego i skanowania zaplanowanego. Zaplanuj skanowanie naprzemiennie.

- Skonfiguruj agentów tak, aby funkcja Skanuj teraz nie była uruchamiana na wszystkich jednocześnie.
- Dostosuj Serwer Smart Protection do wolniejszych połączeń sieciowych o przepustowości około 512 Kb/s, dokonując zmian w pliku `ptngrowth.ini`.

Dostosowywanie pliku ptngrowth.ini dla serwera autonomicznego

Procedura

1. Otwórz plik `ptngrowth.ini` w katalogu `/var/tmcss/conf/`.
2. Zmodyfikuj plik `ptngrowth.ini` przy użyciu poniższych zalecanych wartości:
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. Zapisz plik `ptngrowth.ini`.
4. Uruchom ponownie usługę `lighttpd`, wpisując następujące polecenie w interfejsie wiersza polecenia:
   - `service lighttpd restart`

Dostosowywanie pliku ptngrowth.ini dla serwera zintegrowanego

Procedura

1. Otwórz plik `ptngrowth.ini` w lokalizacji <*Folder instalacyjny serwera*>`\PCCSRV\WSS\`.
2. Zmodyfikuj plik `ptngrowth.ini` przy użyciu poniższych zalecanych wartości:

- `[COOLDOWN]`
- `ENABLE=1`
- `MAX_UPDATE_CONNECTION=1`
- `UPDATE_WAIT_SECOND=360`

3. Zapisz plik `ptngrowth.ini`.
4. Uruchom ponownie usługę `Serwer Trend Micro Smart Protection`.

Zarządzanie zintegrowanym serwerem Smart Protection

Zintegrowanym serwerem Smart Protection można zarządzać, wykonując następujące zadania:

- Włączanie usług File Reputation Services i Web Reputation Services serwera zintegrowanego
- Rejestrowanie adresów serwera zintegrowanego
- Aktualizowanie składników serwera zintegrowanego
- Konfiguracja listy dozwolonych/zablokowanych adresów URL serwera zintegrowanego

Szczegółowe informacje zawiera sekcja *Konfigurowanie ustawień zintegrowanego serwera Smart Protection na stronie 4-22*.

Włączanie usług File Reputation Services i Web Reputation Services serwera zintegrowanego

W przypadku agentów, które wysyłają żądania skanowania i zapytania do serwera zintegrowanego, należy włączyć usługi File Reputation Services i Web Reputation Services. Włączenie tych usług umożliwi także serwerowi zintegrowanemu aktualizowanie składników z serwera ActiveUpdate.

Te usługi są włączane automatycznie, jeśli użytkownik zdecyduje się zainstalować zintegrowany serwer podczas instalacji serwera OfficeScan.

Po wyłączeniu tych usług należy się upewnić, że zainstalowano oddzielne serwery Smart Protection, do których agenci mogą wysyłać zapytania.

Szczegółowe informacje zawiera sekcja *Konfigurowanie ustawień zintegrowanego serwera Smart Protection na stronie 4-22*.

Rejestrowanie adresów serwera zintegrowanego

Adresy serwera zintegrowanego są wymagane podczas konfigurowania listy źródeł Smart Protection dla agentów wewnętrznych. Szczegółowe informacje o tej liście zawiera temat *Lista źródeł Smart Protection na stronie 4-23*.

Kiedy agenci wysyłają żądania skanowania do serwera zintegrowanego, identyfikują serwer przy użyciu jednego z dwóch adresów usług File Reputation Services — adresu HTTP lub HTTPS. Połączenie HTTPS zapewnia większe bezpieczeństwo danych, a połączenie HTTP — większą szybkość transmisji.

Kiedy agenci wysyłają zapytania do usługi Web Reputation Web Reputation, identyfikują serwer zintegrowany przy użyciu jego adresu usług Web Reputation Services.

Porada

Z serwerem zintegrowanym mogą się również łączyć agenci zarządzani przez inny serwer OfficeScan. Adres serwera zintegrowanego można dodać do listy serwera Smart Protection z poziomu konsoli Web innego serwera OfficeScan.

Szczegółowe informacje zawiera sekcja *Konfigurowanie ustawień zintegrowanego serwera Smart Protection na stronie 4-22*.

Aktualizowanie składników serwera zintegrowanego

Serwer zintegrowany aktualizuje następujące składniki:

- **Sygnatury Smart Scan**: agenci weryfikują potencjalne zagrożenia względem sygnatury Smart Scan, wysyłając żądania skanowania do serwera zintegrowanego.
- **Lista blokowania Web**: agenci objęci regułami usługi Web Reputation weryfikują reputację witryny internetowej względem funkcji Lista blokowania Web, wysyłając zapytania usługi Web Reputation do serwera zintegrowanego.

Składniki można aktualizować ręcznie lub skonfigurować harmonogram aktualizacji. Serwer zintegrowany pobiera składniki z serwera ActiveUpdate.

Uwaga

Zintegrowany serwer wykorzystujący wyłącznie protokół IPv6 nie może wykonywać aktualizacji bezpośrednio z serwera Trend Micro ActiveUpdate Server. Aby umożliwić serwerowi zintegrowanemu nawiązanie połączenia z serwerem ActiveUpdate, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.

Szczegółowe informacje zawiera sekcja *Konfigurowanie ustawień zintegrowanego serwera Smart Protection na stronie 4-22*.

Konfiguracja listy dozwolonych/zablokowanych adresów URL serwera zintegrowanego

Agenci mają własną listę dozwolonych/zablokowanych adresów URL. Skonfiguruj listę agentów podczas tworzenia reguł usługi Web Reputation (szczegółowe informacje zawarto w temacie *Reguły Web Reputation na stronie 12-5*). Dowolny adres URL na liście agenta będzie automatycznie dozwolony lub zablokowany.

Serwer zintegrowany ma własną listę dozwolonych/zablokowanych adresów URL. W przypadku, gdy adres URL nie znajduje się na liście agenta, agent wysyła zapytanie usługi Web Reputation do serwera zintegrowanego (jeśli serwer zintegrowany zostały przypisany jako źródło programu Smart Protection). Jeśli adres URL znajduje się na liście dozwolonych/zablokowanych adresów URL serwera zintegrowanego, serwer powiadamia agenta o dozwoleniu lub zablokowaniu adresu URL.

Uwaga

Lista zablokowanych adresów URL ma wyższy priorytet niż lista blokowania Web.

Aby dodać adresy URL do listy dozwolonych/zablokowanych adresów URL serwera zintegrowanego, należy zaimportować listę z samodzielnego serwera Smart Protection. Nie jest możliwe ręczne dodawanie adresów URL.

Szczegółowe informacje zawiera sekcja *Konfigurowanie ustawień zintegrowanego serwera Smart Protection na stronie 4-22*.

Konfigurowanie ustawień zintegrowanego serwera Smart Protection

Procedura

1. Przejdź do opcji **Administracja** > **Smart Protection** > **Zintegrowany serwer**.
2. Wybierz opcję **Włącz usługi File Reputation Services**.
3. Wybierz protokół (HTTP lub HTTPS), który będzie używany przez agentów podczas wysyłania żądań skanowania do serwera zintegrowanego.
4. Wybierz opcję **Włącz usługi Web Reputation Services**.
5. Zapisz adresy serwera zintegrowanego, które znajdują się w kolumnie **Adres serwera**.
6. Aby zaktualizować składniki serwera zintegrowanego:
   - Wyświetl bieżącą wersję sygnatury Smart Scan i listy blokowania Web. Jeśli dostępna jest aktualizacja, kliknij opcję **Aktualizuj teraz**. Wyniki aktualizacji zostaną wyświetlone w górnej części ekranu.
   - Aby automatycznie zaktualizować sygnaturę:
     a. Wybierz opcję **Włącz zaplanowane aktualizacje**.
     b. Wybierz, czy aktualizacja ma być wykonywana co godzinę lub co 15 minut.
     c. Wybierz źródło aktualizacji w sekcji **Usługi File Reputation Services**. Sygnatury Smart Scan będzie aktualizowana z tego źródła.
     d. Wybierz źródło aktualizacji w sekcji **Usługi Web Reputation Services**. Lista blokowania Web będzie aktualizowana z tego źródła.

Uwaga

- W przypadku wybrania serwera ActiveUpdate jako źródła aktualizacji należy się upewnić, że serwer ma dostęp do Internetu oraz, jeśli jest używany serwer proxy, sprawdzić, czy połączenie z Internetem można nawiązać za pomocą obecnych ustawień proxy. Szczegółowe informacje można znaleźć w części *Serwer proxy do aktualizacji serwera OfficeScan na stronie 6-21*.

- W przypadku wybrania niestandardowego źródła aktualizacji należy skonfigurować odpowiednie środowisko i zaktualizować zasoby dotyczące wybranego źródła aktualizacji. Należy się również upewnić, że połączenie między serwerem a źródłem aktualizacji działa prawidłowo. W przypadku konieczności uzyskania pomocy dotyczącej konfigurowania źródła aktualizacji należy się skontaktować z dostawcą obsługi technicznej.

7. Aby skonfigurować listę dozwolonych/zablokowanych adresów URL serwera zintegrowanego:

   a. Kliknij przycisk **Importuj**, aby zapełnić listę adresami URL z wstępnie sformatowanego pliku `.csv`. Plik `.csv` można uzyskać z samodzielnego serwera Smart Protection.

   b. Jeśli lista istnieje, kliknij przycisk **Eksportuj**, aby zapisać listę do pliku `.csv`.

8. Kliknij przycisk **Zapisz**.

Lista źródeł Smart Protection

Agenci wysyłają zapytania do źródeł programu Smart Protection podczas skanowania w poszukiwaniu zagrożeń bezpieczeństwa i określania reputacji witryny internetowej.

Obsługa protokołu IPv6 dla źródeł Smart Protection

Agent wykorzystujący wyłącznie protokół IPv6 nie może wysyłać żądań bezpośrednio do źródeł wykorzystujących wyłącznie protokół IPv4, takich jak:

- Serwer Smart Protection 2.0 (zintegrowany lub oddzielny)

Uwaga

Obsługa protokołu IPv6 została wprowadzona w wersji 2.5 serwera Smart Protection.

- Trend Micro Smart Protection Network

Analogicznie, agent wykorzystujący wyłącznie protokół IPv4 nie może wysyłać żądań bezpośrednio do serwerów Smart Protection wykorzystujących wyłącznie protokół IPv6.

Aby umożliwić agentom nawiązanie połączenia ze źródłami, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.

Źródła programu Smart Protection i lokalizacja punktu końcowego

To, z którym źródłem programu Smart Protection agent łączy się, zależy od lokalizacji punktu końcowego agenta.

Szczegółowe informacje na temat konfiguracji ustawień lokalizacji zawiera sekcja *Lokalizacja punktu końcowego na stronie 15-2*.

TABELA 4-5. Źródła Smart Protection według lokalizacji

LOKALIZACJA	ŹRÓDŁA SMART PROTECTION
Zewnętrzne	Agenci zewnętrzni wysyłają żądania skanowania i zapytania usługi Web Reputation do sieci Trend Micro Smart Protection Network.

LOKALIZACJA	ŹRÓDŁA SMART PROTECTION
Wewnętrzne	Agenci wewnętrzni wysyłają żądania skanowania i zapytania usługi Web Reputation do serwerów Smart Protection lub do sieci Trend Micro Smart Protection Network. W przypadku zainstalowania serwerów Smart Protection należy skonfigurować listę tych serwerów w konsoli Web programu OfficeScan. Agent wewnętrzny przed wysłaniem zapytania wybiera serwer z listy. Jeśli nawiązanie połączenia z pierwszym serwerem nie jest możliwe, agent wybiera kolejny serwer z listy. **Porada** Należy określić samodzielny Serwer Smart Protection jako podstawowe źródło skanowania, a zintegrowany serwer jako źródło zapasowe. Ogranicza to ruch kierowany do punktu końcowego, na którym znajduje się serwer OfficeScan i serwer zintegrowany. Indywidualny serwer może też przetwarzać więcej zapytań. Można skonfigurować standardową lub niestandardową listę źródeł Smart Protection. Lista standardowa jest używana przez wszystkich agentów wewnętrznych. Lista niestandardowa definiuje zakres adresów IP. Jeśli adres IP agenta wewnętrznego mieści się w wybranym zakresie, ten agent będzie korzystać z listy niestandardowej.

Konfigurowanie listy standardowej źródeł Smart Protection

Procedura

1. Przejdź do opcji **Administracja** > **Smart Protection** > **Źródła programu Smart Protection**.
2. Kliknij kartę **Agenci wewnętrzni**.
3. Wybierz opcję **Użyj listy standardowej (dla wszystkich agentów wewnętrznych)**.
4. Kliknij łącze **Lista standardowa**.

   Zostanie wyświetlony nowy ekran.

5. Kliknij przycisk **Dodaj**.

   Zostanie wyświetlony nowy ekran.

6. Określ nazwę hosta serwera Smart Protection lub adres IPv4/IPv6. Adres IPv6 należy umieścić w nawiasach.

   Uwaga

   Określ nazwę hosta, jeśli z serwerem Smart Protection łączą się agenci IPv4 i IPv6.

7. Wybierz opcję **Usługi File Reputation Services**. Agenci wysyłają żądania skanowania przy użyciu protokołu HTTP lub HTTPS. Połączenie HTTPS zapewnia większe bezpieczeństwo danych, a połączenie HTTP — większą szybkość transmisji.

   a. Aby agenci używali protokołu HTTP, wpisz port nasłuchiwania serwera dla żądań HTTP. Aby agenci używali protokołu HTTPS, wybierz opcję SSL i wpisz port nasłuchiwania serwera dla żądań HTTPS.

   b. Kliknij opcję **Sprawdź połączenie**, aby sprawdzić, czy można nawiązać połączenie z serwerem.

   Porada

   Port nasłuchiwania stanowi część adresu serwera. Aby uzyskać adres serwera:

   W przypadku serwera zintegrowanego otwórz konsolę Web programu OfficeScan i przejdź do opcji **Administracja** > **Smart Protection** > **Zintegrowany serwer**.

   W przypadku samodzielnego serwera otwórz jego konsolę i przejdź do ekranu **Podsumowanie**.

8. Wybierz opcję **Usługi Web Reputation Services**. Agenci wysyłają zapytania Web Reputation przy użyciu protokołu HTTP. Protokół HTTPS nie jest obsługiwany.

   a. Wpisz port nasłuchiwania serwera dla żądań HTTP.

   b. Kliknij opcję **Sprawdź połączenie**, aby sprawdzić, czy można nawiązać połączenie z serwerem.

9. Kliknij przycisk **Zapisz**.

   Ekran zostanie zamknięty.

10. Dodaj więcej serwerów, powtarzając wcześniejsze kroki.

11. Na górze ekranu wybierz opcję **Kolejność** lub **Losowo**.

    - **Kolejność**: agenci wybierają serwery w kolejności, w jakiej znajdują się na liście. W przypadku wybrania opcji **Kolejność** skorzystaj ze strzałek w kolumnie **Kolejność**, aby przesuwać serwery w górę i w dół listy.
    - **Losowo**: agenci wybierają serwery losowo.

Porada

Ponieważ zintegrowany Serwer Smart Protection i serwer OfficeScan są uruchomione na tym samym punkcie końcowym, jego wydajność może się znacznie pogorszyć podczas największego obciążenia obu serwerów. Aby ograniczyć ruch kierowany do komputera serwera OfficeScan, należy określić samodzielny Serwer Smart Protection jako podstawowe źródło Smart Protection, a zintegrowany serwer jako źródło zapasowe.

12. Na tym ekranie można wykonywać różne zadania.

    - Jeśli masz listę wyeksportowaną z innego serwera i chcesz ją zaimportować na ten ekran, kliknij polecenie **Importuj** i wskaż plik `.dat`. Lista zostanie wczytana.
    - Aby wyeksportować listę do pliku `.dat`, kliknij przycisk **Eksportuj**, a następnie kliknij przycisk **Zapisz**.
    - Aby odświeżyć stan usługi serwerów, kliknij przycisk **Odśwież**.
    - Kliknij nazwę serwera, aby wykonać następujące czynności:
      - wyświetlić lub edytować dane serwera,
      - wyświetlić pełny adres serwera dla usług Web Reputation Services lub File Reputation Services.
    - Aby otworzyć konsolę serwera Smart Protection, kliknij polecenie **Uruchom konsolę**.

- W przypadku zintegrowanego serwera Smart Protection zostanie wyświetlony ekran z informacjami o jego konfiguracji.
- W przypadku samodzielnego serwera Smart Protection oraz zintegrowanego serwera Smart Protection innego serwera OfficeScan zostanie wyświetlony ekran logowania konsoli.

- Aby usunąć wpis, zaznacz pole wyboru obok serwera i kliknij polecenie **Usuń**.

13. Kliknij przycisk **Zapisz**.

    Ekran zostanie zamknięty.

14. Kliknij polecenie **Powiadom wszystkich agentów**.

Konfigurowanie list niestandardowych źródeł Smart Protection

Procedura

1. Przejdź do opcji **Administracja** > **Smart Protection** > **Źródła programu Smart Protection**.
2. Kliknij kartę **Agenci wewnętrzni**.
3. Wybierz opcję **Użyj list niestandardowych w oparciu o adres IP agenta**.
4. (Opcjonalnie) Wybierz opcję **Użyj listy standardowej, gdy wszystkie serwery na liście niestandardowej będą niedostępne**.

   Porada

   Firma Trend Micro zaleca włączenie tej funkcji, aby zapewnić agentom możliwość połączenia ze źródłem usługi Smart Protection, jeśli źródła niestandardowe staną się niedostępne.

5. Kliknij przycisk **Dodaj**.

   Zostanie wyświetlony nowy ekran.

6. W sekcji **Zakresy adresów IP** określ zakres adresów IPv4 lub IPv6 bądź oba te zakresy.

Uwaga

Agenci z adresem IPv4 mogą nawiązać połączenie z serwerami Smart Protection korzystającymi wyłącznie z protokołu IPv4 lub z serwerami z dwoma stosami. Agenci z adresem IPv6 mogą nawiązać połączenie z serwerami Smart Protection korzystającymi wyłącznie z protokołu IPv6 lub z serwerami z dwoma stosami. Agenci z adresami IPv4 i IPv6 mogą nawiązać połączenie z dowolnym serwerem Smart Protection.

7. W sekcji **Ustawienia proxy** określ ustawienia proxy, które będą używane przez agentów w celu nawiązania połączenia z serwerami Smart Protection.

   a. Wybierz opcję **Używaj serwera proxy do komunikacji z agentem i Serwer Smart Protection**.

   b. Wpisz nazwę serwera proxy lub jego adres IPv4/IPv6 i numer portu.

   c. Jeżeli serwer proxy wymaga uwierzytelniania, wpisz nazwę użytkownika i hasło.

8. W sekcji **Niestandardowa lista Serwer Smart Protection** dodaj serwery Smart Protection.

   a. Określ nazwę hosta serwera Smart Protection lub adres IPv4/IPv6. Adres IPv6 należy umieścić w nawiasach.

Uwaga

Określ nazwę hosta, jeśli z serwerem Smart Protection łączą się agenci IPv4 i IPv6.

   b. Wybierz opcję **Usługi File Reputation Services**. Agenci wysyłają żądania skanowania przy użyciu protokołu HTTP lub HTTPS. Połączenie HTTPS zapewnia większe bezpieczeństwo danych, a połączenie HTTP — większą szybkość transmisji.

      i. Aby agenci używali protokołu HTTP, wpisz port nasłuchiwania serwera dla żądań HTTP. Aby agenci używali protokołu HTTPS, wybierz opcję **SSL** i wpisz port nasłuchiwania serwera dla żądań HTTPS.

ii. Kliknij opcję **Sprawdź połączenie**, aby sprawdzić, czy można nawiązać połączenie z serwerem.

Porada

Port nasłuchiwania stanowi część adresu serwera. Aby uzyskać adres serwera:

W przypadku serwera zintegrowanego otwórz konsolę Web programu OfficeScan i przejdź do opcji **Administracja** > **Smart Protection** > **Zintegrowany serwer**.

W przypadku samodzielnego serwera otwórz jego konsolę i przejdź do ekranu Podsumowanie.

---

c. Wybierz opcję **Usługi Web Reputation Services**. Agenci wysyłają zapytania Web Reputation przy użyciu protokołu HTTP. Protokół HTTPS nie jest obsługiwany.

i. Wpisz port nasłuchiwania serwera dla żądań HTTP.

ii. Kliknij opcję **Sprawdź połączenie**, aby sprawdzić, czy można nawiązać połączenie z serwerem.

d. Kliknij opcję **Dodaj do listy**.

e. Dodaj więcej serwerów, powtarzając wcześniejsze kroki.

f. Wybierz opcję **Kolejność** lub **Losowo**.

- **Kolejność**: agenci wybierają serwery w kolejności, w jakiej znajdują się na liście. W przypadku wybrania opcji **Kolejność** skorzystaj ze strzałek w kolumnie **Kolejność**, aby przesuwać serwery w górę i w dół listy.
- **Losowo**: agenci wybierają serwery losowo.

Porada

Ponieważ zintegrowany Serwer Smart Protection i serwer OfficeScan są uruchomione na tym samym komputerze, jego wydajność może się znacznie pogorszyć podczas największego obciążenia obu serwerów. Aby ograniczyć ruch kierowany do komputera serwera OfficeScan, należy określić samodzielny Serwer Smart Protection jako podstawowe źródło Smart Protection, a zintegrowany serwer jako źródło zapasowe.

---

g. Na tym ekranie można wykonywać różne zadania.

- Aby odświeżyć stan usługi serwerów, kliknij przycisk **Odśwież**.
- Aby otworzyć konsolę serwera Smart Protection, kliknij polecenie **Uruchom konsolę**.
  - W przypadku zintegrowanego serwera Smart Protection zostanie wyświetlony ekran z informacjami o jego konfiguracji.
  - W przypadku samodzielnego serwera Smart Protection oraz zintegrowanego serwera Smart Protection innego serwera OfficeScan zostanie wyświetlony ekran logowania konsoli.
- Aby usunąć pozycję, kliknij przycisk **Usuń** (

).

9. Kliknij przycisk **Zapisz**.

Ekran zostanie zamknięty. Dodana lista zostanie wyświetlona jako łącze z zakresem adresów IP w tabeli **Zakres adresów IP**.

10. Powtórz procedurę od kroku 4 do kroku 8, aby dodać więcej list niestandardowych.

11. Na tym ekranie można wykonywać różne zadania.

- Aby zmodyfikować listę, kliknij łącze z zakresem adresów IP, a następnie zmodyfikuj ustawienia na wyświetlonym ekranie.
- Aby wyeksportować listę do pliku .dat, kliknij przycisk **Eksportuj**, a następnie kliknij przycisk **Zapisz**.
- Jeśli masz listę wyeksportowaną z innego serwera i chcesz ją zaimportować na ten ekran, kliknij polecenie **Importuj** i wskaż plik `.dat`. Lista zostanie wczytana.

12. Kliknij polecenie **Powiadom wszystkich agentów**.

Ustawienia proxy dla połączenia agenta

Jeśli nawiązanie połączenia z siecią Smart Protection Network wymaga uwierzytelnienia na serwerze proxy, należy wprowadzić poświadczenia uwierzytelniania. Szczegółowe informacje zawiera sekcja *Zewnętrzny serwer proxy dla agentów OfficeScan na stronie 15-53*.

Skonfiguruj ustawienia wewnętrznego serwera proxy agentów do użytku podczas łączenia się z serwerem Smart Protection. Szczegółowe informacje zawiera sekcja *Wewnętrzny serwer proxy dla agentów OfficeScan na stronie 15-52*.

Ustawienia lokalizacji punktu końcowego

Program OfficeScan zapewnia funkcję rozpoznawania lokalizacji, która rozpoznaje lokalizację komputera agenta i ustala, czy agent łączy się z siecią Smart Protection Network, czy z serwerem Smart Protection. Dzięki temu istnieje pewność, że agenci są chronieni niezależnie od ich lokalizacji.

Aby skonfigurować ustawienia lokalizacji, patrz *Lokalizacja punktu końcowego na stronie 15-2*.

Instalacja usługi Trend Micro Network VirusWall

Jeśli jest zainstalowany produkt Trend Micro™ Network VirusWall™ Enforcer:

- Zainstaluj pakiet hot fix (wersja 1047 w przypadku produktu Network VirusWall Enforcer 2500 i wersja 1013 w przypadku produktu Network VirusWall Enforcer 1200).
- W celu umożliwienia produktowi wykrywania metody skanowania agenta zaktualizuj silnik OPSWAT do wersji 2.5.1017.

Korzystanie z usług Smart Protection

Po prawidłowym skonfigurowaniu środowiska Smart Protection agenci mogą rozpocząć korzystanie z usług File Reputation Services i Web Reputation Services. Można także rozpocząć konfigurowanie ustawień funkcji Smart Feedback.

Uwaga

Instrukcje dotyczące konfigurowania środowiska Smart Protection zawiera temat *Konfigurowanie usług Smart Protection na stronie 4-13*.

Aby skorzystać z ochrony zapewnianej przez usługi File Reputation Services, agenci muszą używać metody skanowania o nazwie Smart Scan. Szczegółowe informacje o rozwiązaniu Smart Scan i sposobie jego włączania na agentach zawiera temat *Typy metod skanowania na stronie 7-9*.

Aby umożliwić agentom OfficeScan korzystanie z usług Web Reputation Services, należy skonfigurować reguły usługi Web Reputation. Szczegółowe informacje zawiera sekcja *Reguły Web Reputation na stronie 12-5*.

Uwaga

Ustawienia metod skanowania i reguł usługi Web Reputation są szczegółowe. W zależności od wymagań można skonfigurować ustawienia, które mają zastosowanie do wszystkich agentów, lub skonfigurować oddzielne ustawienia dla pojedynczych agentów lub grup agentów.

Instrukcje dotyczące konfigurowania funkcji Smart Feedback zawiera temat *Smart Feedback na stronie 14-67*.

Rozdział 5

Instalowanie agenta OfficeScan

W tym rozdziale opisano wymagania systemowe programu OfficeScan i procedury instalacji agenta OfficeScan.

Szczegółowe informacje na temat uaktualniania agenta OfficeScan znajdują się w *Podręczniku instalacji oraz uaktualniania programu OfficeScan.*

Rozdział składa się z następujących tematów:

Nowe instalacje agenta OfficeScan

Agent OfficeScan może być zainstalowany na komputerach z systemami operacyjnymi Microsoft Windows. Program OfficeScan jest także zgodny z różnymi produktami innych firm.

Pełna lista wymagań systemowych i zgodnych produktów innych firm jest dostępna pod adresem:

http://docs.trendmicro.com/pl-pl/enterprise/officescan.aspx

Uwagi dotyczące instalacji

Przed zainstalowaniem agentów należy rozważyć poniższe kwestie:

TABELA 5-1. Uwagi dotyczące instalacji agentów

UWAGA	OPIS
Obsługa systemu Windows	Niektóre funkcje agenta OfficeScan Agent OfficeScan są niedostępne na określonych platformach Windows.
Obsługa IPv6	Agenta OfficeScan można zainstalować na agentach z dwoma stosami lub wykorzystujących wyłącznie protokół IPv6. Jednakże: • Niektóre systemy operacyjne Windows, na których można zainstalować agenta OfficeScan, nie obsługują adresowania IPv6. • W przypadku niektórych metod instalacji agenta OfficeScan jej powodzenie wymaga spełnienia specjalnych wymogów.
Adresy IP agentów OfficeScan	W przypadku agentów z adresami IPv4 i IPv6 można wybrać, który adres IP zostanie użyty podczas rejestrowania agenta na serwerze.

Uwaga	Opis
Listy wyjątków	sprawdź, czy listy wyjątków poniższych funkcji zostały prawidłowo skonfigurowane: • **Monitorowanie zachowań**: dodaj krytyczne aplikacje punktu końcowego do listy dozwolonych programów, aby uniemożliwić agentowi OfficeScan blokowanie tych aplikacji. Aby uzyskać więcej informacji, patrz *Lista wyjątków monitorowania zachowań na stronie 9-10*. • **Web Reputation**: dodaj witryny internetowe uznawane za bezpieczne do listy Lista dozwolonych adresów URL, aby uniemożliwić agentowi OfficeScan blokowanie dostępu do tych witryn. Aby uzyskać więcej informacji, patrz *Reguły Web Reputation na stronie 12-5*.

Funkcje agenta OfficeScan

Funkcje Agent OfficeScan dostępne na punkcie końcowym zależą od systemu operacyjnego punktu końcowego.

Tabela 5-2. Funkcje agenta OfficeScan na platformach serwerowych

Funkcja	System operacyjny Windows			
	Serwer 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
Skanowanie ręczne, skanowanie w czasie rzeczywistym i skanowanie zaplanowane	Tak	Tak	Tak	Tak

Funkcja	System operacyjny Windows			
	Serwer 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
Aktualizacja składników (aktualizacja ręczna i zaplanowana)	Tak	Tak	Tak	Tak
Agent aktualizacji	Tak	Tak	Tak	Tak
Usługa Web Reputation	Tak, ale wyłączona domyślnie podczas instalacji serwera	Tak, ale wyłączona domyślnie podczas instalacji serwera	Tak, ale wyłączona domyślnie podczas instalacji serwera	Tak, ale wyłączona domyślnie podczas instalacji serwera
Usługi Usuwania Szkód Services	Tak	Tak	Tak	Tak
Zapora programu OfficeScan	Tak, ale wyłączona domyślnie podczas instalacji serwera	Tak, ale wyłączona domyślnie podczas instalacji serwera	Tak, ale wyłączona domyślnie podczas instalacji serwera	Tak, ale wyłączona domyślnie podczas instalacji serwera
Monitorowanie zachowań	Tak (32-bitowe), ale wyłączone domyślnie	Tak (32-bitowe), ale wyłączone domyślnie	Tak (64-bitowe), ale wyłączone domyślnie	Tak (64-bitowe), ale wyłączone domyślnie
	Nie (64-bitowe)	Tak (64-bitowe), ale wyłączone domyślnie		

Funkcja	System operacyjny Windows			
	Serwer 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
Własna ochrona agenta następujących elementów: • Klucze rejestru • Procesy	Tak (32-bitowe), ale wyłączone domyślnie	Tak (32-bitowe), ale wyłączone domyślnie	Tak (64-bitowe), ale wyłączone domyślnie	Tak (64-bitowe), ale wyłączone domyślnie
	Nie (64-bitowe)	Tak (64-bitowe), ale wyłączone domyślnie		
Własna ochrona agenta następujących elementów: • Usługi • Ochrona plików	Tak	Tak	Tak	Tak
Kontrola urządzeń (Usługa zapobiegania nieautoryzowanym zmianom)	Tak (32-bitowe), ale wyłączone domyślnie	Tak (32-bitowe), ale wyłączone domyślnie	Tak (64-bitowe), ale wyłączone domyślnie	Tak (64-bitowe), ale wyłączone domyślnie
	Nie (64-bitowe)	Tak (64-bitowe), ale wyłączone domyślnie		

Funkcja	System operacyjny Windows			
	Serwer 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
Ochrona danych (zawiera Ochrona danych do kontroli urządzeń)	Tak (32-bitowe), ale wyłączone domyślnie	Tak (32-bitowe), ale wyłączone domyślnie	Tak (64-bitowe), ale wyłączone domyślnie	Tak (64-bitowe), ale wyłączone domyślnie
	Tak (64-bitowe), ale wyłączone domyślnie	Tak (64-bitowe), ale wyłączone domyślnie		
Ustawienia podejrzanego połączenia	Tak	Tak	Tak	Tak
Przesyłanie próbek	Tak	Tak	Tak	Tak
Skanowanie poczty POP3	Tak	Tak	Tak	Tak
Program Plug-in Manager agenta	Tak	Tak	Tak	Tak
Tryb niezależny	Tak	Tak (serwer) Nie (Server Core)	Tak	Tak
Smart Feedback	Tak	Tak	Tak	Tak

Tabela 5-3. Funkcje agenta OfficeScan na platformach komputerów stacjonarnych

Funkcja	System operacyjny Windows				
	XP	Vista	Windows 7	Windows 8/8.1	Windows 10
Skanowanie ręczne, skanowanie w czasie rzeczywistym i skanowanie zaplanowane	Tak	Tak	Tak	Tak	Tak
Aktualizacja składników (aktualizacja ręczna i zaplanowana)	Tak	Tak	Tak	Tak	Tak
Agent aktualizacji	Tak	Tak	Tak	Tak	Tak
Usługa Web Reputation	Tak	Tak	Tak	Tak, ale ograniczona obsługa trybu interfejsu użytkownika systemu Windows	Tak
Usługi Usuwania Szkód Services	Tak	Tak	Tak	Tak	Tak
Zapora programu OfficeScan	Tak	Tak	Tak	Tak	Tak

Funkcja	System operacyjny Windows				
	XP	Vista	Windows 7	Windows 8/8.1	Windows 10
Monitorowanie zachowania	Tak (32-bitowe)	Tak (32-bitowe)	Tak (32-bitowe)	Tak (32-bitowe)	Tak (32-bitowe)
	Nie (64-bitowe)	Tak (64-bitowe) Vista w wersji 64-bitowej wymaga dodatku SP1 lub SP2	Tak (64-bitowe)	Tak (64-bitowe)	Tak (64-bitowe)
Własna ochrona agenta następujących elementów: • Klucze rejestru • Procesy	Tak (32-bitowe)	Tak (32-bitowe)	Tak (32-bitowe)	Tak (32-bitowe)	Tak (32-bitowe)
	Nie (64-bitowe)	Tak (64-bitowe) Vista w wersji 64-bitowej wymaga dodatku SP1 lub SP2	Tak (64-bitowe)	Tak (64-bitowe)	Tak (64-bitowe)
Własna ochrona agenta następujących elementów: • Usługi • Ochrona plików	Tak	Tak	Tak	Tak	Tak

Funkcja	System operacyjny Windows				
	XP	Vista	Windows 7	Windows 8/8.1	Windows 10
Kontrola urządzeń (Usługa zapobiegania nieautoryzowanym zmianom)	Tak (32-bitowe)	Tak (32-bitowe)	Tak (32-bitowe)	Tak (32-bitowe)	Tak (32-bitowe)
	Nie (64-bitowe)	Tak (64-bitowe) Vista w wersji 64-bitowej wymaga dodatku SP1 lub SP2	Tak (64-bitowe)	Tak (64-bitowe)	Tak (64-bitowe)
Ochrona danych (zawiera Ochrona danych do kontroli urządzeń)	Tak (32-bitowe)	Tak (32-bitowe)	Tak (32-bitowe)	Tak (32-bitowe) w trybie pulpitu	Tak (32-bitowe)
	Tak (64-bitowe)	Tak (64-bitowe)	Tak (64-bitowe)	Tak (64-bitowe) w trybie pulpitu	Tak (64-bitowe)
Ustawienia podejrzanego połączenia	Tak	Tak	Tak	Tak	Tak
Przesyłanie próbek	Tak	Tak	Tak	Tak	Tak
Skanowanie poczty POP3	Tak	Tak	Tak	Tak	Tak
Program Plug-in Manager agenta	Tak	Tak	Tak	Tak	Tak
Tryb niezależny	Tak	Tak	Tak	Tak	Tak
Funkcja Smart Feedback	Tak	Tak	Tak	Tak	Tak

Instalacja agenta OfficeScan i obsługa protokołu IPv6

W tym temacie omówiono kwestie związane z instalacją agenta OfficeScan na agentach z dwoma stosami lub wykorzystujących wyłącznie protokół IPv6.

System operacyjny

Agenta OfficeScan można zainstalować wyłącznie w następujących systemach operacyjnych, które obsługują adresowanie IPv6:

- Windows Vista™ (wszystkie wersje)
- Windows Server 2008 (wszystkie wersje)
- Windows 7 (wszystkie wersje)
- Windows Server 2012 (wszystkie wersje)
- Windows 8/8.1 (wszystkie wersje)
- Windows 10 (wersje Home, Pro, Education i Enterprise)
- Windows Server 2016 (wszystkie wersje)

Pełna lista wymagań systemowych jest dostępna pod adresem:

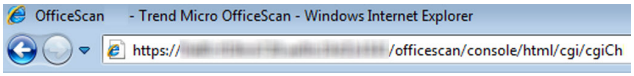
http://docs.trendmicro.com/pl-pl/enterprise/officescan.aspx

Metody instalacji

W celu zainstalowania agenta OfficeScan na agentach z dwoma stosami lub wykorzystujących wyłącznie protokół IPv6 można użyć wszystkich metod instalacji agenta OfficeScan. W przypadku niektórych metod instalacji agenta OfficeScan jej powodzenie wymaga spełnienia specjalnych wymogów.

Nie można dokonać migracji programu ServerProtect™ na agenta OfficeScan przy użyciu narzędzia ServerProtect Normal Server Migration, ponieważ to narzędzie nie obsługuje adresowania IPv6.

TABELA 5-4. Metody instalacji i obsługa protokołu IPv6

METODA INSTALACJI	WYMAGANIA/UWAGI
Strona instalacyjna w sieci Web i instalacja oparta na przeglądarce internetowej	Adres URL strony instalacyjnej zawiera nazwę hosta lub adres IP serwera OfficeScan.  Jeśli instalacja odbywa się na agencie wykorzystującym wyłącznie protokół IPv6, serwer musi mieć dwa stosy lub wykorzystywać wyłącznie protokół IPv6, a jego nazwa hosta lub adres IPv6 musi stanowić część adresu URL. W przypadku agenci z dwoma stosami adres IPv6, który jest wyświetlany na ekranie stanu instalacji, jest zależny od opcji wybranej w sekcji **Preferowany adres IP** w pozycji **Agenci** > **Ustawienia agenta globalnego** na karcie **Sieć**.
Agent Packager	Jeśli używane jest narzędzie do pakowania, należy wybrać, czy uprawnienia agenta aktualizacji zostaną przydzielone agentowi. Należy pamiętać, że agent aktualizacji wykorzystujący wyłącznie protokół IPv6 może rozsyłać aktualizacje tylko do agentów wykorzystujących wyłącznie protokół IPv6 lub do agentów z dwoma stosami.
Zgodność z zabezpieczeniami, narzędzie Vulnerability Scanner i instalacja zdalna	Serwer wykorzystujący wyłącznie protokół IPv6 nie umożliwia instalacji agenta OfficeScan na punktach końcowych wykorzystujących wyłącznie protokół IPv4. Analogicznie, serwer wykorzystujący wyłącznie protokół IPv4 nie umożliwia instalacji agenta OfficeScan na punktach końcowych wykorzystujących wyłącznie protokół IPv6.

Adresy IP agentów

Serwer OfficeScan zainstalowany w środowisku obsługującym adresowanie IPv6 może zarządzać następującymi agentami OfficeScan:

- Serwer OfficeScan zainstalowany na hoście wykorzystującym wyłącznie protokół IPv6 może zarządzać agentami wykorzystującymi wyłącznie protokół IPv6.
- Serwer OfficeScan zainstalowany na hoście z dwoma stosami, do którego przypisano adresy IPv4 i IPv6, może zarządzać agentami wykorzystującymi

wyłącznie protokół IPv6, agentami z dwoma stosami i agentami wykorzystującymi wyłącznie protokół IPv4.

Po zainstalowaniu lub uaktualnieniu agentów rejestrują się oni na serwerze przy użyciu adresu IP.

- Agenci wykorzystujący wyłącznie protokół IPv6 rejestrują się przy użyciu adresu IPv6.
- Agenci wykorzystujący wyłącznie protokół IPv4 rejestrują się przy użyciu adresu IPv4.
- Agenci z dwoma stosami rejestrują się przy użyciu adresu IPv4 lub IPv6. Można wybrać adres IP, który będzie używany przez tych agentów.

Konfigurowanie adresów IP używanych przez agentów z dwoma stosami podczas rejestrowania się na serwerze

Ustawienie to jest dostępne wyłącznie na serwerach OfficeScan z dwoma stosami i stosowane tylko do agentów z dwoma stosami.

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Kliknij kartę **Sieć**.
3. Przejdź do sekcji **Preferowany adres IP**.
4. Wybierz jedną z następujących opcji:
   - **Tylko IPv4**: Agenci używają adresu IPv4.
   - **Najpierw IPv4, następnie IPv6**: Agenci najpierw używają adresu IPv4. Jeśli agent nie może zarejestrować się przy użyciu adresu IPv4, używa adresu IPv6. Jeśli rejestracja nie powiedzie się przy użyciu obu adresów IP, agent ponawia próbę zgodnie z priorytetem adresów IP wybranym w tym miejscu.
   - **Najpierw IPv6, następnie IPv4**: Agenci używają najpierw adresu IPv6. Jeśli agent nie może zarejestrować się przy użyciu adresu IPv6, używa adresu IPv4. Jeśli rejestracja nie powiedzie się przy użyciu obu adresów IP, agent ponawia próbę zgodnie z priorytetem adresów IP wybranym w tym miejscu.

5. Kliknij przycisk **Zapisz**.

Uwagi dotyczące instalacji

W tym rozdziale znajduje się podsumowanie różnych metod nowej instalacji agenta OfficeScan. Wszystkie metody instalacji wymagają posiadania uprawnień administratora dla komputerów docelowych.

Jeśli podczas instalowania agentów konieczne jest włączenie obsługi protokołu IPv6, należy zapoznać się z wytycznymi w temacie *Instalacja agenta OfficeScan i obsługa protokołu IPv6 na stronie 5-10*.

Tabela 5-5. Uwagi dotyczące instalacji

Metoda instalacji / Obsługa systemu operacyjnego	Uwagi dotyczące instalacji					
	Wdrożenie sieci WAN	Zarządzanie centralne	Wymaga udziału użytkownika	Wymaga zasobów informatycznych	Instalacja masowa	Wykorzystanie łącza
Strona instalacyjna w sieci Web Obsługiwana we wszystkich systemach operacyjnych z wyjątkiem systemu Windows Server Core 2008 oraz Windows 8/8.1/Server 2012/ Server Core 2012 w trybie interfejsu użytkownika systemu Windows	Nie	Nie	Tak	Nie	Nie	Wysoki

Metoda instalacji / Obsługa systemu operacyjnego	Uwagi dotyczące instalacji					
	Wdrożenie sieci WAN	Zarządzanie centralne	Wymaga udziału użytkownika	Wymaga zasobów informatycznych	Instalacja masowa	Wykorzystanie łącza
Instalacja oparta na przeglądarce internetowej Obsługiwana we wszystkich systemach operacyjnych **Uwaga** Nieobsługiwana w systemie Windows 8, 8.1 lub Windows Server 2012 w trybie interfejsu użytkownika systemu Windows.	Nie	Nie	Tak	Tak	Nie	Wysokie, jeśli instalacje rozpoczynają się jednocześnie
Instalacja oparta na UNC Obsługiwana we wszystkich systemach operacyjnych	Nie	Nie	Tak	Tak	Nie	Wysokie, jeśli instalacje rozpoczynają się jednocześnie

Metoda instalacji / Obsługa systemu operacyjnego	Uwagi dotyczące instalacji					
	Wdrożenie sieci WAN	Zarządzanie centralne	Wymaga udziału użytkownika	Wymaga zasobów informatycznych	Instalacja masowa	Wykorzystanie łącza
Instalacja zdalna Obsługiwana we wszystkich systemach operacyjnych z wyjątkiem • Windows Vista Home Basic i Home Premium • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 (wersje podstawowe) • Windows 10 Home Edition	Nie	Tak	Nie	Tak	Nie	Wysoki
Ustawienia skryptu logowania Obsługiwana we wszystkich systemach operacyjnych	Nie	Nie	Tak	Tak	Nie	Wysokie, jeśli instalacje rozpoczynają się jednocześnie

Metoda instalacji / Obsługa systemu operacyjnego	Uwagi dotyczące instalacji					
	Wdrożenie sieci WAN	Zarządzanie centralne	Wymaga udziału użytkownika	Wymaga zasobów informatycznych	Instalacja masowa	Wykorzystanie łącza
Agent Packager Obsługiwana we wszystkich systemach operacyjnych	Nie	Nie	Tak	Tak	Nie	Niskie (przy instalacji zaplanowanej)
Agent Packager (pakiet MSI instalowany za pomocą programu Microsoft SMS) Obsługiwana we wszystkich systemach operacyjnych	Tak	Tak	Tak/Nie	Tak	Tak	Niskie (przy instalacji zaplanowanej)
Agent Packager (pakiet MSI wdrażany przez usługę Active Directory) Obsługiwana we wszystkich systemach operacyjnych	Tak	Tak	Tak/Nie	Tak	Tak	Wysokie, jeśli instalacje rozpoczynają się jednocześnie

Metoda instalacji / Obsługa systemu operacyjnego	Uwagi dotyczące instalacji					
	Wdrożenie sieci WAN	Zarządzanie centralne	Wymaga udziału użytkownika	Wymaga zasobów informatycznych	Instalacja masowa	Wykorzystanie łącza
Obraz dysku agenta Obsługiwana we wszystkich systemach operacyjnych	Nie	Nie	Nie	Tak	Nie	Niskie
Narzędzie Trend Micro Vulnerability Scanner (TMVS) Obsługiwana we wszystkich systemach operacyjnych z wyjątkiem • Windows Vista Home Basic i Home Premium • Windows XP Home Edition • Windows 8/8.1 (wersje podstawowe) • Windows 10 Home Edition	Nie	Tak	Nie	Tak	Nie	Wysoki

Metoda instalacji / Obsługa systemu operacyjnego	Uwagi dotyczące instalacji					
	Wdrożenie sieci WAN	Zarządzanie centralne	Wymaga udziału użytkownika	Wymaga zasobów informatycznych	Instalacja masowa	Wykorzystanie łącza
Instalacja ze zgodnością z zabezpieczeniami Obsługiwana we wszystkich systemach operacyjnych z wyjątkiem • Windows Vista Home Basic i Home Premium • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 (wersje podstawowe) • Windows 10 Home Edition	Nie	Tak	Nie	Tak	Nie	Wysoki

Instalacje witryny instalacyjnej w sieci Web

Program Agent OfficeScan można instalować z poziomu strony instalacyjnej w sieci Web, jeśli na punktach końcowych z następującymi systemami operacyjnymi i oprogramowaniem zainstalowano serwer OfficeScan:

- system operacyjny Windows Server 2008 i serwer Internet Information Server (IIS) 7.0.
- Windows Server 2008 R2 z serwerem Internet Information Server (IIS) 7.5
- system operacyjny Windows Server 2012 i serwer Internet Information Server (IIS) 8.0.
- Windows Server 2012 R2 z serwerem Internet Information Server (IIS) 8.5
- system operacyjny Windows Server 2016 i serwer Internet Information Server (IIS) 10.0.

Do instalowania ze strony instalacyjnej sieci Web jest wymagany program:

- Internet Explorer z poziomem zabezpieczeń umożliwiającym wykonywanie formantów ActiveX™. Wymagane wersje:
  - 7.0 w przypadku systemu Windows Vista i Windows Server 2008:
  - 8.0 w przypadku systemu Windows 7
  - 10.0 w przypadku systemu Windows 8/8.1 i Windows Server 2012
  - 11.0 w przypadku systemu Windows 10 i Windows Server 2016
- Uprawnienia administratora na punkcie końcowym

Do użytkowników należy przesłać pocztą elektroniczną instrukcje instalacji agenta OfficeScan z poziomu strony instalacyjnej w sieci Web. Informacje na temat wysyłania pocztą elektroniczną powiadomienia o instalacji znajdują się w sekcji *Inicjowanie instalacji opartej na przeglądarce internetowej na stronie 5-23*.

Instalowanie z witryny instalacyjnej w sieci Web

Procedura

1. Zaloguj się na punkcie końcowym, używając wbudowanego konta administratora.

   Uwaga

   W systemie Windows 7, 8, 8.1 lub 10 należy najpierw włączyć wbudowane konto administratora. System Windows 7, 8, 8.1 lub 10 domyślnie wyłącza wbudowane konto administratora. Szczegółowe informacje znajdują się na stronie pomocy technicznej Microsoft (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx).

2. W przypadku instalowania programu na punktach końcowych z systemem Windows Vista, Server 2008, 7, 8, 8.1, 10, Server 2012, 2012R2 lub 2016 należy wykonać następujące operacje:

   a. Uruchom przeglądarkę Internet Explorer i dodaj adres URL serwera OfficeScan (np. `https://<OfficeScan server name>:4343/officescan`) do listy zaufanych witryn. W systemie Windows 7 dostęp do listy można uzyskać, klikając kolejno pozycje **Narzędzia** > **Opcje internetowe** > **Zabezpieczenia**, wybierając ikonę **Zaufane witryny** i klikając pozycję **Witryny**.

   b. Zmień ustawienia zabezpieczeń programu Internet Explorer, aby włączyć opcję **Automatyczne monitowanie dla formantów ActiveX**. W systemie Windows 7 można to zrobić, wybierając kolejno pozycje **Narzędzia** > **Opcje internetowe** > **Zabezpieczenia**, a następnie klikając pozycję **Poziom niestandardowy**.

3. Otwórz okno programu Internet Explorer i wpisz następujący adres:

   `https://<nazwa serwera OfficeScan>:<numer portu>/officescan`

4. Kliknij łącze **instalator** na stronie logowania, aby wyświetlić następujące opcje instalacji:

   - **Instalacja agenta w oparciu o przeglądarkę internetową** (tylko Internet Explorer): postępuj zgodnie z instrukcjami wyświetlanymi na ekranie w zależności od używanego systemu operacyjnego.

- **Instalacja agenta MSI**: pobierz 32- lub 64-bitowy pakiet w zależności od używanego systemu operacyjnego, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Uwaga

Po wyświetleniu monitu zezwól na instalację formantu ActiveX.

5. Po zakończeniu instalacji ikona agenta OfficeScan pojawia się na pasku zadań systemu Windows.

Uwaga

Listę ikon wyświetlanych na pasku zadań zawiera sekcja *Ikony agenta OfficeScan na stronie 15-27*.

Instalacja oparta na przeglądarce internetowej

Można skonfigurować wiadomość e-mail powiadamiającą użytkowników w sieci o potrzebie instalacji agenta OfficeScan. W celu rozpoczęcia instalacji użytkownicy powinni kliknąć łącze instalatora agenta OfficeScan znajdujące się w wiadomości e-mail.

Przed zainstalowaniem agentów OfficeScan:

- Sprawdź wymagania dotyczące instalacji agentów OfficeScan.
- Określ, które komputery w sieci nie są obecnie wyposażone w ochronę przed zagrożeniami. Wykonaj następujące czynności:
  - Uruchom narzędzie Trend Micro Vulnerability Scanner. Narzędzie to, na podstawie podanego zakresu adresów IP, analizuje punkty końcowe pod względem zainstalowanego oprogramowania antywirusowego. Szczegółowe informacje zawiera sekcja *Używanie narzędzia Vulnerability Scanner na stronie 5-43*.
  - Sprawdź zgodność z zabezpieczeniami. Szczegółowe informacje zawiera sekcja *Zgodność z zabezpieczeniami dla niezarządzanych punktów końcowych na stronie 15-74*.

Inicjowanie instalacji opartej na przeglądarce internetowej

Procedura

1. Przejdź do opcji **Agenci** > **Instalacja agenta** > **W przeglądarce**.
2. W razie potrzeby zmień zawartość wiersza tematu wiadomości e-mail.
3. Kliknij przycisk **Utwórz e-mail**.

   Otwarty zostanie domyślny program pocztowy.
4. Wyślij wiadomość e-mail do wskazanych odbiorców.

Przeprowadzanie instalacji opartej na ścieżkach formatu UNC

`AutoPcc.exe` to samodzielny program, który instaluje agenta OfficeScan na niechronionych punktach końcowych oraz aktualizuje pliki programów i składniki oprogramowania. Korzystanie z programu AutoPcc z wykorzystaniem ścieżek UNC jest możliwe tylko na punktach końcowych należących do domeny.

Procedura

1. Przejdź do opcji **Agenci** > **Instalacja agenta** > **Oparte na UNC**.
   - Aby zainstalować agenta OfficeScan na niechronionym punkcie końcowym przy użyciu programu `AutoPcc.exe`:
     a. Połącz się z serwerem. Przejdź do ścieżki UNC:

        ```
        \\<nazwa komputera serwera>\ofcscan
        ```

     b. Kliknij prawym przyciskiem myszy plik `AutoPcc.exe` i wybierz polecenie **Uruchom jako administrator**.
   - Instalacje zdalne na komputerze przy użyciu programu `AutoPcc.exe`:

a. Otwórz okno Podłączanie pulpitu zdalnego (Mstsc.exe) w trybie konsoli. Powoduje to wymuszenie instalacji przy użyciu programu `AutoPcc.exe` w sesji 0.

b. Przejdź do katalogu `\\<nazwa komputera serwera>\ofcscan` i uruchom plik `AutoPcc.exe`.

Instalacja zdalna z konsoli Web programu OfficeScan

Agenta OfficeScan można zainstalować zdalnie na jednym lub wielu punktach końcowych podłączonych do sieci.<!--Agent OfficeScan--> Aby przeprowadzić instalację zdalną, należy upewnić się, że masz uprawnienia administratora na docelowych punktach końcowych. Instalacja zdalna nie umożliwia instalowania Agent OfficeScan na punktach końcowych z już zainstalowanym serwerem OfficeScan.

Uwaga

Z tej metody instalacji nie można korzystać w przypadku punktów końcowych z systemami Windows XP Home, Vista Home Basic i Home Premium Edition, Windows 7 Home Basic i Home Premium Edition (wersje 32- i 64-bitowe), Windows 8/8.1 (wersje 32- i 64-bitowe) oraz Windows 10 Home Edition. Serwer wykorzystujący wyłącznie protokół IPv6 nie umożliwia instalacji Agent OfficeScan na agentach wykorzystujących wyłącznie protokół IPv4. Analogicznie, serwer wykorzystujący wyłącznie protokół IPv4 nie umożliwia instalacji Agent OfficeScan na agentach wykorzystujących wyłącznie protokół IPv6.

Procedura

1. Wykonaj poniższe czynności przedinstalacyjne w danej wersji systemu Windows.

   - W przypadku systemu Windows XP:

     a. Włącz wbudowane konto administratora domeny i ustaw hasło dla tego konta.

     b. Na punkcie końcowym przejdź do karty **Mój komputer** > **Narzędzia** > **Opcje folderów** > **Widok** i wyłącz opcję **Użyj prostego udostępniania plików**.

c. Przejdź do karty **Start** > **Programy** > **Zapora systemu Windows** > **Wyjątki** i włącz wyjątek **Udostępnianie plików i drukarek**.

d. Otwórz konsolę Microsoft Management Console (kliknij **Start** > **Uruchom** i wpisz `services.msc`) i uruchom usługi **Rejestr zdalny** i **Zdalne wywoływanie procedur**. Podczas instalacji agenta OfficeScan należy używać wbudowanego konta i hasła administratora.<!--Agent OfficeScan-->

- W przypadku systemu Windows Vista:

  a. Włącz wbudowane konto administratora domeny i ustaw hasło dla tego konta.

  b. Kliknij polecenie **Start** > **Panel sterowania** > **Zabezpieczenia** > **Zapora systemu Windows** > **Zmień ustawienia**.

  c. Kliknij kartę **Wyjątki** i włącz wyjątek **Udostępnianie plików i drukarek**.

  d. Otwórz konsolę Microsoft Management Console (kliknij **Start** > **Uruchom** i wpisz `services.msc`) i uruchom usługi **Rejestr zdalny** i **Zdalne wywoływanie procedur**. Podczas instalacji agenta OfficeScan należy używać wbudowanego konta i hasła administratora.

- W przypadku systemów Windows 7, Windows 8 (Pro, Enterprise), Windows 8.1, Windows 10 (Pro, Education, Enterprise) i Windows Server 2012/2016:

  a. Włącz wbudowane konto administratora domeny i ustaw hasło dla tego konta.

  b. Przejdź do opcji **Start** > **Programy** > **Narzędzia administracyjne** > **Zapora systemu Windows z zabezpieczeniami zaawansowanymi**.

  c. Włącz dla reguły **Udostępnianie plików i drukarek** profil "Domena", "Prywatny" i/lub "Publiczny", zależnie od środowiska sieciowego.

  d. Otwórz konsolę Microsoft Management Console (kliknij **Start** > **Uruchom** i wpisz `services.msc`) i uruchom usługi **Rejestr zdalny** i **Zdalne wywoływanie procedur**. Podczas instalacji agenta OfficeScan należy używać wbudowanego konta i hasła administratora.

2. W konsoli Web przejdź do pozycji **Agenci** > **Instalacja agenta** > **Zdalny**.
3. Wybierz docelowe punkty końcowe.
   - Lista **Domeny i punkty końcowe** zawiera wszystkie domeny systemu Windows w sieci. Aby wyświetlić punkty końcowe w domenie, kliknij dwukrotnie nazwę domeny. Wybierz dowolny punkt końcowy, a następnie kliknij przycisk **Dodaj**.
   - Jeśli ma być dodany punkt końcowy o określonej nazwie, wpisz tę nazwę w polu **Wyszukaj punkty końcowe** w górnej części strony i naciśnij przycisk ENTER.

   Program OfficeScan wyświetli monit o podanie nazwy użytkownika docelowego punktu końcowego i hasła. Aby kontynuować, wprowadź nazwę i hasło konta administratora.
4. Wpisz nazwę użytkownika i hasło, a następnie kliknij polecenie **Zaloguj**.

   Docelowy punkt końcowy zostanie wyświetlony w tabeli **Wybrane punkty końcowe**.
5. Powtórz kroki 3 i 4, aby dodać więcej punktów końcowych.
6. Kliknij przycisk **Instaluj**, aby zainstalować agenta Agent OfficeScan na docelowych punktach końcowych.

   Zostanie wyświetlone okno potwierdzenia.
7. Kliknij przycisk **Tak**, aby potwierdzić zamiar instalacji agenta OfficeScan na docelowych punktach końcowych.

   Podczas kopiowania plików programu na każdy z docelowych punktów końcowych pojawi się ekran postępu.

Kiedy w programie OfficeScan zostanie zakończona instalacja na docelowym punkcie końcowym, jego nazwa zniknie z listy **Wybrane punkty końcowe** i pojawi się na liście **Domeny i punkty końcowe**, oznaczona czerwonym znacznikiem.

Instalacja zdalna będzie zakończona, gdy na liście **Domeny i punkty końcowe** zostaną wyświetlone wszystkie docelowe punkty końcowe oznaczone czerwonymi znacznikami wyboru.

Uwaga

Jeżeli instalacja jest przeprowadzana na wielu punktach końcowych, wszystkie nieudane instalacje zostaną zarejestrowane przez program OfficeScan w dziennikach (szczegółowe informacji znajdują się w części *Dzienniki świeżej instalacji na stronie 18-16*), ale nie opóźni to innych instalacji. Po kliknięciu przycisku **Instaluj** nie ma potrzeby nadzorowania procesu instalacji. Po jej ukończeniu należy wyświetlić dzienniki, aby sprawdzić wyniki instalacji.

Instalowanie za pomocą skryptu logowania

Stosując ustawienia skryptu logowania, można zautomatyzować proces instalacji agenta OfficeScan na niezabezpieczonych komputerach zaraz po zalogowaniu się użytkownika w sieci. Ustawienia skryptu logowania powodują dodanie programu `AutoPcc.exe` do skryptu logowania serwera.

Program `AutoPcc.exe` instaluje agenta OfficeScan na niezarządzanych komputerach oraz aktualizuje pliki programów i składniki oprogramowania. Korzystanie z programu AutoPcc za pośrednictwem skryptu logowania jest możliwe tylko na punktach końcowych należących do domeny.

Instalacja dodatku

Program `AutoPcc.exe` automatycznie instaluje Agent OfficeScan na niezabezpieczonym punkcie końcowym z systemem Windows Server 2003 po jego zalogowaniu na serwerze, którego skrypty logowania zostały zmodyfikowane. Program`AutoPcc.exe` nie instaluje jednak automatycznie Agent OfficeScan na punktach końcowych z systemem Windows Vista, 7, 8, 8.1, 10, Server 2008, Server 2012 i Server 2016. Użytkownicy muszą nawiązać połączenie z serwerem, przejść do lokalizacji `\\<nazwa komputera serwera>\ofcscan`, kliknąć prawym przyciskiem myszy plik `AutoPcc.exe`, a następnie wybrać polecenie **Uruchom jako administrator**.

Zdalna instalacja na komputerze przy użyciu programu `AutoPcc.exe`:

- Punkt końcowy musi być uruchomiony w trybie `Mstsc.exe /console mode`. Powoduje to wymuszenie instalacji przy użyciu programu `AutoPcc.exe` w sesji 0.

- Przypisz napęd do katalogu ofcscan i uruchom program `AutoPcc.exe` z tej lokalizacji.

Aktualizacje programów i składników

Program `AutoPcc.exe` aktualizuje pliki programów oraz składniki oprogramowania do ochrony antywirusowej i oprogramowania spyware oraz składniki Usługi Usuwania Szkód Services.

Skrypty systemu Windows Server

Jeżeli istnieje już skrypt logowania, narzędzie Ustawienia skryptu logowania doda do niego polecenie uruchamiające program `AutoPcc.exe`. W przeciwnym przypadku program OfficeScan utworzy plik wsadowy `ofcscan.bat` zawierający polecenie uruchamiające program `AutoPcc.exe`.

Na końcu skryptu narzędzie Ustawienia skryptu logowania dopisuje następujące informacje:

```
\\<nazwa_serwera>\ofcscan\autopcc
```

Gdzie:

- `<nazwa_serwera>` to nazwa punktu końcowego lub adres IP komputera serwera OfficeScan.
- „`ofcscan`” to udostępniony folder programu OfficeScan na serwerze.
- „`autopcc`” to łącze do pliku wykonywalnego autopcc, który zainstaluje Agent OfficeScan.

Lokalizacja skryptu logowania (poprzez udostępniony katalog logowania do sieci):

- `Windows Server 2003: \\Windows 2003 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2008: \\Windows 2008 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2012: \\Windows 2012 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`

- `Windows Server 2016: \\Windows 2016 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`

Dodawanie programu Autopcc.exe do skryptu logowania za pomocą Ustawień skryptu logowania

Procedura

1. W menu Start systemu Windows na punkcie końcowym użytym do instalacji serwera kliknij kolejno polecenia **Programy** > **Trend Micro OfficeScan Server <nazwa serwera>** > **Ustawienia skryptu logowania**.

   Zostanie załadowane narzędzie **Ustawienia skryptu logowania**. Na konsoli zostanie wyświetlone drzewo ze wszystkimi domenami sieci.

2. Znajdź serwer, którego skrypt logowania chcesz zmienić, wybierz go, a następnie kliknij przycisk **Wybierz**. Upewnij się, że serwer to podstawowy kontroler domeny oraz że masz dostęp do serwera z uprawnieniami administratora.

   W programie Ustawienia skryptu logowania zostanie wyświetlony monit o podanie nazwy użytkownika i hasła.

3. Wpisz nazwę użytkownika i hasło. Kliknij przycisk **OK**, aby kontynuować.

   Zostanie wyświetlony ekran **Wybór użytkownika**. Lista **Użytkownicy** zawiera profile użytkowników, którzy logują się na serwerze. Lista **Wybrani użytkownicy** zawiera profile użytkowników, których skrypty logowania zostaną zmienione.

4. Aby zmodyfikować skrypt logowania profilu użytkownika, wybierz profil z listy **Użytkownicy** i kliknij polecenie **Dodaj**.

5. Aby zmienić skrypty logowania wszystkich użytkowników, kliknij przycisk **Dodaj wszystkich**.

6. Aby wykluczyć poprzednio wybrany profil użytkownika, kliknij jego nazwę na liście **Wybrani użytkownicy**, a następnie kliknij polecenie **Usuń**.

7. Aby anulować zaznaczenie wszystkich opcji, kliknij przycisk **Usuń wszystkie**.

8. Kliknij **Zastosuj**, gdy wszystkie docelowe profile użytkowników znajdują się na liście **Wybrani użytkownicy**.

Zostanie wyświetlony komunikat informujący o pomyślnej modyfikacji skryptów logowania serwera.

9. Kliknij przycisk **OK**.

   Narzędzie Ustawienia skryptu logowania powróci do ekranu początkowego.

10. Aby zmodyfikować skrypty logowania na innych serwerach, powtórz kroki od 2 do 4.

11. Aby zamknąć narzędzie Ustawienia skryptu logowania, kliknij przycisk **Zakończ**.

Instalacja za pomocą programu Agent Packager

Program Agent Packager tworzy pakiet instalacyjny, który można wysłać do użytkowników na nośniku tradycyjnym, na przykład na dysku CD-ROM. Użytkownicy uruchamiają pakiet na punkcie końcowym agenta, aby zainstalować lub zaktualizować agenta OfficeScan oraz zaktualizować składniki.

Program Agent Packager jest szczególnie przydatny podczas instalacji agenta OfficeScan lub składników na agentach znajdujących się w odległych biurach o małej przepustowości łącza. Agenci OfficeScan zainstalowani przy użyciu programu Agent Packager przesyłają do serwera informacje o lokalizacji, w której utworzono pakiet.

Wymagania programu Agent Packager:

- 350 MB wolnej przestrzeni dyskowej
- Instalator Windows 2.0 (w celu uruchomienia pakietu MSI)

Wytyczne dotyczące instalacji pakietu

1. Wyślij pakiet do użytkowników i poleć im, aby uruchomili na swoich punktach końcowych pakiet agenta OfficeScan, klikając dwukrotnie plik `EXE` lub `MSI`.

   Uwaga

   Wyślij pakiet tylko do użytkowników, których Agent OfficeScan podlega serwerowi, na którym utworzono pakiet.

2. Jeśli użytkownicy będą instalować pakiet `EXE` na punktach końcowych z systemem Windows Vista, Server 2008, 7, 8, 8.1, 10, Server 2012 lub Server 2016, należy polecić im, aby kliknęli prawym przyciskiem myszy plik `EXE` i wybrali opcję **Uruchom jako administrator**.

3. W przypadku utworzenia pliku `MSI` pakiet należy zainstalować, wykonując następujące czynności:

   - Użyć usługi Active Directory lub programu Microsoft SMS.

     Aby uzyskać więcej informacji, patrz *Instalowanie pakietu MSI za pomocą usługi Active Directory na stronie 5-35* lub *Instalowanie pakietu MSI za pomocą programu Microsoft SMS na stronie 5-37*.

4. Uruchom pakiet MSI w oknie wiersza polecenia i przeprowadź instalację agenta Agent OfficeScan w trybie cichym na zdalnym punkcie końcowym z systemem Windows XP, Vista, Server 2008, 7, 8, 8.1, 10, Server 2012 lub Server 2016.

Wskazówki dotyczące metody skanowania dla pakietów agenta

Wybierz metodę skanowania dla pakietu. Szczegółowe informacje można znaleźć w części *Typy metod skanowania na stronie 7-9*.

W zależności od wybranej metody skanowania do pakietu są dołączane różne składniki. Szczegółowe informacje o składnikach dostępnych dla każdej metody skanowania zawiera temat *Aktualizacje agenta OfficeScan na stronie 6-29*.

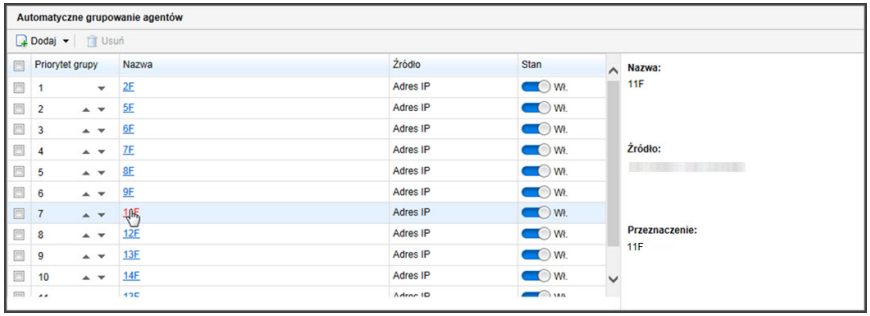
W celu zapewnienia optymalnej instalacji pakietu przed wybraniem metody skanowania należy się zapoznać z poniższymi wytycznymi:

- Jeśli pakiet będzie używany do uaktualnienia agenta do tej wersji programu OfficeScan, należy w konsoli Web sprawdzić metodę skanowania na poziomie domeny. W konsoli przejdź do pozycji **Agenci** > **Zarządzanie agentami**, wybierz domenę drzewa agentów, do której należy agent, a następnie kliknij kolejno opcje **Ustawienia** > **Ustawienia skanowania** > **Metody skanowania**. Metoda skanowania na poziomie domeny powinna odpowiadać metodzie skanowania wybranej w przypadku pakietu.

- Jeśli pakiet będzie używany do wykonywania nowej instalacji agenta OfficeScan, należy sprawdzić ustawienia grupowania agentów. W konsoli Web przejdź do pozycji **Agenci** > **Grupowanie agentów**.

- Jeżeli agenci są grupowani według NetBIOS, Active Directory lub domeny DNS, sprawdź, do której domeny należy docelowy punkt końcowy. Jeśli domena istnieje, sprawdź skonfigurowaną dla niej metodę skanowania. Jeśli domena nie istnieje, sprawdź metodę skanowania na poziomie głównym (wybierz ikonę domeny głównej ( ) w drzewie agentów i kliknij kolejno opcje **Ustawienia** > **Ustawienia skanowania** > **Metody skanowania**). Metoda skanowania na poziomie domeny lub głównym powinna odpowiadać metodzie skanowania wybranej w przypadku pakietu.

- Jeżeli agenci są grupowani w oparciu o niestandardowe grupy agentów, sprawdź **Priorytet grupowania** i **Źródło**.



ILUSTRACJA 5-1. Panel podglądu automatycznego grupowania agentów

Jeżeli docelowy punkt końcowy należy do danego źródła, sprawdź odpowiednie **Przeznaczenie**. Lokalizacja docelowa to nazwa domeny wyświetlona w drzewie agentów. Po instalacji agent zastosuje metodę skanowania tej domeny.

- Jeśli pakiet będzie używany do aktualizowania składników agenta korzystającego z tej wersji programu OfficeScan, należy sprawdzić metodę skanowania skonfigurowaną dla domeny drzewa agentów, do której należy agent. Metoda skanowania na poziomie domeny powinna odpowiadać metodzie skanowania wybranej w przypadku pakietu.

Tworzenie pakietu instalacyjnego za pomocą programu Agent Packager

Procedura

1. Na komputerze serwera OfficeScan przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\ClientPackager`.
2. Kliknij dwukrotnie plik `ClnPack.exe`, aby uruchomić narzędzie.

   Zostanie otwarta konsola programu **Agent Packager**.
3. Wybierz typ pakietu, który chcesz utworzyć.

   TABELA 5-6. Typy pakietów agenta

TYP PAKIETU	OPIS
Instalacja	By utworzyć pakiet w postaci pliku wykonywalnego, wybierz **Konfiguruj**. Pakiet zainstaluje oprogramowanie agenta OfficeScan z aktualnie dostępnymi na serwerze składnikami. Jeśli na docelowym punkcie końcowym znajduje się wcześniej zainstalowana wersja agenta, uruchomienie pliku wykonywalnego spowoduje aktualizację agenta.
Aktualizacja	Wybierz polecenie **Aktualizuj**, aby utworzyć pakiet zawierający składniki obecnie dostępne na serwerze. Pakiet zostanie utworzony jako plik wykonywalny. Należy użyć tego pakietu, jeśli aktualizacja składników agenta na punkcie końcowym powoduje problemy.
MSI	Wybierz opcję **MSI** w przypadku tworzenia pakietu zgodnego z formatem pakietu Microsoft Installer. Pakiet zainstaluje także oprogramowanie agenta OfficeScan z aktualnie dostępnymi na serwerze składnikami. Jeśli na docelowym punkcie końcowym znajduje się wcześniej zainstalowana wersja agenta, uruchomienie pliku MSI spowoduje aktualizację agenta.

4. Wybierz system operacyjny, do którego chcesz utworzyć pakiet. Zainstaluj pakiet tylko na punktach końcowych, na których jest zainstalowany system operacyjny odpowiedniego typu. W przypadku zamiaru instalacji w systemie operacyjnym innego typu należy utworzyć kolejny pakiet.

5. Wybierz metodę skanowania, która zostanie zainstalowana przez pakiet agenta.

   Wskazówki dotyczące wyboru metody skanowania zawiera sekcja *Wskazówki dotyczące metody skanowania dla pakietów agenta na stronie 5-31*.

6. W obszarze **Domena** wybierz jedną z następujących opcji:

   - **Zezwól agentom na automatyczne zgłaszanie swojej domeny**: po zainstalowaniu agenta OfficeScan agent wysyła zapytanie do bazy danych serwera OfficeScan i zgłasza serwerowi swoje ustawienia domeny.
   - Dowolna domena na liście: program Agent Packager synchronizuje się z serwerem OfficeScan i wyświetla listę domen aktualnie używanych w drzewie agentów.

7. W obszarze **Opcje** wybierz jedną z następujących opcji:

Opcja	Opis
Tryb cichy	Ta opcja zapewnia możliwość utworzenia pakietu, który instaluje się w tle na punkcie końcowym agenta w sposób niezauważalny dla agenta, bez wyświetlenia okna stanu instalacji. Tę opcję należy włączyć w przypadku zamiaru zdalnej instalacji pakietu na docelowym punkcie końcowym.
Wymuś zastąpienie najnowszą wersją	Ta opcja powoduje zastąpienie wersji składnika agenta wersją, która jest obecnie dostępna na serwerze. Z tej opcji należy korzystać w celu zapewnienia synchronizacji między składnikami serwera i agenta.
Wyłącz skanowanie wstępne (tylko w przypadku nowej instalacji)	Jeśli na docelowym punkcie końcowym nie zainstalowano agenta OfficeScan, przed jego zainstalowaniem pakiet skanuje punkt końcowy pod względem zagrożeń bezpieczeństwa. W przypadku pewności, że docelowy punkt końcowy nie jest narażony na zagrożenia bezpieczeństwa, można wyłączyć tę funkcję. Jeśli funkcja wstępnego skanowania jest włączona, instalator skanuje pod względem wirusów/złośliwego oprogramowania najbardziej narażone na ataki obszary punktu końcowego: • Obszar rozruchowy i katalog rozruchowy (pod kątem wirusów sektora rozruchowego) • Folder systemu Windows

OPCJA	OPIS
	• Folder Program files

8. W sekcji **Możliwości agenta aktualizacji** wybierz funkcje, które mogą być zainstalowane przez agenta aktualizacji.

9. W sekcji **Składniki** wybierz składniki i funkcje dołączane do pakietu.

   - Szczegółowe informacje na temat składników zawiera sekcja *Składniki i programy pakietu OfficeScan na stronie 6-2*.
   - moduł Ochrona danych jest dostępny tylko w przypadku zainstalowania i aktywacji Ochrona danych. Szczegółowe informacje o usłudze Ochrona danych zawiera temat *Wprowadzenie do modułu Ochrona danych na stronie 3-1*.

10. Upewnij się, że lokalizacja pliku `ofcscan.ini` jest prawidłowa, sprawdzając ją obok pola **Plik źródłowy**. Aby zmienić ścieżkę, kliknij przycisk (...) w celu odnalezienia pliku `ofcscan.ini`.

    Domyślnie ten plik znajduje się w lokalizacji `<Folder instalacji serwera>\PCCSRV` serwera OfficeScan.

11. W obszarze **Plik wyjściowy** kliknij przycisk (...), aby określić lokalizację, w której ma zostać utworzony pakiet agenta OfficeScan, a następnie wpisz nazwę pliku pakietu (np. `AgentSetup.exe`).

12. Kliknij przycisk **Utwórz**.

    Po utworzeniu pakietu w programie Agent Packager pojawi się komunikat "Pakiet został pomyślnie utworzony". Znajdź pakiet w katalogu określonym w poprzednim kroku.

13. Zainstaluj pakiet.

Instalowanie pakietu MSI za pomocą usługi Active Directory

Funkcje usługi Active Directory umożliwiają jednoczesne instalowanie pakietu MSI na wielu punktach końcowych agenta.

Instrukcje dotyczące tworzenia pliku MSI zawiera część *Instalacja za pomocą programu Agent Packager na stronie 5-30*.

Procedura

1. Wykonaj następujące czynności:
   - W systemie Windows Server 2003 i starszych:
     a. Otwórz konsolę usługi Active Directory.
     b. Kliknij prawym przyciskiem myszy jednostkę organizacyjną (OU), w której chcesz zainstalować pakiet MSI, a następnie kliknij polecenie **Właściwości**.
     c. Kliknij pozycję **Nowy** na karcie **Reguły grupy**.
   - W systemie Windows Server 2008 i Windows Server 2008 R2:
     a. Otwórz **Konsolę zarządzania zasadami grupy**. Kliknij **Start** > **Panel sterowania** > **Narzędzia administracyjne** > **Zarządzanie zasadami grupy**.
     b. W drzewie konsoli rozwiń element **Obiekty zasad grupy** w lesie i domenie zawierającej GPO do edycji.
     c. Prawym przyciskiem myszy kliknij GPO do edycji, a następnie kliknij **Edytuj**. Uruchomi się **Edytor obiektów zasad grupy**.
   - W systemie Windows Server 2012 i Windows Server 2016:
     a. Otwórz **Konsolę zarządzania zasadami grupy**. Kliknij kolejno opcje **Zarządzanie serwerem** > **Narzędzia** > **Zarządzanie zasadami grupy**.
     b. W drzewie konsoli rozwiń element **Obiekty zasad grupy** w lesie i domenie zawierającej GPO do edycji.
     c. Prawym przyciskiem myszy kliknij GPO do edycji, a następnie kliknij **Edytuj**. Uruchomi się **Edytor obiektów zasad grupy**.
2. Wybierz opcję **Konfiguracja komputera** lub **Konfiguracja użytkownika**, a następnie wybierz opcję **Ustawienia oprogramowania** poniżej.

Porada

Firma Trend Micro zaleca wybranie opcji **Konfiguracja komputera** zamiast opcji **Konfiguracja użytkownika** w celu zapewnienia prawidłowej instalacji pakietu MSI niezależnie od tego, który z użytkowników zaloguje się na punkcie końcowym.

3. Kliknij prawym przyciskiem myszy opcję **Instalacja oprogramowania** znajdującą się poniżej opcji **Ustawienia oprogramowania**, a następnie wybierz kolejno polecenia **Nowy** i **Pakiet**.
4. Wyszukaj i zaznacz pakiet MSI.
5. Wybierz metodę instalacji, a następnie kliknij przycisk **OK**.
   - **Przypisana**: Pakiet MSI jest automatycznie instalowany po następnym zalogowaniu użytkownika na punkt końcowy (w przypadku zaznaczenia opcji Konfiguracja użytkownika) lub po ponownym uruchomieniu punkt końcowy (w przypadku zaznaczenia opcji Konfiguracja komputera). Ta metoda nie wymaga udziału użytkownika.
   - **Publikowana**: Aby uruchomić pakiet MSI, należy polecić użytkownikom, aby przeszli do Panelu sterowania, uzyskali dostęp do ekranu Dodaj/Usuń programy, a następnie wybrali opcję dodawania/instalowania programów w sieci. Po wyświetleniu ekranu pakietu MSI agenta OfficeScan użytkownicy mogą przystąpić do instalowania agenta OfficeScan.

Instalowanie pakietu MSI za pomocą programu Microsoft SMS

Jeśli na serwerze zainstalowano oprogramowanie Microsoft BackOffice SMS, pakiet MSI można zainstalować za pomocą programu Microsoft System Management Server (SMS).

Instrukcje dotyczące tworzenia pliku MSI zawiera część *Instalacja za pomocą programu Agent Packager na stronie 5-30*.

Serwer SMS przed zainstalowaniem pakietu na docelowych punktach końcowych wymaga pobrania pliku MSI z serwera OfficeScan.

- Lokalny: serwer SMS i serwer OfficeScan znajdują się na tym samym punkcie końcowym.

- Zdalny: serwer SMS i serwer OfficeScan znajdują się różnych punktach końcowych.

Znane problemy podczas instalacji programu Microsoft SMS:

- W kolumnie **Czas działania** konsoli programu SMS zostaje wyświetlony komunikat "Unknown" (Nieznany).
- Jeżeli instalacja nie powiedzie się, jej stan na monitorze programu SMS może wskazywać, że została zakończona.

  Instrukcje dotyczące sprawdzania poprawności instalacji zawiera sekcja *Po instalacji na stronie 5-76*.

Poniższe instrukcje mają zastosowanie w przypadku korzystania z programu Microsoft SMS w wersji 2.0 lub 2003.

Lokalne pobieranie pakietu

Procedura

1. Otwórz konsolę **Administrator programu SMS**.
2. Na karcie **Drzewo** kliknij pozycję **Pakiety**.
3. W menu **Operacja** kliknij kolejno pozycje **Nowa** > **Pakiety według definicji**.

   Zostanie wyświetlony ekran **Zapraszamy kreatora tworzenia pakietów według definicji**.
4. Kliknij przycisk **Dalej**.

   Zostanie wyświetlony ekran **Package Definition** (Definicja pakietu).
5. Kliknij przycisk **Przeglądaj**.

   Zostanie wyświetlony ekran **Open** (Otwórz).
6. Przejdź do pliku pakietu MSI utworzonego w programie Agent Packager i zaznacz go, a następnie kliknij przycisk **Otwórz**.

   Nazwa pakietu MSI zostanie wyświetlona na ekranie **Definicja pakietu**. Informacje dotyczące pakietu zawierają nazwę „Agent OfficeScan" oraz wersję programu.

7. Kliknij przycisk **Dalej**.

   Zostanie wyświetlony ekran **Source Files** (Pliki źródłowe).

8. Kliknij przycisk **Zawsze uzyskuj pliki z katalogu źródłowego**, a następnie przycisk **Dalej**.

   Zostanie wyświetlony ekran **Katalog źródłowy** zawierający nazwę tworzonego pakietu i katalog źródłowy.

9. Kliknij pozycję **Dysk lokalny na serwerze witryny**.

10. Kliknij przycisk **Przeglądaj** i wybierz katalog źródłowy zawierający plik MSI.

11. Kliknij przycisk **Dalej**.

    Za pomocą kreatora zostaną utworzone pakiety. Po zakończeniu procesu nazwa pakietu zostanie wyświetlona na konsoli **administratora programu SMS**.

Zdalne pobieranie pakietu

Procedura

1. Na serwerze OfficeScan za pomocą programu Agent Packager utwórz pakiet instalacyjny z rozszerzeniem `EXE` (nie można utworzyć pakietu `MSI`). Szczegółowe informacje można znaleźć w części *Instalacja za pomocą programu Agent Packager na stronie 5-30*.

2. Na punkcie końcowym, na którym chcesz przechowywać źródło, utwórz folder udostępniony.

3. Otwórz konsolę administratora programu Microsoft SMS.

4. Na karcie **Drzewo** kliknij pozycję **Pakiety**.

5. W menu **Operacja** kliknij kolejno pozycje **Nowa** > **Pakiety według definicji**.

   Zostanie wyświetlony ekran **Zapraszamy kreatora tworzenia pakietów według definicji**.

6. Kliknij przycisk **Dalej**.

Zostanie wyświetlony ekran **Package Definition** (Definicja pakietu).

7. Kliknij przycisk **Przeglądaj**.

   Zostanie wyświetlony ekran **Open** (Otwórz).

8. Wyszukaj plik pakietu MSI. Plik znajduje się w utworzonym folderze udostępnionym.

9. Kliknij przycisk **Dalej**.

   Zostanie wyświetlony ekran **Source Files** (Pliki źródłowe).

10. Kliknij przycisk **Zawsze uzyskuj pliki z katalogu źródłowego**, a następnie przycisk **Dalej**.

    Zostanie wyświetlony ekran **Katalog źródłowy**.

11. Kliknij pozycję **Ścieżka sieciowa (nazwa UNC)**.

12. Kliknij przycisk **Przeglądaj** i wybierz katalog źródłowy zawierający plik MSI (utworzony wcześniej folder udostępniony).

13. Kliknij przycisk **Dalej**.

    Za pomocą kreatora zostaną utworzone pakiety. Po zakończeniu procesu nazwa pakietu zostanie wyświetlona na konsoli **administratora programu SMS**.

Dystrybucja pakietu na docelowe punkty końcowe

Procedura

1. Na karcie **Drzewo** kliknij **Anonse**.

2. W menu **Operacja** kliknij kolejno pozycje **Wszystkie zadania** > **Dystrybuuj oprogramowanie**.

   Zostanie wyświetlony ekran **Powitanie Kreatora dystrybucji oprogramowania**.

3. Kliknij przycisk **Dalej**.

   Zostanie wyświetlony ekran **Package** (Pakiet).

4. Kliknij opcję **Dystrybuuj istniejący pakiet**, a następnie kliknij nazwę utworzonego pakietu instalacyjnego.

5. Kliknij przycisk **Dalej**.

   Zostanie wyświetlony ekran **Distribution Points** (Punkty dystrybucji).

6. Wybierz punkt rozprowadzania, do którego chcesz skopiować pakiet, a następnie kliknij przycisk **Dalej**.

   Zostanie wyświetlony ekran **Advertise a Program** (Anonsowanie programu).

7. Kliknij przycisk **Tak**, aby zaanonsować pakiet instalacyjny agenta OfficeScan, a następnie kliknij przycisk **Dalej**.

   Zostanie wyświetlony ekran **Advertisement Target** (Obiekt docelowy anonsowania).

8. Kliknij przycisk **Przeglądaj**, aby wybrać docelowe punkty końcowe.

   Zostanie wyświetlony ekran **Browse Collection** (Przeglądanie kolekcji).

9. Kliknij pozycję **Wszystkie systemy Windows NT**.

10. Kliknij przycisk **OK**.

    Ponownie zostanie wyświetlony ekran **Advertisement Target** (Obiekt docelowy anonsowania).

11. Kliknij przycisk **Dalej**.

    Zostanie wyświetlony ekran **Advertisement Name** (Nazwa anonsowanego obiektu).

12. W polach tekstowych wpisz nazwę i komentarz dla anonsu, a następnie kliknij przycisk **Dalej**.

    Zostanie wyświetlony ekran **Advertise to Subcollections** (Anonsowanie do podkolekcji).

13. Określ, czy pakiet ma być anonsowany w podkolekcjach. Można wybrać opcję anonsowania programu tylko członkom określonej kolekcji lub członkom podkolekcji.

14. Kliknij przycisk **Dalej**.

    Zostanie wyświetlony ekran **Advertisement Schedule** (Harmonogram anonsowania).

15. Wpisując lub wybierając datę i godzinę, określ, kiedy ma być anonsowany pakiet instalacyjny agenta OfficeScan.

    Uwaga

    Aby program Microsoft SMS przestał anonsować pakiet określonego dnia, kliknij opcję **Tak. Ten anons powinien wygasnąć**, a następnie określ datę i godzinę w oknach list **Data i godzina wygaśnięcia**.

16. Kliknij przycisk **Dalej**.

    Zostanie wyświetlony ekran **Assign Program** (Przydzielanie programu).

17. Kliknij opcję **Tak, przydziel program**, a następnie kliknij przycisk **Dalej**.

    Program Microsoft SMS utworzy anons i będzie go wyświetlać w konsoli administratora programu SMS.

18. Gdy program Microsoft SMS dystrybuuje i anonsuje program (tzn. program agenta OfficeScan) na komputerach docelowych, na każdym z tych punktów końcowych zostanie wyświetlony odpowiedni ekran. Należy poinformować użytkowników, aby kliknęli przycisk **Tak** i postępowali według instrukcji podanych przez kreatora w celu instalacji agenta OfficeScan na punktach końcowych.

Instalacja za pomocą obrazu dysku agenta

Technologia tworzenia obrazu dysku umożliwia utworzenie obrazu agenta OfficeScan za pomocą oprogramowania do tworzenia obrazów dysków i sklonowanie tego obrazu na innych komputerach w sieci.

Przy każdej instalacji agenta OfficeScan jest potrzebny unikatowy identyfikator globalny (GUID, Globally Unique Identifier) umożliwiający serwerowi identyfikowanie poszczególnych agentów. Program `ImgSetup.exe` wchodzący w skład programu OfficeScan pozwala tworzyć różne identyfikatory GUID dla każdego z klonów.

Tworzenie obrazu dysku agenta OfficeScan

Procedura

1. Zainstaluj agenta OfficeScan na punkcie końcowym.
2. Skopiuj plik `ImgSetup.exe` z lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\ImgSetup` na ten punkt końcowy.
3. Uruchom plik `ImgSetup.exe` na tym punkcie końcowym.

   Spowoduje to utworzenie klucza rejestru `RUN` w gałęzi `HKEY_LOCAL_MACHINE`.
4. Utwórz obraz dysku agenta OfficeScan za pomocą oprogramowania do tworzenia obrazów dysków.
5. Uruchom ponownie klon.

   Program `imgsetup.exe` uruchamia się automatycznie i tworzy nową wartość identyfikatora GUID. Agent OfficeScan zgłasza nową wartość identyfikatora GUID do serwera, a serwer tworzy nowy zapis dla nowego agenta OfficeScan.

OSTRZEŻENIE!

Aby uniknąć sytuacji, w której dwa komputery w bazie danych OfficeScan mają taką samą nazwę, należy pamiętać o ręcznej zmianie nazwy punktu końcowego lub domeny sklonowanego agenta OfficeScan.

Używanie narzędzia Vulnerability Scanner

Narzędzie Vulnerability Scanner służy do wykrywania zainstalowanych programów antywirusowych, wyszukiwania w sieci niezabezpieczonych komputerów oraz instalowania na nich agentów OfficeScan.

Uwagi dotyczące korzystania z narzędzia Vulnerability Scanner

Decydując się na zastosowanie narzędzia Vulnerability Scanner, należy wziąć pod uwagę następujące kwestie:

- *Zarządzanie siecią na stronie 5-44*
- *Topologia i architektura sieci na stronie 5-45*
- *Programowe/sprzętowe dane techniczne na stronie 5-45*
- *Struktura domeny na stronie 5-46*
- *Ruch sieciowy na stronie 5-46*
- *Rozmiar sieci na stronie 5-47*

Zarządzanie siecią

TABELA 5-7. Zarządzanie siecią

INSTALACJA	EFEKTYWNOŚĆ NARZĘDZIA VULNERABILITY SCANNER
Zarządzanie z zastosowaniem ścisłych reguł zabezpieczeń	Rozwiązanie zapewniające dużą efektywność. Narzędzie Vulnerability Scanner informuje, czy wszystkie komputery mają zainstalowany program antywirusowy.
Odpowiedzialność administratora rozłożona na różne witryny	Rozwiązanie zapewniające średnią wydajność
Administracja scentralizowana	Rozwiązanie zapewniające średnią wydajność
Usługa wykonywana przez zewnętrznych dostawców	Rozwiązanie zapewniające średnią wydajność
Użytkownicy sami zarządzają swoimi komputerami	Rozwiązanie nieefektywne. Ponieważ narzędzie Vulnerability Scanner skanuje sieć w poszukiwaniu zainstalowanych programów antywirusowych, nie ma możliwości, aby użytkownicy sami skanowali własne komputery.

Topologia i architektura sieci

Tabela 5-8. Topologia i architektura sieci

Instalacja	Efektywność narzędzia Vulnerability Scanner
Pojedyncza lokalizacja.	Rozwiązanie zapewniające dużą efektywność. Narzędzie Vulnerability Scanner zapewnia możliwość skanowania całego segmentu IP oraz łatwej instalacji agenta OfficeScan w sieci LAN.
Wiele lokalizacji z połączeniem o dużej szybkości	Rozwiązanie zapewniające średnią wydajność
Wiele lokalizacji z połączeniem o małej szybkości	Rozwiązanie nieefektywne. Narzędzie Vulnerability Scanner trzeba uruchamiać w każdej lokalizacji, a instalacja agenta OfficeScan musi być przekazywana na lokalny serwer OfficeScan.
Komputery zdalne i odizolowane	Rozwiązanie zapewniające średnią wydajność

Programowe/sprzętowe dane techniczne

Tabela 5-9. Programowe/sprzętowe dane techniczne

Instalacja	Efektywność narzędzia Vulnerability Scanner
System operacyjny typu Windows NT	Rozwiązanie zapewniające dużą efektywność. Narzędzie Vulnerability Scanner może z łatwością zdalnie instalować agenta OfficeScan na komputerach z systemem operacyjnym opartym na systemie Windows NT.
Mieszane systemy operacyjne	Rozwiązanie zapewniające średnią wydajność. Narzędzie Vulnerability Scanner może instalować klientów tylko na komputerach, na których jest uruchomiony system operacyjny oparty na systemie Windows NT.

Instalacja	Efektywność narzędzia Vulnerability Scanner
Oprogramowanie do zarządzania pulpitem	Rozwiązanie nieefektywne. Narzędzia Vulnerability Scanner nie można używać z oprogramowaniem do zarządzania pulpitem. Można go jednak używać do śledzenia postępu instalacji agenta OfficeScan.

Struktura domeny

Tabela 5-10. Struktura domeny

Instalacja	Efektywność narzędzia Vulnerability Scanner
Microsoft Active Directory	Rozwiązanie zapewniające dużą efektywność. Aby zezwolić na zdalną instalację agenta OfficeScan, w narzędziu Vulnerability Scanner należy określić konto administratora domeny.
Grupa robocza	Rozwiązanie nieefektywne. Narzędzie Vulnerability Scanner może mieć trudności z instalacją na komputerach korzystających z różnych kont administratora i haseł.
Usługa Novell™ Directory	Rozwiązanie nieefektywne. Do zainstalowania agenta OfficeScan narzędzie Vulnerability Scanner wymaga konta w domenie Windows.
Połączenia Peer-to-Peer	Rozwiązanie nieefektywne. Narzędzie Vulnerability Scanner może mieć trudności z instalacją na komputerach korzystających z różnych kont administratora i haseł.

Ruch sieciowy

Tabela 5-11. Ruch sieciowy

Instalacja	Efektywność narzędzia Vulnerability Scanner
Połączenie LAN	Rozwiązanie zapewniające dużą efektywność

Instalacja	Efektywność narzędzia Vulnerability Scanner
512 kb/s	Rozwiązanie zapewniające średnią wydajność
Łącze T1 lub szybsze	Rozwiązanie zapewniające średnią wydajność
Łącze telefoniczne	Rozwiązanie nieefektywne. Zakończenie instalacji agenta OfficeScan potrwa długo.

Rozmiar sieci

Tabela 5-12. Rozmiar sieci

Instalacja	Efektywność narzędzia Vulnerability Scanner
Bardzo duża korporacja	Rozwiązanie zapewniające dużą efektywność. Im większa sieć, tym więcej narzędzi Vulnerability Scanner jest potrzebnych do sprawdzenia instalacji agentów OfficeScan.
Małe i średnie firmy	Rozwiązanie zapewniające średnią wydajność. W małych sieciach narzędzie Vulnerability Scanner może być alternatywą do instalacji agenta OfficeScan. Inne metody instalacji agenta OfficeScan mogą się okazać o wiele łatwiejsze w realizacji.

Wytyczne dotyczące instalowania agenta OfficeScan przy użyciu narzędzia Vulnerability Scanner

Narzędzie Vulnerability Scanner nie zainstaluje agenta OfficeScan, jeśli:

- Serwer OfficeScan lub inne oprogramowanie zabezpieczające jest zainstalowane na hoście docelowym.
- Na zdalnym punkcie końcowym jest uruchomiony system operacyjny Windows XP Home, Windows Vista Home Basic, Windows Vista Home Premium, Windows 7 Home Basic, Windows 7 Home Premium, Windows 8 (wersje podstawowe), Windows 8.1 (wersje podstawowe) lub Windows 10 Home.

Uwaga

Agenta OfficeScan można zainstalować na hoście docelowym przy użyciu innych metod instalacji, które omówiono w temacie *Uwagi dotyczące instalacji na stronie 5-13*.

Przed użyciem narzędzia Vulnerability Scanner w celu zainstalowania agenta OfficeScan należy wykonać następujące czynności:

- W systemach Windows Vista (Business, Enterprise lub Ultimate), Windows 7 (Professional, Enterprise lub Ultimate), Windows 8 (Pro, Enterprise), Windows 8.1 (Pro, Enterprise), Windows 10 (Pro, Education, Enterprise), Windows Server 2012 (wszystkie edycje) albo Windows Server 2016 (wszystkie edycje):

  1. Włącz wbudowane konto administratora i ustaw hasło dla tego konta.
  2. Kliknij polecenie **Start** > **Programy** > **Narzędzia administracyjne** > **Zapora systemu Windows z zabezpieczeniami zaawansowanymi**.
  3. Dla opcji Profil domeny, Profil prywatny i Profil publiczny, ustaw stan zapory jako „Wyłączony”.
  4. Otwórz konsolę Microsoft Management Console (kliknij kolejno **Start**>**Uruchom**, wpisz polecenie `services.msc`) i uruchom usługę **Rejestr zdalny**. Podczas instalacji agenta OfficeScan należy używać wbudowanego konta i hasła administratora.

- W systemie Windows XP Professional (wersja 32- i 64-bitowa):

  1. Otwórz Eksploratora Windows i kliknij kolejno pozycje **Narzędzia**>**Opcje folderów**.
  2. Kliknij kartę **Widok** i wyłącz funkcję **Proste udostępnianie plików (zalecane)**.

Metody skanowania narażenia na atak

Skanowanie narażenia na atak sprawdza obecność oprogramowania zabezpieczającego na hostach i umożliwia instalację agenta OfficeScan na niezabezpieczonych hostach.

Istnieje kilka sposobów uruchamiania skanowania narażenia na atak.

TABELA 5-13. Metody skanowania narażenia na atak

METODA	SZCZEGÓŁY
Ręczne skanowanie narażenia na atak	Administratorzy mogą uruchamiać na żądanie skanowanie narażenia na atak.
Skanowanie DHCP	Administratorzy mogą uruchamiać skanowanie narażenia na atak na hostach żądających adresów IP z serwera DHCP. Narzędzie Vulnerability Scanner nasłuchuje na porcie 67, który stanowi port nasłuchiwania serwera DHCP dla żądań DHCP. Po wykryciu żądania DHCP z hosta uruchamiane jest skanowanie narażenia na atak na tym komputerze. **Uwaga** Narzędzie Vulnerability Scanner nie może wykrywać żądań DHCP w przypadku uruchomienia go w systemie Windows Server 2008, Windows 7, Windows 8, Windows 8.1, Windows 10 lub Windows Server 2012.
Zaplanowane skanowanie narażenia na atak	Skanowanie zaplanowane uruchamia się automatycznie zgodnie z harmonogramem skonfigurowanym przez administratora.

Po uruchomieniu narzędzie Vulnerability Scanner wyświetla stan agenta OfficeScan na hostach docelowych. Możliwe stany są następujące:

- **Zwykły**: Agent OfficeScan jest uruchomiony i działa prawidłowo
- **Nietypowy**: usługi agenta OfficeScan nie działają lub agent nie jest chroniony w czasie rzeczywistym
- **Niezainstalowany**: brak usługi TMListen lub Agent OfficeScan nie został zainstalowany
- **Nieosiągalny**: narzędzie Vulnerability Scanner nie mogło nawiązać połączenia z hostem ani określić stanu agenta OfficeScan

Uruchamianie ręcznego skanowania narażenia na atak

Procedura

1. Aby uruchomić skanowanie narażenia na atak na komputerze serwera OfficeScan, przejdź do lokalizacji <Folder instalacji serwera>`\PCCSRV\Admin\Utility\TMVS` i kliknij dwukrotnie plik `TMVS.exe`. Zostanie wyświetlona konsola narzędzia **Trend Micro Vulnerability Scanner**. Aby uruchomić skanowanie luk w zabezpieczeniach na innym punkcie końcowym z systemem Windows Server 2003, Server 2008, Vista, 7, 8, 8.1, 10 lub Server 2012/2016:

   a. Na komputerze serwera OfficeScan przejdź do lokalizacji `<Folder instalacji serwera>\PCCSRV\Admin\Utility`.

   b. Skopiuj folder `TMVS` na inny komputer.

   c. Na innym komputerze otwórz folder `TMVS` i kliknij dwukrotnie plik `TMVS.exe`.

      Zostanie wyświetlona konsola narzędzia **Trend Micro Vulnerability Scanner**.

   Uwaga

   Narzędzia nie można uruchamiać za serwera terminali.

2. Przejdź do sekcji **Skanowanie ręczne**.

3. Wpisz zakres adresów IP punktów końcowych, które mają być skanowane.

   a. Wpisz zakres adresów IPv4.

   Uwaga

   Narzędzie Vulnerability Scanner umożliwia sprawdzanie zakresu adresów IPv4 tylko w przypadku uruchomienia go na hoście wykorzystującym wyłącznie protokół IPv4 lub na hoście z dwoma stosami. Narzędzie Vulnerability Scanner obsługuje jedynie zakres adresów IP klasy B, na przykład od `168.212.1.1` do `168.212.254.254`.

b. W przypadku zakresu adresów IPv6 wpisz prefiks IPv6 i długość.

> **Uwaga**
>
> Narzędzie Vulnerability Scanner umożliwia sprawdzanie zakresu adresów IPv6 tylko w przypadku uruchomienia go na hoście wykorzystującym wyłącznie protokół IPv6 lub na hoście z dwoma stosami.

4. Kliknij **Ustawienia**.

   Zostanie wyświetlony ekran **Ustawienia**.

5. Skonfiguruj następujące ustawienia:

OPCJA	OPIS
Ustawienia polecenia ping	Narzędzie Vulnerability Scan może wysyłać polecenie „ping” na adresy IP określone w poprzednim kroku w celu sprawdzenia, czy są one obecnie używane. Jeśli host docelowy używa adresu IP, narzędzie Vulnerability Scanner może określić system operacyjny hosta. Szczegółowe informacje zawiera sekcja *Ustawienia polecenia ping na stronie 5-67*.
Metoda pobierania opisów komputerów	W przypadku hostów, które odpowiadają na polecenie „ping”, narzędzie Vulnerability Scanner może pobrać dodatkowe informacje o tych hostach. Szczegółowe informacje zawiera sekcja *Metoda pobierania opisów punktów końcowych na stronie 5-64*.
Zapytanie dotyczące produktu	Narzędzie Vulnerability Scanner może sprawdzać obecność oprogramowania zabezpieczającego na hostach docelowych. Szczegółowe informacje zawiera sekcja *Zapytanie dotyczące produktu na stronie 5-60*.
Ustawienia serwera OfficeScan	Ustawienia te należy skonfigurować, aby narzędzie Vulnerability Scanner automatycznie instalowało agenta OfficeScan na niezabezpieczonych hostach. Ustawienia serwera identyfikują serwer macierzysty agenta OfficeScan i poświadczenia administracyjne w celu użycia podczas logowania na hostach.

OPCJA	OPIS
	Szczegółowe informacje zawiera sekcja *Ustawienia serwera OfficeScan na stronie 5-68*. **Uwaga** Pewne warunki mogą uniemożliwiać instalację agenta OfficeScan na hostach docelowych. Szczegółowe informacje zawiera sekcja *Wytyczne dotyczące instalowania agenta OfficeScan przy użyciu narzędzia Vulnerability Scanner na stronie 5-47*.
Powiadomienia	Narzędzie Vulnerability Scanner może wysyłać wyniki skanowania narażenia na atak do administratorów OfficeScan. Może także wyświetlać powiadomienia na niezabezpieczonych hostach. Szczegółowe informacje zawiera sekcja *Powiadomienia na stronie 5-65*.
Zapisz wyniki	Oprócz wysyłania wyników skanowania narażenia na atak do administratorów, narzędzie Vulnerability Scan umożliwia także zapisywanie wyników do pliku `.csv`. Szczegółowe informacje zawiera sekcja *Wyniki skanowania narażenia na atak na stronie 5-66*.

6. Kliknij przycisk **OK**.

7. Kliknij przycisk **Start**.

   Wynik skanowania zostanie wyświetlony w tabeli **Wyniki** na karcie **Skanowanie ręczne**.

Uwaga

Jeśli na punkcie końcowym jest uruchomiony system operacyjny Windows Server 2008 lub Windows Server 2012, w tabeli **Wyniki** nie są wyświetlane informacje o adresie MAC.

8. Aby zapisać wyniki do pliku oddzielanego przecinkami (CSV), kliknij polecenie **Eksportuj**, wskaż folder, w którym ma zostać zapisany plik, a następnie wpisz nazwę pliku i kliknij polecenie **Zapisz**.

Uruchamianie skanowania DHCP

Procedura

1. Skonfiguruj ustawienia protokołu DHCP w pliku `TMVS.ini` znajdującym się w następującym katalogu: <Folder instalacji serwera>`\PCCSRV\Admin\Utility\TMVS`.

TABELA 5-14. Ustawienia DHCP w pliku `TMVS.ini`

USTAWIENIE	OPIS
DhcpThreadNum=x	Liczba wątków trybu DHCP. Minimalna wartość to 3, a maksymalna — 100. Domyślna wartość to 8.
DhcpDelayScan=x	To wyrażone w sekundach opóźnienie przed sprawdzeniem instalacji programu antywirusowego na punkcie końcowym wysyłającym żądanie. Minimalna wartość to 0 (nie czekaj), a maksymalna — 600. Domyślna wartość to 30.
LogReport=x	Wartość 0 wyłącza rejestrowanie, 1 — włącza. Narzędzie Vulnerability Scanner może wysyłać wyniki skanowania do serwera OfficeScan. Dzienniki są wyświetlane na ekranie **Dzienniki zdarzeń systemowych** w konsoli Web.
OsceServer=x	Adres IP lub nazwa DNS serwera OfficeScan.
OsceServerPort=x	Jest to port serwera Web na serwerze OfficeScan.

2. Aby uruchomić skanowanie narażenia na atak na komputerze serwera OfficeScan, przejdź do lokalizacji <Folder instalacji serwera>`\PCCSRV\Admin\Utility\TMVS` i kliknij dwukrotnie plik `TMVS.exe`. Zostanie wyświetlona konsola narzędzia **Trend Micro Vulnerability Scanner**. Aby uruchomić skanowanie luk

w zabezpieczeniach na innym punkcie końcowym z systemem Windows Server 2003, Server 2008, Vista, 7, 8, 8.1, 10 lub Server 2012/2016:

a. Na komputerze serwera OfficeScan przejdź do lokalizacji `<Folder instalacji serwera>\PCCSRV\Admin\Utility`.

b. Skopiuj folder `TMVS` na inny komputer.

c. Na innym komputerze otwórz folder `TMVS` i kliknij dwukrotnie plik `TMVS.exe`.

   Zostanie wyświetlona konsola narzędzia **Trend Micro Vulnerability Scanner**.

Uwaga

Narzędzia nie można uruchamiać za serwera terminali.

3. W sekcji **Skanowanie ręczne** kliknij opcję **Ustawienia**.

   Zostanie wyświetlony ekran **Ustawienia**.

4. Skonfiguruj następujące ustawienia:

OPCJA	OPIS
Zapytanie dotyczące produktu	Narzędzie Vulnerability Scanner może sprawdzać obecność oprogramowania zabezpieczającego na hostach docelowych. Szczegółowe informacje zawiera sekcja *Zapytanie dotyczące produktu na stronie 5-60*.
Ustawienia serwera OfficeScan	Ustawienia te należy skonfigurować, aby narzędzie Vulnerability Scanner automatycznie instalowało agenta OfficeScan na niezabezpieczonych hostach. Ustawienia serwera identyfikują serwer macierzysty agenta OfficeScan i poświadczenia administracyjne w celu użycia podczas logowania na hostach. Szczegółowe informacje zawiera sekcja *Ustawienia serwera OfficeScan na stronie 5-68*.

OPCJA	OPIS
	Uwaga Pewne warunki mogą uniemożliwiać instalację agenta OfficeScan na hostach docelowych. Szczegółowe informacje zawiera sekcja *Wytyczne dotyczące instalowania agenta OfficeScan przy użyciu narzędzia Vulnerability Scanner na stronie 5-47*.
Powiadomienia	Narzędzie Vulnerability Scanner może wysyłać wyniki skanowania narażenia na atak do administratorów OfficeScan. Może także wyświetlać powiadomienia na niezabezpieczonych hostach. Szczegółowe informacje zawiera sekcja *Powiadomienia na stronie 5-65*.
Zapisz wyniki	Oprócz wysyłania wyników skanowania narażenia na atak do administratorów, narzędzie Vulnerability Scan umożliwia także zapisywanie wyników do pliku `.csv`. Szczegółowe informacje zawiera sekcja *Wyniki skanowania narażenia na atak na stronie 5-66*.

5. Kliknij przycisk **OK**.

6. Na karcie **Wyniki** kliknij kartę **Skanowanie DHCP**.

Uwaga

Karta **Skanowanie DHCP** jest niedostępna na komputerach z systemem operacyjnym Windows Server 2008, Windows 7, Windows 8, Windows 8.1, Windows 10 oraz Windows Server 2012.

7. Kliknij przycisk **Start**.

   Narzędzie Vulnerability Scanner rozpocznie nasłuchiwanie żądań DHCP i sprawdzi narażenie komputerów na atak, kiedy będą się logować do sieci.

8. Aby zapisać wyniki do pliku oddzielanego przecinkami (CSV), kliknij polecenie **Eksportuj**, wskaż folder, w którym ma zostać zapisany plik, a następnie wpisz nazwę pliku i kliknij polecenie **Zapisz**.

Konfigurowanie zaplanowanego skanowania narażenia na atak

Procedura

1. Aby uruchomić skanowanie narażenia na atak na komputerze serwera OfficeScan, przejdź do lokalizacji <Folder instalacji serwera>`\PCCSRV\Admin\Utility\TMVS` i kliknij dwukrotnie plik `TMVS.exe`. Zostanie wyświetlona konsola narzędzia **Trend Micro Vulnerability Scanner**. Aby uruchomić skanowanie luk w zabezpieczeniach na innym punkcie końcowym z systemem Windows Server 2003, Server 2008, Vista, 7, 8, 8.1, 10 lub Server 2012/2016:

   a. Na komputerze serwera OfficeScan przejdź do lokalizacji `<Folder instalacji serwera>\PCCSRV\Admin\Utility`.

   b. Skopiuj folder `TMVS` na inny komputer.

   c. Na innym komputerze otwórz folder `TMVS` i kliknij dwukrotnie plik `TMVS.exe`.

      Zostanie wyświetlona konsola narzędzia **Trend Micro Vulnerability Scanner**.

   Uwaga

   Narzędzia nie można uruchamiać za serwera terminali.

2. Przejdź do sekcji **Skanowanie zaplanowane**.

3. Kliknij przycisk **Dodaj/Edytuj**.

   Zostanie wyświetlony ekran **Skanowanie zaplanowane**.

4. Wpisz nazwę zaplanowanego skanowania narażenia na atak.

5. Wpisz zakres adresów IP punktów końcowych, które mają być skanowane.

   a. Wpisz zakres adresów IPv4.

Uwaga

Narzędzie Vulnerability Scanner umożliwia sprawdzanie zakresu adresów IPv4 tylko w przypadku uruchomienia go na hoście wykorzystującym wyłącznie protokół IPv4 lub na hoście z dwoma stosami. Narzędzie Vulnerability Scanner obsługuje jedynie zakres adresów IP klasy B, na przykład od `168.212.1.1` do `168.212.254.254`.

b. W przypadku zakresu adresów IPv6 wpisz prefiks IPv6 i długość.

Uwaga

Narzędzie Vulnerability Scanner umożliwia sprawdzanie zakresu adresów IPv6 tylko w przypadku uruchomienia go na hoście wykorzystującym wyłącznie protokół IPv6 lub na hoście z dwoma stosami.

6. Określ godzinę początkową **harmonogramu** przy użyciu 24-godzinnego formatu czasu, a następnie ustal częstotliwość uruchamiania skanowania: codziennie, raz w tygodniu lub raz w miesiącu.

7. Wybierz zestaw ustawień skanowania narażenia na atak, które mają być używane.

   a. Wybierz opcję **Użyj bieżących ustawień**, jeśli skonfigurowano ustawienia ręcznego skanowania narażenia na atak i chcesz użyć tych ustawień.

      Szczegółowe informacje o ustawieniach ręcznego skanowania narażenia na atak zawiera sekcja *Uruchamianie ręcznego skanowania narażenia na atak na stronie 5-50*.

   b. Jeśli ustawienia ręcznego skanowania na atak nie zostały określone lub chcesz użyć innego zestawu ustawień, wybierz opcję **Zmień ustawienia**, a następnie kliknij opcję **Ustawienia**.

      Zostanie wyświetlony ekran **Ustawienia**.

   c. Skonfiguruj następujące ustawienia:

Ustawienia polecenia ping	Narzędzie Vulnerability Scan może wysyłać polecenie „ping” na adresy IP określone w poprzednim kroku w celu sprawdzenia, czy są one obecnie używane. Jeśli host docelowy używa adresu IP, narzędzie Vulnerability Scanner może określić system operacyjny hosta. Szczegółowe informacje zawiera sekcja *Ustawienia polecenia ping na stronie 5-67*.
Metoda pobierania opisów komputerów	W przypadku hostów, które odpowiadają na polecenie „ping”, narzędzie Vulnerability Scanner może pobrać dodatkowe informacje o tych hostach. Szczegółowe informacje zawiera sekcja *Metoda pobierania opisów punktów końcowych na stronie 5-64*.
Zapytanie dotyczące produktu	Narzędzie Vulnerability Scanner może sprawdzać obecność oprogramowania zabezpieczającego na hostach docelowych. Szczegółowe informacje zawiera sekcja *Zapytanie dotyczące produktu na stronie 5-60*.
Ustawienia serwera OfficeScan	Ustawienia te należy skonfigurować, aby narzędzie Vulnerability Scanner automatycznie instalowało agenta OfficeScan na niezabezpieczonych hostach. Ustawienia serwera identyfikują serwer macierzysty agenta OfficeScan i poświadczenia administracyjne w celu użycia podczas logowania na hostach. Szczegółowe informacje zawiera sekcja *Ustawienia serwera OfficeScan na stronie 5-68*. **Uwaga** Pewne warunki mogą uniemożliwiać instalację agenta OfficeScan na hostach docelowych. Szczegółowe informacje zawiera sekcja *Wytyczne dotyczące instalowania agenta OfficeScan przy użyciu narzędzia Vulnerability Scanner na stronie 5-47*.

Powiadomienia	Narzędzie Vulnerability Scanner może wysyłać wyniki skanowania narażenia na atak do administratorów OfficeScan. Może także wyświetlać powiadomienia na niezabezpieczonych hostach. Szczegółowe informacje zawiera sekcja *Powiadomienia na stronie 5-65*.
Zapisz wyniki	Oprócz wysyłania wyników skanowania narażenia na atak do administratorów, narzędzie Vulnerability Scan umożliwia także zapisywanie wyników do pliku `.csv`. Szczegółowe informacje zawiera sekcja *Wyniki skanowania narażenia na atak na stronie 5-66*.

8. Kliknij przycisk **OK**.

   Ekran **Skanowanie zaplanowane** zostanie zamknięty. Utworzone zaplanowane skanowanie narażenia na atak pojawi się w sekcji **Skanowanie zaplanowane**. Jeśli włączono powiadomienia, narzędzie Vulnerability Scanner wyśle wyniki zaplanowanego skanowania narażenia na atak.

9. Aby natychmiast wykonać zaplanowane skanowanie narażenia na atak, kliknij opcję **Uruchom teraz**.

   Wyniki skanowania zostaną wyświetlone w tabeli **Wyniki** na karcie **Skanowanie zaplanowane**.

   Uwaga

   Jeśli na punkcie końcowym jest uruchomiony system operacyjny Windows Server 2008 lub Windows Server 2012, w tabeli **Wyniki** nie są wyświetlane informacje o adresie MAC.

10. Aby zapisać wyniki do pliku oddzielanego przecinkami (CSV), kliknij polecenie **Eksportuj**, wskaż folder, w którym ma zostać zapisany plik, a następnie wpisz nazwę pliku i kliknij polecenie **Zapisz**.

Ustawienia skanowania narażenia na atak

Ustawienia skanowania narażenia na atak są konfigurowane za pomocą narzędzia Trend Micro Vulnerability Scanner (`TMVS.exe`) lub w pliku `TMVS.ini`.

Uwaga

W sekcji *Tworzenie dzienników diagnostycznych serwera z wykorzystaniem pliku LogServer.exe na stronie 18-3* można znaleźć więcej informacji na temat sposobów debugowania dzienników narzędzia Vulnerability Scanner.

Zapytanie dotyczące produktu

Narzędzie Vulnerability Scanner może sprawdzać obecność oprogramowania zabezpieczającego na agentach. Poniższa tabela przedstawia sposób sprawdzania programów zabezpieczających przez narzędzie Vulnerability Scanner:

TABELA 5-15. Programy zabezpieczające sprawdzane przez narzędzie Vulnerability Scanner

PRODUKT	OPIS
ServerProtect do systemów Windows	Narzędzie Vulnerability Scanner wykorzystuje punkt końcowy RPC, aby sprawdzić, czy jest uruchomiony proces `SPNTSVC.exe`. Zwraca informacje zawierające dane na temat systemu operacyjnego, silnika skanowania antywirusowego, sygnatur wirusów oraz wersji programu. Narzędzie Vulnerability Scanner nie wykrywa programów ServerProtect Information Server ani ServerProtect Management Console.
ServerProtect do systemów Linux	Jeśli docelowy punkt końcowy nie działa w systemie Windows, narzędzie Vulnerability Scanner sprawdzi, czy ma on zainstalowany program ServerProtect for Linux, próbując połączyć się z portem 14942.

PRODUKT	OPIS
Agent OfficeScan	W celu sprawdzenia, czy jest zainstalowany Agent OfficeScan, narzędzie Vulnerability Scanner wykorzystuje port agenta OfficeScan. Sprawdza również, czy jest uruchomiony proces `TmListen.exe`. Narzędzie automatycznie pobiera numer portu, o ile działa w domyślnej lokalizacji. Jeśli narzędzie Vulnerability Scanner zostało uruchomione na innym punkcie końcowym niż serwer OfficeScan, należy sprawdzić port komunikacyjny tego punktu końcowego i użyć go.
PortalProtect™	Aby sprawdzić instalację produktu, narzędzie Vulnerability Scanner otwiera stronę internetową `http://localhost:port/PortalProtect/index.html`.
ScanMail™ for Microsoft Exchange™	Aby sprawdzić instalację programu ScanMail, narzędzie Vulnerability Scanner otwiera stronę internetową `http://ipaddress:port/scanmail.html`. Domyślnie program ScanMail wykorzystuje port 16372. W przypadku korzystania z innego portu należy wpisać jego numer. W przeciwnym razie narzędzie Vulnerability Scanner nie wykryje programu ScanMail.
Rodzina InterScan™	W celu sprawdzenia, czy jest zainstalowany program, narzędzie Vulnerability Scanner wczytuje odpowiednie strony internetowe. • InterScan Messaging Security Suite 5.x: `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan eManager 3.x: `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan VirusWall™ 3.x: `http://localhost:port/InterScan/cgi-bin/interscan.dll`
Trend Micro Internet Security™ (PC-cillin)	W celu sprawdzenia, czy jest zainstalowany program Trend Micro Internet Security, narzędzie Vulnerability Scanner wykorzystuje port 40116.

Produkt	Opis
McAfee VirusScan ePolicy Orchestrator	Aby zapewnić połączenie pomiędzy serwerem a agentem, narzędzie Vulnerability Scanner wysyła specjalny znacznik do portu 8081 protokołu TCP, domyślnego portu programu ePolicy Orchestrator. Punkt końcowy, na którym jest zainstalowane to oprogramowanie antywirusowe, odpowiada za pomocą znacznika specjalnego typu. Narzędzie Vulnerability Scanner nie wykrywa samodzielnych instalacji programu McAfee VirusScan.
Norton Antivirus™ Corporate Edition	Narzędzie Vulnerability Scanner wyśle specjalny token do portu 2967 protokołu UDP, domyślnego portu programu Norton Antivirus Corporate Edition RTVScan. Punkt końcowy, na którym jest zainstalowane to oprogramowanie antywirusowe, odpowiada za pomocą znacznika specjalnego typu. Ponieważ oprogramowanie Norton Antivirus Corporate Edition komunikuje się za pomocą protokołu UDP, skuteczność odpowiedzi nie jest gwarantowana. Dodatkowo wzmożony ruch sieciowy może wpływać na wydłużenie czasu oczekiwania protokołu UDP.

Narzędzie Vulnerability Scanner wykrywa programy i komputery, wykorzystując następujące protokoły:

- **RPC**: do wykrywania programu ServerProtect w systemie NT
- **UDP**: do wykrywania klientów oprogramowania Norton AntiVirus Corporate Edition
- **TCP**: do wykrywania programu McAfee VirusScan ePolicy Orchestrator
- **ICMP**: do wykrywania komputerów przez wysyłanie pakietów ICMP
- **HTTP**: do wykrywania agentów OfficeScan
- **DHCP**: jeśli wykryto żądanie DHCP, narzędzie Vulnerability Scanner sprawdza, czy na punkcie końcowym wysyłającym żądanie jest już zainstalowane oprogramowanie antywirusowe.

Konfigurowanie ustawień zapytań dotyczącej produktu

Ustawienia zapytań dotyczącej produktu stanowią podzestaw ustawień skanowania narażenia na atak. Szczegółowe informacje o ustawieniach skanowania narażenia na atak zawiera sekcja *Metody skanowania narażenia na atak na stronie 5-48*.

Procedura

1. Aby określić ustawienia zapytań dotyczącej produktu w narzędziu Vulnerability Scanner (`TMVS.exe`):
   a. Uruchom plik `TMVS.exe`.
   b. Kliknij **Ustawienia**.
      Zostanie wyświetlony ekran **Ustawienia**.
   c. Przejdź do sekcji **Zapytanie dotyczące produktu**.
   d. Wybierz produkty do sprawdzenia.
   e. Kliknij opcję **Ustawienia** obok nazwy produktu, a następnie podaj numer portu, który będzie sprawdzany przez narzędzie Vulnerability Scanner.
   f. Kliknij przycisk **OK**.
      Ekran **Ustawienia** zostanie zamknięty.
2. Aby ustawić liczbę komputerów, które narzędzie Vulnerability Scanner będzie jednocześnie sprawdzać po kątem oprogramowania zabezpieczającego:
   a. Przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\TMVS` i otwórz plik `TMVS.ini` za pomocą edytora tekstu, np. Notatnika.
   b. Aby ustawić liczbę komputerów sprawdzanych podczas ręcznego skanowania narażenia na atak, zmień wartość opcji `ThreadNumManual`. Podaj wartość między 8 a 64.
      Można na przykład wpisać wartość `ThreadNumManual=60`, aby narzędzie Vulnerability Scanner sprawdzało jednocześnie 60 komputerów.
   c. Aby ustawić liczbę komputerów sprawdzanych podczas zaplanowanego skanowania narażenia na atak, zmień wartość opcji `ThreadNumSchedule`. Podaj wartość między 8 a 64.

Można na przykład wpisać wartość `ThreadNumSchedule=50`, aby narzędzie Vulnerability Scanner sprawdzało jednocześnie 50 komputerów.

d. Zapisz plik `TMVS.ini`.

Metoda pobierania opisów punktów końcowych

Gdy narzędzie Vulnerability Scanner może wysyłać polecenia „ping" do hostów, możliwe jest uzyskanie dodatkowych informacji o tych hostach. Istnieją dwie metody pobierania informacji:

- **Szybkie pobieranie**: jest pobierana tylko nazwa punktu końcowego.
- **Zwykłe pobieranie**: są pobierane informacje o domenie i punkcie końcowym

Konfigurowanie ustawień pobierania

Ustawienia pobierania stanowią podzestaw ustawień skanowania narażenia na atak. Szczegółowe informacje o ustawieniach skanowania narażenia na atak zawiera sekcja *Metody skanowania narażenia na atak na stronie 5-48*.

Procedura

1. Uruchom plik `TMVS.exe`.
2. Kliknij **Ustawienia**.

   Zostanie wyświetlony ekran **Ustawienia**.
3. Przejdź do sekcji **Metoda pobierania opisów komputerów**.
4. Wybierz opcję **Normalna** lub **Szybka**.
5. W przypadku wybrania metody **Normalna** wybierz opcję **Pobierz opisy komputerów, kiedy tylko są dostępne**.
6. Kliknij przycisk **OK**.

   Ekran **Ustawienia** zostanie zamknięty.

Powiadomienia

Narzędzie Vulnerability Scanner może wysyłać wyniki skanowania narażenia na atak do administratorów OfficeScan. Może także wyświetlać powiadomienia na niezabezpieczonych hostach.

Konfigurowanie ustawień powiadamiania

Ustawienia powiadamiania stanowią podzestaw ustawień skanowania narażenia na atak. Szczegółowe informacje o ustawieniach skanowania narażenia na atak zawiera sekcja *Metody skanowania narażenia na atak na stronie 5-48*.

Procedura

1. Uruchom plik `TMVS.exe`.
2. Kliknij **Ustawienia**.

   Zostanie wyświetlony ekran **Ustawienia**.
3. Przejdź do sekcji **Powiadomienia**.
4. Aby automatycznie wysyłać wyniki narzędzia Vulnerability Scan do administratorów w organizacji:

   a. Wybierz opcję **Wyślij wyniki pocztą e-mail do administratora systemu**.

   b. Kliknij opcję **Konfiguruj**, aby określić ustawienia poczty e-mail.

   c. W polu **Do** wpisz adres e-mail odbiorcy.

   d. W polu **Od** wpisz adres e-mail nadawcy.

   e. W polu **Serwer SMTP** wpisz adres serwera SMTP.

      Przykładowy adres to `smtp.firma.com`. Informacja o serwerze SMTP jest wymagana.

   f. W polu **Temat** wpisz nowy temat wiadomości lub zatwierdź domyślny.

   g. Kliknij przycisk **OK**.
5. Aby poinformować użytkowników, że na ich komputerach nie jest zainstalowane żadne oprogramowanie zabezpieczające:

a. Wybierz opcję **Wyświetl powiadomienie na niechronionych komputerach**.

b. Kliknij polecenie **Dostosuj,** aby skonfigurować powiadomienia programu.

c. Na ekranie **Powiadomienie programu** wpisz treść nowej wiadomości lub zatwierdź domyślną wiadomość.

d. Kliknij przycisk **OK**.

6. Kliknij przycisk **OK**.

   Ekran **Ustawienia** zostanie zamknięty.

Wyniki skanowania narażenia na atak

Narzędzie Vulnerability Scanner można skonfigurować w celu zapisywania wyników skanowania narażenia na atak do pliku rozdzielanego przecinkami (CSV).

Konfigurowanie wyników skanowania

Ustawienia wyników skanowania narażenia na atak stanowią podzestaw ustawień skanowania narażenia na atak. Szczegółowe informacje o ustawieniach skanowania narażenia na atak zawiera sekcja *Metody skanowania narażenia na atak na stronie 5-48*.

Procedura

1. Uruchom plik `TMVS.exe`.
2. Kliknij **Ustawienia**.

   Zostanie wyświetlony ekran **Ustawienia**.

3. Przejdź do sekcji **Zapisz wyniki**.
4. Wybierz opcję **Automatycznie zapisz wyniki w pliku CSV**.
5. Aby zmienić domyślny folder zapisywania plików `CSV`:

   a. Kliknij przycisk **Przeglądaj**.

b. Wybierz folder docelowy na punkcie końcowym lub w sieci.

c. Kliknij przycisk **OK**.

6. Kliknij przycisk **OK**.

   Ekran **Ustawienia** zostanie zamknięty.

Ustawienia polecenia ping

Ustawienia polecenia „ping" umożliwiają sprawdzenie istnienia komputera docelowego i określenie jego systemu operacyjnego. Jeśli ustawienia te są wyłączone, narzędzie Vulnerability Scanner skanuje wszystkie adresy IP w określonym zakresie adresów IP — nawet te, które nie są używane przez żadnego hosta — przez co skanowanie trwa dłużej niż powinno.

Konfigurowanie ustawień polecenia ping

Ustawienia polecenia ping stanowią podzestaw ustawień skanowania narażenia na atak. Szczegółowe informacje o ustawieniach skanowania narażenia na atak zawiera sekcja *Metody skanowania narażenia na atak na stronie 5-48*.

Procedura

1. Aby określić ustawienia polecenia ping w narzędziu Vulnerability Scanner (`TMVS.exe`):

   a. Uruchom plik `TMVS.exe`.

   b. Kliknij **Ustawienia**.

      Zostanie wyświetlony ekran **Ustawienia**.

   c. Przejdź do sekcji ustawień polecenia **ping**.

   d. Wybierz opcję **Zezwól narzędziu Vulnerability Scanner na wysyłanie polecenia ping do komputerów w sieci w celu sprawdzenia ich stanu**.

   e. W polach **Rozmiar pakietu** i **Limit czasu** zaakceptuj lub zmodyfikuj wartości domyślne.

f. Wybierz opcję **Wykryj typ systemu operacyjnego za pomocą pakietu identyfikacyjnego ICMP OS**.

Jeśli wybierzesz tę opcję, narzędzie Vulnerability Scanner będzie sprawdzać, czy na hoście działa system operacyjny Windows lub inny system. W przypadku hostów z systemem Windows narzędzie Vulnerability Scanner może zidentyfikować wersję systemu Windows.

g. Kliknij przycisk **OK**.

Ekran **Ustawienia** zostanie zamknięty.

2. Aby ustawić liczbę komputerów, do których narzędzie Vulnerability Scanner będzie jednocześnie wysyłać polecenie ping:

a. Przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\TMVS` i otwórz plik `TMVS.ini` za pomocą edytora tekstu, np. Notatnika.

b. Zmień wartość opcji `EchoNum`. Podaj wartość między 1 a 64.

Przykładowo, można wpisać wartość `EchoNum=60`, aby narzędzie Skaner narażenia na atak wysyłało polecenie ping jednocześnie do 60 komputerów.

c. Zapisz plik `TMVS.ini`.

Ustawienia serwera OfficeScan

Ustawienia serwera OfficeScan są używane w następujących przypadkach:

- Narzędzie Vulnerability Scanner instaluje agenta OfficeScan na niezabezpieczonych komputerach docelowych. Ustawienia serwera umożliwiają narzędziu Vulnerability Scanner zidentyfikowanie serwera macierzystego agenta OfficeScan i poświadczeń administracyjnych w celu użycia podczas logowania na komputerach docelowych.

Uwaga

Pewne warunki mogą uniemożliwiać instalację agenta OfficeScan na hostach docelowych.

Szczegółowe informacje zawiera sekcja *Wytyczne dotyczące instalowania agenta OfficeScan przy użyciu narzędzia Vulnerability Scanner na stronie 5-47*.

- Narzędzie Vulnerability Scanner wysyła dzienniki instalacji agenta do serwera OfficeScan.

Konfigurowanie ustawień serwera OfficeScan

Ustawienia serwera OfficeScan stanowią podzestaw ustawień skanowania narażenia na atak. Szczegółowe informacje o ustawieniach skanowania narażenia na atak zawiera sekcja *Metody skanowania narażenia na atak na stronie 5-48*.

Procedura

1. Uruchom plik `TMVS.exe`.
2. Kliknij **Ustawienia**.

   Zostanie wyświetlony ekran **Ustawienia**.
3. Przejdź do sekcji **Ustawienia serwera OfficeScan**.
4. Wpisz nazwę serwera OfficeScan i jego numer portu.
5. Wybierz opcję **Automatycznie instaluj agenta OfficeScan na niezabezpieczonych komputerach**.
6. Aby skonfigurować poświadczenia administracyjne:
   a. Kliknij opcję **Konto instalacyjne**.
   b. Na ekranie **Informacje o koncie** wpisz nazwę użytkownika i hasło.
   c. Kliknij przycisk **OK**.
7. Wybierz opcję **Prześlij dzienniki do serwera OfficeScan**.
8. Kliknij przycisk **OK**.

   Ekran **Ustawienia** zostanie zamknięty.

Instalowanie zgodne z zabezpieczeniami

Zainstaluj agentów OfficeScan na komputerach wewnątrz domeny sieciowej lub zainstaluj agenta OfficeScan na docelowym punkcie końcowym z użyciem adresu IP.

Przed zainstalowaniem agenta OfficeScan należy wziąć pod uwagę następujące kwestie:

Procedura

1. Zapisać poświadczenia logowania dotyczące poszczególnych punktów końcowych. Program OfficeScan wyświetli monit o podanie tych poświadczeń podczas instalacji.

2. Agent OfficeScan nie jest instalowany na punkcie końcowym w następujących przypadkach:

   - Na punkcie końcowym jest zainstalowany serwer OfficeScan.

   - Na punkcie końcowym jest uruchomiony system operacyjny Windows XP Home, Windows Vista Home Basic, Windows Vista Home Premium, Windows 7™ Starter, Windows 7 Home Basic, Windows 7 Home Premium, Windows 8 (wersje podstawowe), Windows 8.1 (wersje podstawowe) lub Windows 10 Home. W przypadku posiadania komputera z jednym z wymienionych systemów należy wybrać inną metodę instalacji. Szczegółowe informacje można znaleźć w części *Uwagi dotyczące instalacji na stronie 5-13*.

3. Jeśli na docelowym punkcie końcowym jest uruchomiony system operacyjny Windows Vista (Business, Enterprise lub Ultimate), Windows 7 (Professional, Enterprise lub Ultimate), Windows 8 (Pro, Enterprise), Windows 8.1 (Pro, Enterprise), Windows 10 (Pro, Education, Enterprise) lub Windows Server 2012 (Standard), należy na nim wykonać następujące czynności:

   a. Włącz wbudowane konto administratora i ustaw hasło dla tego konta.

   b. Wyłącz zaporę systemu Windows.

   c. Kliknij polecenie **Początek** > **Programy** > **Narzędzia administracyjne** > **Zapora systemu Windows z zabezpieczeniami zaawansowanymi**.

   d. Dla opcji Profil domeny, Profil prywatny i Profil publiczny, ustaw stan zapory jako „Wyłączony”.

   e. Otwórz konsolę Microsoft Management Console (kliknij **pozycje Początek** > **Uruchom** i wpisz polecenie `services.msc`) i uruchom usługę **Rejestr zdalny**. Podczas instalacji agenta OfficeScan należy używać wbudowanego konta i hasła administratora.

4. Jeśli na punkcie końcowym są zainstalowane zabezpieczające punkty końcowe programy firmy Trend Micro lub innych firm, sprawdź, czy program OfficeScan może automatycznie odinstalować to oprogramowanie i zastąpić je agentem OfficeScan. Lista oprogramowania zabezpieczającego agentów, które może być automatycznie odinstalowywane przez program OfficeScan, znajduje się w wymienionych niżej plikach dostępnych w lokalizacji <*Folder instalacji foldera*>\PCCSRV\Admin. Pliki te można otworzyć za pomocą edytora tekstu takiego jak Notatnik.

   - `tmuninst.ptn`
   - `tmuninst_as.ptn`

   Jeśli oprogramowanie docelowego punktu końcowego nie znajduje się na liście, należy je najpierw ręcznie odinstalować. W zależności od procesu dezinstalacji oprogramowania punkt końcowy może wymagać ponownego uruchomienia.

Instalowanie agenta OfficeScan

Procedura

1. Przejdź do opcji **Ocena** > **Niezarządzane punkty końcowe**.
2. Kliknij pozycję **Instaluj** w górnej części drzewa agentów.
   - Jeśli na punkcie końcowym jest zainstalowana starsza wersja agenta OfficeScan i zostanie kliknięte polecenie **Zainstaluj**, instalacja zostanie pominięta, a agent nie zostanie uaktualniony do bieżącej wersji. Aby uaktualnić agenta, należy wyłączyć ustawienie.
     a. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
     b. Kliknij kartę **Ustawienia** > **Uprawnienia i inne ustawienia** > **Inne ustawienia**.
     c. Wyłącz opcję **Agenci OfficeScan mogą aktualizować składniki, ale nie mogą modernizować programu agenta ani instalować poprawek**.

3. Skonfiguruj konto logowania administratora na każdym punkcie końcowym i kliknij polecenie **Zaloguj**. Program OfficeScan rozpocznie instalowanie agenta na docelowym punkcie końcowym.
4. Wyświetl stan instalacji.

Migracja do agenta OfficeScan

Zainstalowane na docelowym punkcie końcowym oprogramowanie zabezpieczające agenta można zastąpić agentem OfficeScan.

Migracja z innego oprogramowania zabezpieczającego punkt końcowy

Podczas instalowania agenta ScanOffice program instalacyjny sprawdza, czy na docelowym punkcie końcowym jest zainstalowane oprogramowanie zabezpieczające punkt końcowy firmy Trend Micro lub innego producenta. Program instalacyjny automatycznie dezinstaluje takie oprogramowanie i zastępuje je agentem OfficeScan.

Lista oprogramowania zabezpieczającego punkty końcowe, które może być automatycznie odinstalowywane przez program OfficeScan, znajduje się w wymienionych niżej plikach dostępnych w lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin`. Pliki ten należy otworzyć za pomocą edytora tekstu takiego jak Notatnik.

- `tmuninst.ptn`
- `tmuninst_as.ptn`

Jeśli oprogramowanie docelowego punktu końcowego nie znajduje się na liście, należy je najpierw ręcznie odinstalować. W zależności od procesu dezinstalacji oprogramowania punkt końcowy może wymagać ponownego uruchomienia.

Problemy z migracją agenta OfficeScan

- Jeśli automatyczna migracja agenta powiedzie się, ale po zainstalowaniu wystąpią problemy z agentem OfficeScan, należy uruchomić ponownie punkt końcowy.
- Jeśli program instalacyjny OfficeScan rozpocznie instalowanie agenta OfficeScan, ale nie będzie w stanie zdezinstalować istniejącego oprogramowania zabezpieczającego, mogą występować konflikty między dwoma programami. Odinstaluj oba programy, a następnie zainstaluj agenta OfficeScan, używając dowolnej metody instalacji omówionej w sekcji *Uwagi dotyczące instalacji na stronie 5-13*.

Migracja z serwerów ServerProtect Normal Server

Narzędzie ServerProtect™ Normal Server Migration umożliwia migrację komputerów z zainstalowanym serwerem Trend Micro ServerProtect Normal Server do agenta OfficeScan.

Narzędzie ServerProtect Normal Server Migration Tool ma takie same wymagania dotyczące konfiguracji sprzętowej i programowej, jak serwer OfficeScan. Narzędzie należy uruchomić na komputerach z systemem Windows Server 2003 lub Windows Server 2008.

Jeśli dezinstalacja serwera ServerProtect Normal Server powiedzie się, zostanie zainstalowany Agent OfficeScan. Narzędzie migruje do agenta OfficeScan również ustawienia lista wykluczeń skanowania (dotyczy wszystkich typów skanowania).

Podczas instalacji agenta OfficeScan może zostać przekroczony limit czasu instalatora agenta narzędzia migracji. Zostanie wtedy wyświetlony komunikat o niepowodzeniu instalacji. Instalacja agenta OfficeScan mogła jednak zakończyć się powodzeniem. Zweryfikuj instalację na punkcie końcowym agenta z poziomu konsoli Web programu OfficeScan.

Migracja zakończy się niepowodzeniem w następujących przypadkach:

- Agent zdalny ma tylko adres IPv6. Narzędzie migracji nie obsługuje adresowania IPv6.
- Agent zdalny nie może używać protokołu NetBIOS.

- Porty 455, 337 lub 339 są zablokowane.
- Agent zdalny nie może używać protokołu RPC.
- Zatrzymano usługę rejestru zdalnego.

Uwaga

Narzędzie ServerProtect Normal Server Migration nie dezinstaluje agenta Control Manager™ serwera ServerProtect. Instrukcje na temat dezinstalacji agenta znajdują się w dokumentacji serwera ServerProtect i/lub programu Control Manager.

Używanie narzędzia ServerProtect Normal Server Migration

Procedura

1. Na komputerze serwera OfficeScan otwórz lokalizację <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\SPNSXfr`, a następnie skopiuj pliki `SPNSXfr.exe` i `SPNSX.ini` do lokalizacji <`Folder instalacji serwera`>`\PCCSRV\Admin`.

2. Dwukrotnie kliknij plik `SPNSXfr.exe`, aby otworzyć narzędzie.

   Zostanie otwarta konsola **ServerProtect Normal Server Migration Tool**.

3. Wybierz serwer OfficeScan. W odpowiednim obszarze zostanie wyświetlona ścieżka serwera OfficeScan. Jeśli ścieżka ta nie jest poprawna, kliknij przycisk **Browse** i wybierz folder`PCCSRV` z katalogu, w którym zainstalowano program OfficeScan. Aby umożliwić automatyczne wyszukanie serwera OfficeScan przy kolejnym uruchomieniu narzędzia, zaznacz pole wyboru **Automatycznie wyszukaj ścieżkę serwera** (domyślnie zaznaczone).

4. Wybierz komputery z zainstalowanym serwerem ServerProtect Normal Server, na których przeprowadzona zostanie migracja, klikając jedną z następujących pozycji w obszarze **Docelowy punkt końcowy**:

   - **Drzewo sieci Windows**: wyświetla drzewo z domenami obecnymi w sieci. Aby wybrać komputery w ten sposób, należy kliknąć domeny, w których będą wyszukiwane komputery agentów.

- **Nazwa serwera Information Server**: wyszukiwanie według nazwy serwera Information Server. Aby wybrać komputery w ten sposób, należy wpisać nazwę serwera Information Server sieci w polu tekstowym. Aby wyszukać wiele serwerów Information Server, oddziel ich nazwy średnikiem „;”.
- **Nazwa serwera Normal Server**: wyszukiwanie według nazwy serwera Normal Server. Aby wybrać komputery w ten sposób, należy wpisać nazwę serwera Normal Server sieci w polu tekstowym. Aby wyszukać wiele serwerów Normal Server, oddziel ich nazwy średnikiem „;”.
- **Przeszukiwanie zakresu adresów IP**: wyszukiwanie według zakresu adresów IP. Aby wybrać komputery w ten sposób, wpisz zakres adresów IP klasy B w obszarze zakres IP.

Uwaga

Jeśli serwer DNS w sieci nie odpowiada podczas wyszukiwania agentów, wyszukiwanie zostanie zawieszone. Należy poczekać, aż minie limit czasu wyszukiwania.

5. Należy wybrać opcję **Ponowne uruchamianie po instalacji**, aby automatycznie ponownie uruchomić komputery docelowe po migracji.

   Ponowne uruchomienie jest wymagane, aby pomyślnie zakończyć migrację. Jeśli ta opcja nie zostanie wybrana, komputery po migracji należy uruchomić ręczne.

6. Kliknij przycisk **Wyszukaj**.

   Wyniki wyszukiwania zostaną wyświetlone w obszarze **Serwery ServerProtect Normal Server**.

7. Kliknij komputery, na których ma być wykonana migracja.

   a. Aby wybrać wszystkie komputery, kliknij pozycję **Wybierz wszystko**.

   b. Aby anulować wybór wszystkich komputerów, kliknij opcję **Usuń zaznaczenie wszystkich**.

   c. Aby wyeksportować dziennik do pliku rozdzielanego przecinkami (CSV), kliknij opcję **Eksport do CSV**.

8. Jeśli do zalogowania na komputerach docelowych jest wymagana nazwa użytkownika i hasło, wykonaj następujące czynności:

a. Zaznacz pole wyboru **Użyj konta/hasła grupy**.

b. Kliknij pozycję **Ustaw konto logowania**.

Zostanie wyświetlone okno Wprowadź dane administratora.

c. Wpisz nazwę użytkownika i hasło.

Uwaga

Aby zalogować się na docelowym punkcie końcowym, należy skorzystać z konta administratora lokalnego lub konta administratora domeny. Użytkownik zalogowany z niewystarczającymi uprawnieniami, takimi jak: „Gość" lub „Normalny użytkownik", nie będzie mógł przeprowadzić instalacji.

d. Kliknij przycisk **OK**.

e. Jeśli nie można się zalogować, kliknij pozycję **Zapytaj ponownie po nieudanym logowaniu**, aby ponownie wpisać nazwę i hasło użytkownika podczas procesu migracji.

9. Kliknij pozycję **Migruj**.

10. Jeśli nie zaznaczono opcji **Ponowne uruchamianie po instalacji**, po zakończeniu migracji należy ponownie uruchomić komputery docelowe.

Po instalacji

Po zakończeniu instalacji należy sprawdzić:

- *Skróty agenta OfficeScan na stronie 5-77*
- *Lista programów na stronie 5-77*
- *Usługi agenta OfficeScan na stronie 5-77*
- *Dzienniki instalacji agenta OfficeScan na stronie 5-78*

Skróty agenta OfficeScan

Skróty programu Agent OfficeScan są dostępne w menu Start systemu Windows na punkcie końcowym agenta.

ILUSTRACJA 5-2. Skróty agenta OfficeScan

Uwaga

Niedostępne na platformach Windows 8/8.1/10 ani Windows Server 2012/2012 R2/2016.

Lista programów

Agent Trend Micro OfficeScan Dodaj/Usuń programy w Panelu sterowania na punkcie końcowym agenta.

Usługi agenta OfficeScan

W konsoli **Microsoft Management Console** są wyświetlane następujące usługi agenta OfficeScan:

- OfficeScan NT Listener (`TmListen.exe`)
- OfficeScan NT RealTime Scan (`NTRtScan.exe`)
- Usługa proxy OfficeScan NT (`TmProxy.exe`)

Uwaga

Usługa proxy OfficeScan NT nie istnieje na platformach Windows 7/8/8.1/10 i Windows Server 2008 R2/2012/2016.

- Zapora OfficeScan NT (`TmPfw.exe`), jeżeli podczas instalacji została włączona opcja zapory
- Usługa zapobiegania nieautoryzowanym zmianom firmy Trend Micro (`TMBMSRV.exe`)
- Ogólne środowisko rozwiązania klienta Trend Micro (`TmCCSF.exe`)

Dzienniki instalacji agenta OfficeScan

Dziennik instalacji agenta OfficeScan (plik `OFCNT.LOG`) występuje w następujących lokalizacjach:

- `%windir%` w przypadku wszystkich metod instalacji z wyjątkiem instalacji za pomocą pakietu MSI
- `%temp%` (dla metody instalacji przy użyciu pakietu MSI)

Czynności zalecane do wykonania po instalacji

Firma Trend Micro zaleca wykonanie poniższych czynności wykonywanych po zainstalowaniu.

Aktualizacje składników

Aby zapewnić agentom najbardziej aktualną ochronę przed zagrożeniami bezpieczeństwa, należy aktualizować składniki agenta OfficeScan. Można wykonać ręczną aktualizację agentów z poziomu konsoli Web lub poinstruować użytkowników, aby uruchomili funkcję „Aktualizuj teraz” na swoich komputerach.

Testowanie programu OfficeScan za pomocą skryptu testowego EICAR

Europejski instytut badań nad ochroną antywirusową komputerów (EICAR, European Institute for Computer Antivirus Research) opracował skrypt testowy będący bezpieczną metodą sprawdzania prawidłowości instalacji i konfiguracji programów antywirusowych. Więcej informacji można znaleźć w witrynie internetowej organizacji EICAR:

http://www.eicar.org

Skrypt testowy EICAR jest plikiem tekstowym z rozszerzeniem `.com`. Plik ten nie jest wirusem i nie zawiera fragmentów kodu wirusów, jednak większość programów antywirusowych potraktuje go jako wirusa. Można za jego pomocą zasymulować zarażenie wirusem i sprawdzić, czy funkcje powiadamiania pocztą e-mail i dzienników wirusów działają prawidłowo.

OSTRZEŻENIE!

Do testowania instalacji produktu antywirusowego nigdy nie wolno używać prawdziwych wirusów.

Wykonywanie skanowania testowego

Procedura

1. Włącz funkcję Skanowanie w czasie rzeczywistym na agencie.
2. Skopiuj następujący ciąg znaków i wklej do pliku utworzonego w Notatniku lub innym edytorze zwykłego tekstu: `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
3. Plik ten należy zapisać jako `EICAR.com` w katalogu temp. Program OfficeScan natychmiast wykryje plik.
4. Aby przetestować inne komputery w sieci, plik EICAR.com należy dołączyć do wiadomości e-mail i wysłać ją na inne komputery.

Porada

Firma Trend Micro zaleca spakowanie pliku EICAR za pomocą oprogramowania kompresującego (takiego jak WinZip), a następnie przeprowadzenie kolejnego skanowania testowego.

Dezinstalacja dodatku

Istnieją dwa sposoby dezinstalacji agenta OfficeScan z komputerów:

- *Dezinstalacja agenta OfficeScan z poziomu konsoli Web na stronie 5-80*
- *Uruchamianie programu dezinstalacyjnego agenta OfficeScan na stronie 5-82*

Jeśli agenta OfficeScan nie można odinstalować za pomocą wymienionych wyżej metod, dezinstalację należy przeprowadzić ręcznie. Szczegółowe informacje zawiera sekcja *Ręczne odinstalowywanie agenta OfficeScan na stronie 5-82*.

Dezinstalacja agenta OfficeScan z poziomu konsoli Web

Program agenta OfficeScan można odinstalować z poziomu konsoli Web. Dezinstalację należy przeprowadzać tylko w przypadku występowania problemów z działaniem programu. Po dezinstalacji należy natychmiast ponownie zainstalować agenta, aby zabezpieczyć punkt końcowy przed zagrożeniami bezpieczeństwa.

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij kolejno pozycje **Zadania** > **Dezinstalacja agenta**.
4. Na ekranie **Dezinstalacja agenta** kliknij polecenie **Rozpocznij dezinstalację**. Serwer wyśle powiadomienie do agentów.
5. Sprawdź stan powiadomienia oraz czy powiadomienia dotarły do wszystkich agentów.
    a. Kliknij pozycję **Wybierz niepowiadomione punkty końcowe**, a następnie kliknij pozycję **Rozpocznij dezinstalację**, aby natychmiast wysłać ponownie powiadomienie do agentów, którzy nie zostali powiadomieni.

b. Kliknij polecenie **Zatrzymaj dezinstalację**, aby program OfficeScan przerwał działanie bieżącej operacji powiadamiania agentów. Powiadomieni oraz już przeprowadzający dezinstalację agenci zignorują to polecenie.

Program dezinstalacyjny agenta OfficeScan

Należy przyznać użytkownikom uprawnienia do dezinstalacji programu agenta OfficeScan, a następnie polecić im, aby uruchomili na swoich komputerach program dezinstalacyjny agenta.

W zależności od konfiguracji, dezinstalacja może wymagać hasła lub nie. Jeśli hasło jest wymagane, należy się upewnić, że to hasło jest znane tylko użytkownikom, którzy mogą uruchamiać program dezinstalacyjny. W przypadku ujawnienia hasła innym osobom należy je natychmiast zmienić.

Przyznawanie uprawnienia do odinstalowywania agenta OfficeScan

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Na karcie **Uprawnienia** przejdź do sekcji **Dezinstalacja**.
5. Aby umożliwić dezinstalację bez użycia hasła, wybierz opcję **Pozwól użytkownikowi na odinstalowanie agenta OfficeScan**. Jeśli hasło jest wymagane, wybierz opcję **Wymagaj hasła od użytkownika, aby odinstalować agenta OfficeScan**, wpisz hasło, a następnie potwierdź je.
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

- **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Uruchamianie programu dezinstalacyjnego agenta OfficeScan

Procedura

1. W menu **Start** systemu Windows kliknij kolejno polecenia **Programy** > **Agent Trend Micro OfficeScan** > **Odinstalowywanie agenta OfficeScan**.

   Można również wykonać następujące czynności:

   a. Kliknij **Panel sterowania** > **Dodaj lub usuń programy**.

   b. Znajdź element **Agent Trend Micro OfficeScan** i kliknij polecenie **Zmień**.

   c. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

2. Po wyświetleniu monitu wpisz hasło dezinstalacji. Program OfficeScan powiadomi użytkownika o postępie dezinstalacji i jej zakończeniu. Użytkownik nie musi ponownie uruchamiać punktu końcowego agenta w celu zakończenia dezinstalacji.

Ręczne odinstalowywanie agenta OfficeScan

Ręczną dezinstalację należy przeprowadzać tylko w przypadku napotkania problemów z dezinstalacją agenta OfficeScan z poziomu konsoli Web lub po uruchomieniu programu dezinstalacyjnego.

Procedura

1. Zaloguj się na punkcie końcowym agenta za pomocą konta z uprawnieniami administratora.

2. Kliknij prawym przyciskiem myszy ikonę agenta OfficeScan na pasku zadań i wybierz polecenie **Zamknij OfficeScan**. W przypadku wyświetlenia monitu o hasło, wprowadź hasło zamykania i kliknij przycisk **OK**.

   Uwaga

   - W systemach Windows 8, 8.1 lub 10 bądź Windows Server 2012 lub Windows Server 2016 należy przełączyć się w tryb pulpitu w celu zamknięcia Agent OfficeScan.
   - Na komputerach, na których Agent OfficeScan będzie zamykany, hasło należy wyłączyć. Szczegółowe informacje zawiera sekcja *Konfigurowanie uprawnień agenta i innych ustawień na stronie 15-96*.

3. Jeśli hasło zamykania nie zostało ustalone, następujące usługi należy zatrzymać z poziomu konsoli Microsoft Management Console:

   - Odbiornik OfficeScan NT
   - OfficeScan NT Firewall
   - Usługa Skanowanie w czasie rzeczywistym OfficeScan NT
   - Usługa proxy OfficeScan NT

     Uwaga

     Usługa proxy OfficeScan NT nie istnieje na platformach Windows 7, 8, 8.1 i 10 oraz Windows Server 2008R2, 2012 i 2016.

   - Usługa zapobiegania nieautoryzowanym zmianom firmy Trend Micro
   - Ogólne środowisko rozwiązania klienta Trend Micro

4. Usuń skrót agenta OfficeScan z menu Start systemu Windows.

   - W systemach Windows 8, 8.1 lub 10 bądź Windows Server 2012 lub Windows Server 2016:

a. Przełącz się w tryb pulpitu.

b. Umieść kursor myszy w prawym dolnym rogu ekranu i kliknij pozycję **Start** w wyświetlonym menu.

Zostanie wyświetlony **ekran początkowy**.

c. Kliknij prawym przyciskiem myszy pozycję **Trend Micro OfficeScan**.

d. Kliknij polecenie **Odepnij od menu Start**.

- Na wszystkich innych platformach Windows:

Kliknij **Start** > **Programy**, kliknij prawym przyciskiem myszy pozycję **Agent Trend Micro OfficeScan** i kliknij polecenie **Usuń**.

5. Otwórz Edytor rejestru (`regedit.exe`).

OSTRZEŻENIE!

Do wykonania kolejnych czynności jest wymagane usunięcie kluczy rejestru. Wprowadzenie nieprawidłowych zmian w rejestrze może spowodować wystąpienie poważnych problemów. Przed wprowadzeniem jakichkolwiek zmian w rejestrze należy zawsze wykonać kopię zapasową. Więcej informacji zawiera Pomoc Edytora rejestru.

6. Usuń następujące klucze rejestru:

- Jeśli na punkcie końcowym nie są zainstalowane inne produkty firmy Trend Micro:
  - Na komputerach 32-bitowych:

    `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

  - Na komputerach 64-bitowych:

    `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

    `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro`

- Jeśli na punkcie końcowym są zainstalowane inne produkty firmy Trend Micro, należy usunąć tylko następujące klucze:

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfcWatchDog

  Na komputerach 64-bitowych:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfcWatchDog

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp

  Na komputerach 64-bitowych:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\PC-cillinNTCorp

7. Usuń następujące klucze/wartości rejestru:
   - W systemach 32-bitowych:
     - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OfficeScanNT
     - Monitor OfficeScanNT (REG_SZ) w kluczu HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
   - W systemach 64-bitowych:
     - HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\OfficeScanNT
     - Monitor OfficeScanNT (REG_SZ) w kluczu HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\Run
8. Usuń wszystkie wystąpienia następujących kluczy rejestru we wskazanych lokalizacjach:
   - Lokalizacje:
     - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
     - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services

- `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services`
- `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services`

- Klucze:
  - NTRtScan
  - tmccsf
  - tmcfw
  - tmcomm
  - TmFilter
  - TmListen
  - tmpfw
  - TmPreFilter
  - TmProxy

    Uwaga

    Usługa TmProxy nie istnieje na platformach Windows 7/8/8.1/10 i Windows Server 2008 R2/2012/2016.

  - tmtdi

    Uwaga

    Usługa tmtdi nie istnieje na platformach Windows 7/8/8.1/10 lub Windows Server 2012/2016.

  - VSApiNt
  - tmlwf (komputery z systemem operacyjnym Windows Vista/Server 2008/7/8/8.1/10/Server 2012/2016)
  - tmwfp (komputery z systemem operacyjnym Windows Vista/Server 2008/7/8/8.1/10/Server 2012/2016)

- tmactmon
- TMBMServer
- TMebc
- tmevtmgr
- tmeevw (komputery z systemem operacyjnym Windows 7/8/8.1/10/ Server 2008 R2/Server 2012)
- tmusa (komputery z systemem operacyjnym Windows 7/8/8.1/10/ Server 2008 R2/Server 2012/2016)
- tmnciesc
- tmeext (dla systemu Windows XP/2003)
- tmel (komputery z systemem operacyjnym Windows 8/8.1/10/Server 2012/2016)
- tmumh

9. Zamknij Edytor rejestru.

10. Kliknij polecenie **Początek** > **Ustawienia** > **Panel sterowania** i dwukrotnie kliknij pozycję **System**.

Uwaga

Pomiń ten krok w przypadku systemu Windows 8/8.1/10, Windows Server 2012 lub Windows Server 2016.

11. Kliknij kartę **Sprzęt**, a następnie przycisk **Menedżer urządzeń**.

Uwaga

Pomiń ten krok w przypadku systemu Windows 8/8.1/10, Windows Server 2012 lub Windows Server 2016.

12. Kliknij **Wyświetl** > **Pokaż ukryte urządzenia**.

Uwaga

Pomiń ten krok w przypadku systemu Windows 8/8.1/10, Windows Server 2012 lub Windows Server 2016.

13. Rozwiń kategorię **Sterowniki niezgodne z Plug and Play**, a następnie odinstaluj następujące urządzenia (w przypadku systemu Windows XP/Vista/7/Server 2003/Server 2008):

    - tmactmon
    - tmcomm
    - TMEBC
    - tmevtmgr
    - TMUMH
    - Trend Micro Filter
    - Trend Micro PreFilter
    - Trend Micro TDI Driver
    - Trend Micro VSAPI NT
    - Usługa zapobiegania nieautoryzowanym zmianom firmy Trend Micro
    - Trend Micro WFP Callout Driver (komputery z systemem operacyjnym Windows Vista/2008/7)

14. Ręcznie usuń sterowniki firmy Trend Micro w edytorze wiersza polecenia (tylko system Windows 8/8.1/10/Server 2012) przy użyciu następujących poleceń:

    - `sc delete tmcomm`
    - `sc delete tmactmon`
    - `sc delete tmevtmgr`
    - `sc delete tmfilter`
    - `sc delete tmprefilter`

- `sc delete tmwfp`
- `sc delete vsapint`
- `sc delete tmeevw`
- `sc delete tmusa`
- `sc delete tmebc`
- `sc delete tmumh`
- `sc delete tmccsf`
- `sc delete Tmnciesc`
- `sc delete tmlwf`

Uwaga

Uruchom edytor wiersza polecenia przy użyciu uprawnień administratora (na przykład kliknij prawym przyciskiem myszy program `cmd.exe` i kliknij opcję **Uruchom jako administrator**), aby zapewnić pomyślne wykonanie poleceń.

15. Odinstaluj ogólny sterownik zapory.

a. Kliknij prawym przyciskiem myszy pozycję **Moje miejsca sieciowe**, a następnie pozycję **Właściwości**.

b. Kliknij prawym przyciskiem pozycję **Połączenie lokalne**, a następnie kliknij pozycję **Właściwości**.

c. Na karcie **Ogólne** wybierz **Ogólny sterownik zapory firmy Trend Micro** i kliknij polecenie **Odinstaluj**.

Uwaga

Poniższe czynności dotyczą wyłącznie systemów operacyjnych Windows Vista/Server 2008/7/8/8.1/10/Server 2012. Agenci używający wszystkich innych systemów operacyjnych powinni przejść do punktu 15.

d. Kliknij prawym przyciskiem myszy pozycję **Sieć** i kliknij polecenie **Właściwości**.

e. Kliknij polecenie **Zarządzaj połączeniami sieciowymi**.

f. Kliknij prawym przyciskiem pozycję **Połączenie lokalne**, a następnie kliknij pozycję **Właściwości**.

g. Na karcie **Sieć** wybierz **Trend Micro NDIS 6.0 Filter Driver** i kliknij polecenie **Odinstaluj**.

16. Uruchom ponownie punkt końcowyagenta.

17. Jeśli na komputerze nie są zainstalowane inne produkty firmy Trend Micro, usuń folder instalacji `Trend Micro` (zazwyczaj `C:\Program Files\Trend Micro`). Na komputerach 64-bitowych folder instalacji można znaleźć w lokalizacji `C:\Program Files (x86)\Trend Micro`.

18. Jeśli na komputerze są zainstalowane inne produkty firmy Trend Micro, usuń następujące foldery:

    - <*Folder instalacji agenta*>
    - Folder `BM` w folderze instalacyjnym `Trend Micro` (zwykle `C:\Program Files\Trend Micro\BM` w systemach 32-bitowych oraz `C:\Program Files (x86)\Trend Micro\BM` w systemach 64-bitowych)

Rozdział 6

Aktualizowanie ochrony

W tym rozdziale opisano składniki i procedury aktualizacji składników programu OfficeScan.

Rozdział składa się z następujących tematów:

Składniki i programy pakietu OfficeScan

Oprogramowanie OfficeScan wykorzystuje składniki i programy w celu ochrony komputerów agentów przed najnowszymi zagrożeniami bezpieczeństwa. Należy zapewnić aktualność tych składników i programów, aktualizując je ręcznie lub konfigurując harmonogram aktualizacji.

Oprócz wyżej wymienionych składników, agenciOfficeScan pobierają z serwera OfficeScan również zaktualizowane pliki konfiguracji. Agenci potrzebują plików konfiguracji, aby zastosować nowe ustawienia. Pliki konfiguracji zmieniają się po każdej modyfikacji ustawień programu OfficeScan z poziomu konsoli Web.

Składniki dzielą się na następujące grupy:

Ochrona antywirusowa

SKŁADNIK	OPIS
Silnik skanowania antywirusowego, 32-bitowe/64-bitowe	Wszystkie produkty Trend Micro są oparte na silniku skanowania, który pierwotnie powstał w reakcji na starsze wirusy rozpowszechniające się przez pliki. Dzisiejszy silnik skanowania jest niezwykle skomplikowany i potrafi wykrywać różne typy wirusów i złośliwego oprogramowania. Silnik skanowania umożliwia także wykrywanie wirusów kontrolowanych, które zostały stworzone i są wykorzystywane na potrzeby badań. Zamiast skanowania każdego bitu w każdym pliku silnik i plik sygnatur uzupełniają się w celu zidentyfikowania następujących elementów: • Cech wyróżniających kod wirusa • Precyzyjnej lokalizacji wirusa w pliku
Sygnatura wirusów	Sygnatura wirusów zawiera informacje ułatwiające Agenci OfficeScan rozpoznawanie najnowszych wirusów/złośliwego oprogramowania, a także ataków ze strony zagrożeń mieszanych. Firma Trend Micro opracowuje i rozpowszechnia nowe wersje sygnatury wirusów kilka razy w tygodniu i po każdym wykryciu wyjątkowo szkodliwego wirusa / złośliwego oprogramowania.
skanowania antywirusowego	Sterownik skanowania antywirusowego monitoruje operacje, jakie użytkownik wykonuje na plikach. Operacje te obejmują otwieranie lub zamykanie pliku oraz uruchamianie aplikacji. Dostępne są dwie wersje tego sterownika. Są to `TmXPFlt.sys` i `TmPreFlt.sys`. `Wersja TmXPFlt.sys` jest używana do konfiguracji silnika skanowania antywirusowego w czasie rzeczywistym, a wersja `TmPreFlt.sys` służy do monitorowania operacji wykonywanych przez użytkownika. **Uwaga** Ten składnik nie jest wyświetlany w konsoli. Aby sprawdzić jego wersję, należy przejść do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Pccnt\Drv`. Kliknij prawym przyciskiem myszy plik `.sys`, wybierz **Właściwości**, a następnie przejdź do karty **Wersja**.

Składnik	Opis
Sygnatury Smart Scan Sygnatura Agenta Smart Scan	W trybie skanowania Smart Scan agenci Agenci OfficeScan wykorzystują dwie niewielkie sygnatury współpracujące ze sobą w celu zapewnienia takiego samego poziomu ochrony, jak inne standardowe sygnatury ochrony przed złośliwym oprogramowaniem i oprogramowaniem spyware. **Sygnatury Smart Scan** zawiera większość definicji sygnatur. **Sygnatura Agenta Smart Scan** zawiera wszystkie inne definicje sygnatur, których nie ma w sygnaturze Smart Scan. Program Agent OfficeScan skanuje klienta pod kątem zagrożeń bezpieczeństwa, korzystając z sygnatury **Smart Scan Agent Pattern**. Agenci OfficeScan, którzy podczas skanowania nie są w stanie określić, czy plik stanowi zagrożenie, sprawdzają to, wysyłając żądanie skanowania do usługi Scan Server obsługiwanej przez serwer Serwer OfficeScan. Usługa Scan Server sprawdza zagrożenie, korzystając z **Sygnatury Smart Scan**. Agent OfficeScan umieszcza wynik żądania skanowania uzyskany od serwera skanowania w pamięci podręcznej w celu zwiększenia wydajności skanowania.
Sygnatura IntelliTrap	Sygnatura IntelliTrap służy do wykrywania plików wykonywalnych kompresowanych w czasie rzeczywistym. Szczegółowe informacje zawiera sekcja *IntelliTrap na stronie E-7*.
Sygnatura wyjątków IntelliTrap	Sygnatura wyjątków IntelliTrap zawiera listę „dozwolonych” plików skompresowanych.

Składnik	Opis
Sygnatura kontroli pamięci	Skanowanie w czasie rzeczywistym wykorzystuje sygnaturę kontroli pamięci w celu dokonania oceny wykonywalnych plików skompresowanych, które zostały zidentyfikowane przez monitorowanie zachowań. Skanowanie w czasie rzeczywistym wykonuje następujące operacje na wykonywalnych plikach skompresowanych: 1. Tworzy plik mapowania w pamięci po sprawdzeniu ścieżki obrazu procesu.  **Uwaga** Lista wykluczeń skanowania ma wyższy priorytet niż skanowanie plików. 2. Wysyła identyfikator procesu do usługi zaawansowanej ochrony, która następnie: a. Używa silnika skanowania antywirusowego do skanowania pamięci. b. Filtruje proces przy użyciu globalnych list dozwolonych elementów dla plików systemu Windows, cyfrowo podpisanych plików z wiarygodnych źródeł oraz plików przetestowanych przez firmę Trend Micro. Po potwierdzeniu bezpieczeństwa pliku program OfficeScan nie wykonuje żadnych operacji na tym pliku. 3. Po przetworzeniu skanu pamięci usługa zaawansowanej ochrony wysyła wyniki do funkcji skanowania w czasie rzeczywistym. 4. Następnie skanowanie w czasie rzeczywistym poddaje kwarantannie wszystkie wykryte zagrożenia złośliwym oprogramowaniem i zatrzymuje proces.
Silnik analizy kontekstowej (32/64 bity)	Silnik analizy kontekstowej monitoruje procesy wykonywane przez sporadycznie występujące pliki i wyodrębnia cechy zachowania, które mechanizm obsługi zapytań analizy kontekstowej wysyła do silnika przewidującego uczenia maszynowego w celu analizy.
Sygnatura analizy kontekstowej	Sygnatura analizy kontekstowej zawiera listę dozwolonych zachowań, które nie odnoszą się do żadnych znanych zagrożeń.

Składnik	Opis
Mechanizm obsługi zapytań analizy kontekstowej (32/64 bity)	Mechanizm obsługi zapytań analizy kontekstowej przetwarza zachowania zidentyfikowane przez silnik analizy kontekstowej i wysyła raport do silnika przewidującego uczenia maszynowego.
Silnik skanowania w poszukiwaniu zagrożeń zaawansowanych (32/64 bity)	Silnik skanowania w poszukiwaniu zagrożeń zaawansowanych wyodrębnia cechy sporadycznie występujących plików i wysyła informacje do silnika przewidującego uczenia maszynowego.
Wzorzec korelacji zagrożeń zaawansowanych	Wzorzec korelacji zagrożeń zaawansowanych zawiera listę cech plików, które nie odnoszą się do żadnych znanych zagrożeń.

Aktualizowanie silnika skanowania

Zapisywanie najbardziej zależnych od upływu czasu informacji o wirusach/złośliwym oprogramowaniu w sygnaturze wirusów, pozwala firmie Trend Micro minimalizować liczbę aktualizacji silnika skanowania, zapewniając aktualność ochrony. Mimo to firma Trend Micro okresowo udostępnia nowe wersje silnika skanowania. Firma Trend Micro publikuje nowe silniki w następujących okolicznościach:

- Wprowadzenie do oprogramowania nowych technologii skanowania i wykrywania
- Odkrycie nowego, potencjalnie szkodliwego wirusa/złośliwego oprogramowania, z którym silnik skanowania nie może sobie poradzić
- Ulepszenie wydajności skanowania
- Dodanie obsługi formatów plików, języków skryptów, szyfrowania i/lub formatów kompresji

Składniki anty-spyware

Składnik	Opis
Sygnatura spyware/grayware	Sygnatura oprogramowania spyware/grayware identyfikuje oprogramowanie spyware/grayware w plikach i programach, modułach pamięci, rejestrze systemu Windows i skrótach URL.
Silnik skanowania spyware/grayware (32/64-bitowe)	Silnik skanowania spyware/grayware skanuje w poszukiwaniu oprogramowania spyware/grayware i przeprowadza odpowiednie operacje skanowania.
Sygnatura aktywnego monitorowania oprogramowania spyware	Sygnatura aktywnego monitorowania oprogramowania spyware służy do skanowania w poszukiwaniu oprogramowania spyware/grayware w czasie rzeczywistym. Z tej sygnatury korzystają wyłącznie agenci skanowania standardowego. Agenci Smart Scan w przypadku skanowania w czasie rzeczywistym w poszukiwaniu oprogramowania spyware/grayware korzystają z sygnatura Agenta Smart Scan. Agenci wysyłają żądania skanowania do źródła programu Smart Protection, jeśli zagrożenia związanego z celem skanowania nie można określić podczas skanowania.

Składniki Usuwania Szkód Services

Składnik	Opis
Silnik usług Usuwania Szkód (32-bitowy/64-bitowy)	Silnik usługi Usuwania Szkód służy do wykrywania i usuwania trojanów oraz ich procesów.
Szablon usługi Usuwania Szkód	Szablon usługi Usuwania Szkód, używany w Silnik usługi Usuwania Szkód, pomaga w identyfikacji plików i procesów trojanów oraz umożliwia ich eliminację.

Składnik	Opis
Sterownik wczesnego czystego rozruchu (32/64-bitowe)	Sterownik wczesnego czystego rozruchu Trend Micro ładuje się przed sterownikami systemu operacyjnego, co umożliwia wykrywanie i blokowanie programów typu rootkit sektora rozruchowego. Po załadowaniu agenta OfficeScan sterownik wczesnego czystego rozruchu Trend Micro wywołuje Usługi Usuwania Szkód Services w celu wyczyszczenia oprogramowania typu rootkit.

Składniki zapory

Składnik	Opis
Ogólny sterownik zapory (32/64-bitowe)	Ogólny sterownik zapory jest używany razem z ogólną sygnaturą zapory i służy do skanowania punktów końcowych agent w poszukiwaniu wirusów sieciowych. Ten sterownik obsługuje platformy 32-bitowe i 64-bitowe.
Ogólna sygnatura zapory	Podobnie jak sygnatura wirusa, ogólna sygnatura zapory ułatwia agentom identyfikację sygnatury wirusów — unikatowe sygnatury bitów i bajtów, które sygnalizują obecność wirusa sieciowego.

Składniki monitorowania zachowań

Składnik	Opis
Sygnatura wykrywania funkcji Monitorowanie zachowań (32-bitowa/64-bitowa)	Ta sygnatura zawiera reguły służące do wykrywania podejrzanego zachowania.
Sterowniki głównego monitora zachowań, 32-bit/64-bit	Sterownik pracujący w trybie jądra, który służy do monitorowania zachowań systemowych i przekazuje informacje o nich do głównej usługi monitorowania zachowania w celu wymuszenia realizacji zasad.

Składnik	Opis
Główna usługa monitorowania zachowania, wersja 32-bitowa/64-bitowa	Ta pracująca w trybie użytkownika usługa zapewnia następujące funkcje: • Wykrywanie rootkitów • Sterowanie dostępem do urządzeń zewnętrznych • Ochrona plików, kluczy rejestru i usług
Sygnatura konfiguracji monitorowania zachowania	Sterownik monitorowania zachowania używa sygnatury do identyfikacji normalnych zachowań systemu i wyłączenia ich z wymuszania realizacji zasad.
Sygnatura podpisu cyfrowego	Sygnatura z listą poprawnych podpisów cyfrowych używanych przez główną usługę monitorowania zachowania w celu określenia, czy program odpowiedzialny za zdarzenie systemowe jest bezpieczny.
Sygnatura stosowania zasad	Usługa główna funkcji Monitorowanie zachowania służy do analizy zdarzeń systemowych w kontekście reguł sygnatury.
Sygnatura Memory Scan Trigger Pattern (32/64-bitowe)	Monitorowanie zachowań używa sygnatury wyzwalacza skanowania pamięci do identyfikowania potencjalnych zagrożeń po wykryciu następujących operacji: • operacja zapisu pliku, • operacja zapisu w rejestrze, • utworzenie nowego procesu. Po zidentyfikowaniu jednej z tych operacji monitorowanie zachowań wywołuje sygnaturę kontroli pamięci skanowania w czasie rzeczywistym, aby sprawdzić zagrożenia bezpieczeństwa. Szczegółowe informacje o operacjach skanowania w czasie rzeczywistym zawiera sekcja *Sygnatura kontroli pamięci na stronie 6-5*.
Sygnatura przywracania po uszkodzeniach	Sygnatura przywracania po uszkodzeniach zawiera reguły służące do monitorowania podejrzanego zachowania.

Składnik	Opis
Sygnatura monitorowania inspekcji programów	Sygnatura monitorowania inspekcji programów monitoruje i zapisuje punkty inspekcji, które służą do monitorowania zachowania.

Składniki usługi podejrzanego połączenia

Składnik	Opis
Globalna lista numerów IP C&C	Globalna lista numerów IP C&C działa w połączeniu z silnikiem kontroli treści sieciowych (NCIE) w zakresie wykrywania połączeń sieciowych ze znanymi serwerami C&C. Silnik NCIE wykrywa kontakt z serwerem C&C za pośrednictwem dowolnego kanału sieciowego. Program OfficeScan rejestruje informacje o wszystkich połączeniach z serwerami z globalnej listy adresów IP C&C na potrzeby oceny.
Sygnatura reguły istotności	Usługa wykrywania podejrzanych połączeń wykorzystuje sygnaturę reguły istotności do wykrywania unikatowych sygnatur rodziny złośliwego oprogramowania umieszczonych w nagłówkach pakietów sieciowych.

Rozwiązanie luki w zabezpieczeniach przeglądarki

Składnik	Opis
Sygnatura zapobiegania wykorzystaniu przeglądarki	Ta sygnatura rozpoznaje najnowsze przypadki wykorzystania przeglądarki i zapobiega ich użyciu zagrażającemu przeglądarce.
Ujednolicona sygnatura analizatora skryptów	Ta sygnatura analizuje skrypty w stronach internetowych i rozpoznaje złośliwe skrypty.

Programy

SKŁADNIK	OPIS
Agent OfficeScan	Pogram agenta OfficeScan zapewnia właściwą ochronę przed zagrożeniami bezpieczeństwa.
Pakiety hot fix, poprawki i dodatki Service Pack	Po oficjalnym wydaniu produktu firma Trend Micro często rozwiązuje wykryte problemy, zwiększa wydajność produktu i dodaje nowe funkcje, opracowując następujące elementy: • *Pakiet Hot Fix na stronie E-5* • *Poprawka na stronie E-10* • *Poprawka zabezpieczeń na stronie E-12* • *Dodatek Service Pack na stronie E-12* Sprzedawcy lub dostawcy mogą zawiadamiać klientów o dostępności tych elementów. Informacje na temat nowych pakietów hot fix, poprawek i dodatków Service Pack można znaleźć na stronie internetowej firmy Trend Micro: http://downloadcenter.trendmicro.com/index.php?regs=PL Wszystkie publikacje zawierają plik Readme z informacjami na temat instalacji, wdrożenia oraz konfiguracji. Przed rozpoczęciem instalacji należy uważnie przeczytać plik Readme.

Historia pakietów hot fix i poprawek

Gdy serwer OfficeScan instaluje pakiet Hot Fix lub pliki poprawki na agentach OfficeScan, program agenta OfficeScan rejestruje informacje o tym działaniu w Edytorze rejestru. Te informacje można przeszukiwać za pomocą oprogramowania logistycznego, takiego jak Microsoft SMS, LANDesk™ czy BigFix™, również w przypadku wielu agentów.

Uwaga

Ta funkcja nie rejestruje informacji o pakietach hot fix i poprawkach instalowanych wyłącznie na serwerze.

Ta funkcja jest dostępna od wersji OfficeScan 8.0 z dodatkiem Service Pack 1 i poprawką 3.1.

- Agenci uaktualnieni z wersji 8.0 z dodatkiem Service Pack 1 i poprawką 3.1 lub nowszą rejestrują informacje o instalowanych pakietach Hot Fix i poprawkach dotyczące wersji 8.0 i nowszych.
- Agenci uaktualnieni z wersji wcześniejszej niż 8.0 z dodatkiem Service Pack 1 i poprawką 3.1 rejestrują informacje o instalowanych pakietach Hot Fix i poprawkach dotyczące wersji 10.0 i nowszych.

Informacje są przechowywane w następujących kluczach rejestru:

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`
- W przypadku komputerów z procesorami typu x64:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\ PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`

Należy sprawdzić następujące klucze:

- **Klucz**: `HotFix_installed`

  Typ: `REG_SZ`

  Wartość: `<Nazwa pakietu Hot Fix lub poprawki>`

- **Klucz**: `HotfixInstalledNum`

  Typ: `DWORD`

  Wartość: `<Numer pakietu Hot Fix lub poprawki>`

Składniki Web Reputation

Składnik	Opis
Silnik filtrowania adresów URL	Silnik filtrowania adresów URL umożliwia komunikację pomiędzy programem OfficeScan i usługą filtrowania adresów URL firmy Trend Micro. Silnik filtrowania adresów URL to system, który ocenia adres URL i przekazuje informację z wydaną oceną do programu OfficeScan.

Przegląd aktualizacji

Wszystkie aktualizacje składników są odbierane z serwera Trend Micro ActiveUpdate Server. Gdy są dostępne aktualizacje, serwer OfficeScan i źródła Smart Protection (Serwer Smart Protection lub sieć Smart Protection Network) pobierają zaktualizowane składniki. Między składnikami pobieranymi za pomocą serwerów OfficeScan oraz źródeł Smart Protection nie ma konfliktów, ponieważ każdy obiekt pobiera oddzielny zestaw składników.

Uwaga

Zarówno serwer OfficeScan, jak i Serwer Smart Protection, można skonfigurować do pobierania aktualizacji ze źródeł innych niż serwer Trend Micro ActiveUpdate Server. W tym celu należy skonfigurować niestandardowe źródło aktualizacji. W przypadku konieczności uzyskania pomocy dotyczącej konfigurowania źródła aktualizacji należy się skontaktować z dostawcą obsługi technicznej.

Aktualizacja serwera OfficeScan i agenta OfficeScan

Serwer OfficeScan pobiera większość składników wymaganych przez agentów. Nie pobiera wyłącznie sygnatury Smart Scan. Jest ona pobierana przez źródła Smart Protection.

Jeśli serwer OfficeScan zarządza wieloma agentami, proces aktualizacji może wykorzystywać znaczną ilość zasobów komputera serwera, zmniejszając jego stabilność i wydajność. Aby rozwiązać ten problem, program OfficeScan zapewnia funkcję agenta

aktualizacji, która umożliwia wyznaczonym agentom rozpowszechnianie aktualizacji do innych agentów.

W poniższej tabeli wymieniono różne opcje aktualizacji składników serwera OfficeScan i jego agentów oraz zalecenia dotyczące ich stosowania:

TABELA 6-1. Opcje aktualizacji serwer-Agent

OPCJA AKTUALIZACJI	OPIS	ZALECENIE
Serwer ActiveUpdate > **Serwer** > **Agent**	Serwer OfficeScan pobiera zaktualizowane składniki z serwera Trend Micro ActiveUpdate (lub innego źródła aktualizacji) i rozpoczyna aktualizację składników na agentach.	Metody tej należy użyć, jeżeli między serwerem OfficeScan a agentami nie znajdują się segmenty sieci o niskiej przepustowości.
Serwer ActiveUpdate > **Serwer** > **Agenci aktualizacji** > **Agent**	Serwer OfficeScan pobiera zaktualizowane składniki z serwera ActiveUpdate (lub innego źródła aktualizacji) i rozpoczyna aktualizację składników na agentach. Agenci funkcjonujący jako agenci aktualizacji powiadamiają następnie agentów o konieczności zaktualizowania składników.	Jeśli między serwerem OfficeScan a agentami występują segmenty sieci o niskiej przepustowości, należy zastosować tę metodę w celu zrównoważenia obciążenia w sieci.
Serwer ActiveUpdate > **Update Agents** > **Agent**	Agenci aktualizacji otrzymują zaktualizowane składniki bezpośrednio z serwera ActiveUpdate (lub innego źródła aktualizacji) i powiadamiają agentów o konieczności zaktualizowania składników.	Metody tej należy używać tylko w przypadku wystąpienia problemów z aktualizacją agentów aktualizacji z serwera OfficeScan lub z innych agentów. W większości przypadków pobieranie przez Agentów aktualizacji z serwera OfficeScan lub z innych Agentów aktualizacji jest szybsze niż pobieranie z zewnętrznego źródła.

Opcja aktualizacji	Opis	Zalecenie
Serwer ActiveUpdate > **Agent**	Agenci OfficeScan otrzymują zaktualizowane składniki bezpośrednio z serwera ActiveUpdate (lub innego źródła aktualizacji).	Metody tej należy używać tylko w przypadku wystąpienia problemów z aktualizacją agentów z serwera OfficeScan lub agentów aktualizacji. W większości wypadków pobieranie przez agentów aktualizacji z serwera OfficeScan lub agentów aktualizacji jest szybsze niż pobieranie z zewnętrznego źródła.

Aktualizacja źródła Smart Protection

Źródło Smart Protection (Serwer Smart Protection lub sieć Smart Protection Network) pobiera sygnatury Smart Scan. Agenci Smart Scan nie pobierają tej sygnatury. Weryfikują oni potencjalne zagrożenia względem sygnatur, wysyłając żądania skanowania do źródła programu Smart Protection.

Uwaga

Więcej informacji o źródłach Smart Protection zawiera temat *Źródła Smart Protection na stronie 4-6*.

W poniższej tabeli znajduje się opis procesu aktualizacji dotyczący źródeł Smart Protection.

Tabela 6-2. Proces aktualizacji źródła Smart Protection

Proces aktualizacji	Opis
Serwer ActiveUpdate > **Smart Protection Network**	Serwer Trend Micro Smart Protection Network pobiera aktualizacje z serwera Trend Micro ActiveUpdate Server. Agenci Smart Scan, którzy nie są podłączeni do sieci firmowej, wysyłają żądania do serwera Trend Micro Smart Protection Network.

Proces aktualizacji	Opis
Serwer ActiveUpdate > **Serwer Smart Protection**	Serwer Smart Protection (zintegrowany lub samodzielny) odbiera aktualizacje z serwera Trend Micro ActiveUpdate Server. Agenci Smart Protection, którzy są podłączeni do sieci firmowej, wysyłają żądania do serwera Smart Protection.
Smart Protection Network > **Serwer Smart Protection**	Serwer Smart Protection (zintegrowany lub samodzielny) pobiera aktualizacje z serwera Trend Micro Smart Protection Network. Agenci Smart Protection, którzy są podłączeni do sieci firmowej, wysyłają żądania do serwera Smart Protection.

Aktualizacje serwera OfficeScan

Serwer OfficeScan pobiera następujące składniki i instaluje je na agentach:

Tabela 6-3. Składniki pobierane przez serwer OfficeScan

Składnik	Dystrybucja	
	Agenci skanowania standardowego	Agenci Smart Scan
Antywirus		
Sygnatura Agenta Smart Scan	Nie	Tak
Sygnatura wirusów	Tak	Nie
Sygnatura IntelliTrap	Tak	Tak
Sygnatura wyjątków IntelliTrap	Tak	Tak
Silnik skanowania antywirusowego, 32-bitowe/64-bitowe	Tak	Tak
Sygnatura kontroli pamięci	Tak	Tak

Składnik	Dystrybucja	
	Agenci skanowania standardowego	Agenci Smart Scan
Sygnatura wczesnego uruchamiania ochrony przed złośliwym oprogramowaniem (32/64-bitowe)	Tak	Tak
Silnik analizy kontekstowej (32/64 bity)	Tak	Tak
Sygnatura analizy kontekstowej	Tak	Tak
Mechanizm obsługi zapytań analizy kontekstowej (32/64 bity)	Tak	Tak
Silnik skanowania w poszukiwaniu zagrożeń zaawansowanych (32/64 bity)	Tak	Tak
Wzorzec korelacji zagrożeń zaawansowanych	Tak	Tak
Oprogramowanie anty-spyware		
Sygnatura spyware/grayware	Tak	Tak
Sygnatura aktywnego monitorowania oprogramowania spyware	Tak	Nie
Silnik skanowania spyware/grayware (32/64-bitowe)	Tak	Tak
Usługi Usuwania Szkód Services		
Szablon usługi Usuwania Szkód	Tak	Tak
Silnik usług Usuwania Szkód (32-bitowy/64-bitowy)	Tak	Tak
Sterownik wczesnego czystego rozruchu (32/64-bitowe)	Tak	Tak
Zapora		

Składnik	Dystrybucja	
	Agenci skanowania standardowego	Agenci Smart Scan
Ogólna sygnatura zapory	Tak	Tak
Składniki monitorowania zachowań		
Sygnatura wykrywania funkcji Monitorowanie zachowań (32-bitowa/64-bitowa)	Tak	Tak
Sterowniki głównego monitora zachowań, 32-bit/64-bit	Tak	Tak
Główna usługa monitorowania zachowania, wersja 32-bitowa/64-bitowa	Tak	Tak
Sygnatura konfiguracji monitorowania zachowania	Tak	Tak
Sygnatura stosowania zasad	Tak	Tak
Sygnatura podpisu cyfrowego	Tak	Tak
Sygnatura Memory Scan Trigger Pattern (32/64-bitowe)	Tak	Tak
Sygnatura monitorowania inspekcji programów	Tak	Tak
Sygnatura przywracania po uszkodzeniach	Tak	Tak
Podejrzane połączenia		
Globalna lista numerów IP C&C	Tak	Tak
Sygnatura reguły istotności	Tak	Tak
Rozwiązanie luki w zabezpieczeniach przeglądarki		

Składnik	Dystrybucja	
	Agenci skanowania standardowego	Agenci Smart Scan
Sygnatura zapobiegania wykorzystaniu przeglądarki	Tak	Tak
Ujednolicona sygnatura analizatora skryptów	Tak	Tak

Przypomnienia i wskazówki dotyczące aktualizacji:

- Aby umożliwić serwerowi instalowanie zaktualizowanych składników na agentach, należy włączyć automatyczną aktualizację agentów. Szczegółowe informacje zawiera sekcja *Aktualizacja automatyczna agentów OfficeScan na stronie 6-40*. Jeśli automatyczne aktualizacje agentów są wyłączone, serwer pobiera aktualizacje, ale nie instaluje ich na agentach.

- Serwer OfficeScan wykorzystujący wyłącznie protokół IPv6 nie umożliwia rozsyłania aktualizacji bezpośrednio do agentów wykorzystujących wyłącznie protokół IPv4. Analogicznie, serwer OfficeScan wykorzystujący wyłącznie protokół IPv4 nie umożliwia rozsyłania aktualizacji bezpośrednio do agentów wykorzystujących wyłącznie protokół IPv6. Aby umożliwić serwerowi OfficeScan rozsyłanie aktualizacji do agentów, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.

- Firma Trend Micro regularnie publikuje nowe wersje plików sygnatur, aby zapewnić agentom stałą ochronę. Ponieważ aktualizacje pliku sygnatur są udostępniane regularnie, program OfficeScan używa mechanizmu zwanego "duplikowaniem składników". Ten mechanizm umożliwia szybsze pobieranie plików sygnatur. Patrz *Duplikacja składników serwera OfficeScan na stronie 6-22* Aby uzyskać więcej informacji.

- Jeśli do łączenia z Internetem jest używany serwer proxy, podczas pobierania aktualizacji należy korzystać z prawidłowych ustawień serwera proxy.

- Na ekranie Pulpit konsoli Web dodaj widget **Aktualizacje agenta**, aby wyświetlić bieżące wersje składników oraz sprawdzić liczbę agentów z aktualnymi i nieaktualnymi składnikami.

Źródła aktualizacji serwera OfficeScan

Serwer OfficeScan można skonfigurować tak, aby składniki były pobierane z serwera Trend Micro ActiveUpdate Server lub z innego źródła. Można określić inne źródło, jeśli serwer OfficeScan nie może osiągnąć bezpośrednio serwera ActiveUpdate. Przykładowy scenariusz zawiera temat *Aktualizacje izolowanego serwera OfficeScan na stronie 6-25*.

Serwer może po pobraniu dostępnych aktualizacji automatycznie powiadamiać agentów o konieczności zaktualizowania ich składników w oparciu o ustawienia określone w pozycji **Aktualizacje** > **Agenci** > **Aktualizacja automatyczna**. Jeśli aktualizacja składników jest krytyczna, należy zezwolić serwerowi na natychmiastowe powiadomienie agentów, przechodząc do pozycji **Aktualizacje** > **Agenci** > **Aktualizacja ręczna**.

Uwaga

Jeśli nie został określony harmonogram instalacji lub ustawienia aktualizacji wywołanej zdarzeniem w pozycji **Aktualizacje** > **Agenci** > **Aktualizacja automatyczna**, serwer pobierze aktualizacje, ale nie powiadomi agentów o konieczności aktualizacji.

Obsługa protokołu IPv6 dla aktualizacji serwera OfficeScan

Serwer OfficeScan wykorzystujący wyłącznie protokół IPv6 nie może wykonywać aktualizacji bezpośrednio ze źródeł wykorzystujących wyłącznie protokół IPv4, takich jak:

- Trend Micro ActiveUpdate Server
- Dowolne niestandardowe źródło aktualizacji wykorzystujące wyłącznie protokół IPv4

Analogicznie, serwer OfficeScan wykorzystujący wyłącznie protokół IPv4 nie może wykonywać aktualizacji bezpośrednio ze źródeł aktualizacji wykorzystujących wyłącznie protokół IPv6.

Aby umożliwić serwerowi nawiązanie połączenia ze źródłami aktualizacji, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.

Serwer proxy do aktualizacji serwera OfficeScan

Można skonfigurować programy serwera tak, aby pobierając aktualizacje z serwera Trend Micro ActiveUpdate Server, korzystały z ustawień serwera proxy. Programy serwera dotyczą serwera OfficeScan oraz zintegrowanego serwera Smart Protection.

Konfigurowanie ustawień proxy

Procedura

1. Przejdź do opcji **Administracja** > **Ustawienia** > **Serwer proxy**.
2. Kliknij kartę **Zewnętrzny serwer proxy**.
3. Przejdź do sekcji **Aktualizacje serwera OfficeScan**.
4. Wybierz opcję **Użyj serwera proxy do pobierania aktualizacji sygnatur, silników i licencji**.
5. Określ protokół serwera proxy, nazwę serwera lub adres IPv4/IPv6 i numer portu.
6. Jeżeli serwer proxy wymaga uwierzytelniania, wpisz nazwę użytkownika i hasło.
7. Kliknij przycisk **Zapisz**.

Konfigurowanie źródła aktualizacji serwera

Procedura

1. Przejdź do opcji **Aktualizacje** > **Serwer** > **Źródło aktualizacji**.
2. Wybierz lokalizację, z której mają być pobierane aktualizacje składników.

   W przypadku wybrania serwera ActiveUpdate należy się upewnić, że serwer ma dostęp do Internetu oraz, jeśli jest używany serwer proxy, sprawdzić, czy połączenie z Internetem można nawiązać za pomocą obecnych ustawień proxy. Szczegółowe informacje zawiera sekcja *Serwer proxy do aktualizacji serwera OfficeScan na stronie 6-21*.

W przypadku wybrania niestandardowego źródła aktualizacji należy skonfigurować odpowiednie środowisko i zaktualizować zasoby dotyczące wybranego źródła aktualizacji. Należy się również upewnić, że połączenie między serwerem a źródłem aktualizacji działa prawidłowo. W przypadku konieczności uzyskania pomocy dotyczącej konfigurowania źródła aktualizacji należy się skontaktować z dostawcą obsługi technicznej.

Uwaga

Podczas pobierania składników ze źródła aktualizacji serwer OfficeScan korzysta z funkcji duplikacji składników. Szczegółowe informacje można znaleźć w części *Duplikacja składników serwera OfficeScan na stronie 6-22*.

3. Kliknij przycisk **Zapisz**.

Duplikacja składników serwera OfficeScan

Kiedy najnowsza wersja kompletnego pliku sygnatur jest dostępna do pobrania z serwera ActiveUpdate firmy Trend Micro, dostępnych jest również 14 przyrostowych plików sygnatur. Przyrostowe wzorce sygnatur są mniejszymi wersjami pliku kompletnego wzorca sygnatur, które odpowiadają różnicy między najnowszą i wcześniejszą wersją pliku kompletnego wzorca sygnatur. Na przykład, jeśli najnowsza wersja to 175, przyrostowy wzorzec sygnatur v_173.175 zawiera sygnatury z wersji 175, które nie występują w wersji 173 (wersja 173 jest poprzednią wersją kompletnego wzorca sygnatur, jako że numery wzorców sygnatur są zwiększane o 2). Przyrostowy wzorzec sygnatur v_171.175 zawiera sygnatury z wersji 175, które nie występują w wersji 171.

Aby zmniejszyć ruch w sieci tworzony podczas pobierania najnowszego wzorca sygnatur, program OfficeScan przeprowadza duplikację składników, czyli stosuje metodę aktualizacji składników, w której serwer OfficeScan lub agent aktualizacji pobiera jedynie przyrostowe wzorce sygnatur. W *Duplikacja składnika agenta aktualizacji na stronie 6-64* można znaleźć więcej informacji na temat sposobów powielania składników przez agentów aktualizacji.

Procedura duplikacji dotyczy następujących składników:

- Sygnatura wirusów

- Sygnatura Agenta Smart Scan
- Szablon usługi Usuwania Szkód
- Sygnatura wyjątków IntelliTrap
- Sygnatura spyware/grayware
- Sygnatura aktywnego monitorowania oprogramowania spyware

Scenariusz duplikacji składników

Proces duplikacji składników serwera objaśniono za pomocą następującego scenariusza:

TABELA 6-4. Scenariusz duplikacji składników serwera

Kompletne wzorce sygnatur na serwerze OfficeScan	Bieżąca wersja: 171 Inne dostępne wersje: 169	167	165	161	159	
Najnowsza wersja na serwerze ActiveUpdate	173.175	171.175	169.175	167.175	165.175	163.175
	161.175	159.175	157.175	155.175	153.175	151.175
	149.175	147.175				

1. Serwer OfficeScan porównuje swoją bieżącą kompletną wersję wzorca sygnatur z najnowszą wersją na serwerze ActiveUpdate. Jeśli różnica między obiema wersjami wynosi 14 lub mniej, serwer pobiera jedynie przyrostowy wzorzec sygnatur, który odpowiada różnicy między obiema wersjami.

   Uwaga

   Jeśli różnica jest większa niż 14, serwer automatycznie pobiera pełną wersję pliku sygnatur i 14 przyrostowych wzorców sygnatur.

   Na przykład:

   - Różnica między wersjami 171 i 175 wynosi 2. Innymi słowy, serwer nie ma wersji 173 i 175.

- Serwer pobiera przyrostowy wzorzec sygnatur 171.175. Ten przyrostowy wzorzec sygnatur odpowiada różnicy między wersjami 171 i 175.

2. Serwer scala przyrostowy wzorzec sygnatur ze swoim bieżącym kompletnym wzorcem sygnatur, aby utworzyć najnowszy kompletny wzorzec sygnatur.

   Na przykład:

   - Na serwerze program OfficeScan scala wersję 171 z przyrostowym wzorcem sygnatur 171.175, aby utworzyć wersję 175.
   - Serwer ma 1 przyrostowy wzorzec sygnatur (171.175) i najnowszy kompletny wzorzec sygnatur (w wersji 175).

3. Serwer tworzy przyrostowe wzorce sygnatur w oparciu o inne kompletne wzorce sygnatur dostępne na serwerze. Jeśli serwer nie tworzy tych przyrostowych wzorców sygnatur, agenci, którzy pominęli pobieranie wcześniejszych przyrostowych sygnatur, automatycznie pobierają pełny plik sygnatur, co powoduje większy ruch w sieci.

   Na przykład:

   - Ponieważ serwer ma wersje wzorca sygnatur 169, 167, 165, 163, 161, 159, może utworzyć następujące przyrostowe wzorce sygnatur:

     169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - Serwer nie musi używać wersji 171, ponieważ ma już przyrostowy wzorzec sygnatur 171.175.
   - Serwer ma teraz 7 przyrostowych wzorców sygnatur:

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - Serwer przechowuje 7 ostatnich wersji kompletnych wzorców sygnatur (wersje 175, 171, 169, 167, 165, 163, 161). Serwer usuwa wszystkie starsze wersje (wersję 159).

4. Serwer porównuje swoje bieżące przyrostowe wzorce sygnatur z przyrostowymi wzorcami sygnatur dostępnymi na serwerze ActiveUpdate. Serwer pobiera przyrostowe wzorce sygnatur, którymi nie dysponuje.

   Na przykład:

- Serwer ActiveUpdate ma 14 przyrostowych wzorców sygnatur:

  173.175, 171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

- Serwer OfficeScan ma 7 przyrostowych wzorców sygnatur:

  171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

- Serwer OfficeScan pobiera dodatkowe 7 przyrostowych wzorców sygnatur:

  173.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

- Serwer ma teraz wszystkie przyrostowe wzorce sygnatur dostępne na serwerze ActiveUpdate.

5. Najnowszy kompletny wzorzec sygnatur i 14 przyrostowych wzorców sygnatur zostają udostępnione agentom.

Aktualizacje izolowanego serwera OfficeScan

Jeśli serwer OfficeScan należy do sieci, która jest całkowicie odizolowana od wszystkich źródeł zewnętrznych, można zachować aktualność składników serwera poprzez umożliwienie aktualizacji ze źródła wewnętrznego, które zawiera najnowsze składniki.

W tym temacie przedstawiono zadania, które należy wykonać w celu aktualizacji izolowanego serwera OfficeScan.

Aktualizowanie izolowanego serwera OfficeScan

Ta procedura została przedstawiona w celach referencyjnych. Jeśli możliwe jest wykonanie wszystkich zadań w tej procedurze, należy poprosić dostawcę pomocy technicznej o szczegółowe kroki dla poszczególnych zadań.

Procedura

1. Zidentyfikuj źródło aktualizacji, takie jak program Trend Micro Control Manager lub dowolny host. Źródło aktualizacji musi zapewniać następujące elementy:

- Niezawodne połączenie internetowe, dzięki czemu można pobierać najnowsze składniki z serwera Trend Micro ActiveUpdate Server. W przypadku braku połączenia internetowym jedynym sposobem zapewnienie najnowszych składników dla źródła aktualizacji będzie samodzielne uzyskanie składników z firmy Trend Micro, a następnie skopiowanie ich do źródła aktualizacji.
- Działające połączenie z serwerem OfficeScan. Jeżeli między serwerem OfficeScan a źródłem aktualizacji znajduje się serwer proxy, należy skonfigurować jego ustawienia. Szczegółowe informacje zawiera sekcja *Serwer proxy do aktualizacji serwera OfficeScan na stronie 6-21*.
- Wystarczająca ilość miejsca na dysku na pobrane składniki.

2. Skieruj serwer OfficeScan do nowego źródła aktualizacji. Szczegółowe informacje zawiera sekcja *Źródła aktualizacji serwera OfficeScan na stronie 6-20*.
3. Zidentyfikuj składniki instalowane przez serwer na agentach. Listę składników, które można zainstalować, zawiera temat *Aktualizacje agenta OfficeScan na stronie 6-29*.

Porada

Jednym ze sposobów określenia, czy składnik jest instalowany na agentach, jest wyświetlenie ekranu **Podsumowanie aktualizacji** w konsoli Web (pozycja **Aktualizacje** > **Podsumowanie**). Na tym ekranie częstotliwość aktualizacji dla zainstalowanego składnika jest zawsze większa od 0%.

4. Określ częstotliwość pobierania składników. Pliki sygnatur są często aktualizowane (niektóre nawet codziennie), dlatego należy aktualizować je regularnie.
W przypadku silników i sterowników można poprosić dostawcę pomocy technicznej o powiadamianie o najważniejszych aktualizacjach.
5. Na źródle aktualizacji:
   a. Połącz się z serwerem ActiveUpdate. Adres URL serwera jest zależny od wersji programu OfficeScan.
   b. Pobierz następujące elementy:
      - Plik `server.ini`. Ten plik zawiera informacje o najnowszych składnikach.

- Składniki zidentyfikowane w kroku 3.

c. Zapisz pobrane elementy w katalogu źródła aktualizacji.

6. Uruchom ręczną aktualizację serwera OfficeScan. Szczegółowe informacje zawiera sekcja *Ręczna aktualizacja serwera OfficeScan na stronie 6-27*.

7. Powtórz procedurę od kroku 5 do kroku 6 za każdym razem, gdy konieczna jest aktualizacja składników.

Metody aktualizacji serwera OfficeScan

Składniki serwera OfficeScan można aktualizować ręcznie lub zgodnie z ustalonym harmonogramem aktualizacji.

Aby umożliwić serwerowi instalowanie zaktualizowanych składników na agentach, należy włączyć automatyczną aktualizację agentów.<agenci--> Szczegółowe informacje zawiera sekcja *Aktualizacja automatyczna agentów OfficeScan na stronie 6-40*. Jeśli automatyczne aktualizacje agentów są wyłączone, serwer pobiera aktualizacje, ale nie instaluje ich na agentach.

Dostępne są następujące metody aktualizacji:

- **Ręczna aktualizacja serwera**: gdy aktualizacja jest krytyczna, należy ją przeprowadzić ręcznie, tak aby serwer niezwłocznie ją uzyskał. Szczegółowe informacje można znaleźć w części *Ręczna aktualizacja serwera OfficeScan na stronie 6-27*.

- **Zaplanowana aktualizacja serwera**: serwer OfficeScan łączy się ze źródłem aktualizacji i pobiera najnowsze składniki zgodnie z datą i godziną ustaloną w harmonogramie. Szczegółowe informacje można znaleźć w części *Konfigurowanie aktualizacji serwera OfficeScan na stronie 6-28*.

Ręczna aktualizacja serwera OfficeScan

Składniki przechowywane na serwerze OfficeScan należy ręcznie aktualizować po zainstalowaniu lub ulepszeniu serwera oraz każdorazowo w przypadku epidemii.

Procedura

1. Przejdź do opcji **Aktualizacje** > **Serwer** > **Aktualizacja ręczna**.
2. Wybierz składniki do zaktualizowania.
3. Kliknij przycisk **Aktualizuj**.

   Serwer pobierze zaktualizowane składniki.

Konfigurowanie aktualizacji serwera OfficeScan

Można skonfigurować serwer OfficeScan do okresowego sprawdzania źródła aktualizacji i automatycznego pobierania dostępnych aktualizacji. Ponieważ agenci zazwyczaj pobierają aktualizacje z serwera, korzystanie z automatycznej zaplanowanej aktualizacji to wygodny i skuteczny sposób zapewniania stale aktualnej ochrony przed zagrożeniami bezpieczeństwa.

Procedura

1. Przejdź do opcji **Aktualizacje** > **Serwer** > **Aktualizacja zaplanowana**.
2. Wybierz **Włącz zaplanowaną aktualizację serwera OfficeScan**.
3. Wybierz składniki do zaktualizowania.
4. Określ harmonogram aktualizacji.

   W przypadku aktualizacji dziennych, tygodniowych i miesięcznych, czas to liczba godzin, w czasie których program OfficeScan przeprowadza aktualizacje. Program OfficeScan dokonuje aktualizacji w dowolnym podanym czasie w tym okresie.
5. Kliknij przycisk **Zapisz**.

Dzienniki aktualizacji serwera OfficeScan

W dziennikach aktualizacji serwera znajdują się informacje umożliwiające sprawdzenie, czy występują problemy dotyczące aktualizacji określonych składników. Dzienniki zawierają informacje o aktualizacjach składników pobieranych z serwera OfficeScan.

Aby dzienniki nie zajmowały zbyt dużo miejsca na dysku twardym, można je ręcznie usunąć lub skonfigurować harmonogram ich usuwania. Dodatkowe informacje dotyczące dzienników zarządzania zawiera sekcja *Zarządzanie dziennikiem na stronie 14-41*.

Wyświetlanie dzienników aktualizacji

Procedura

1. Przejdź do opcji **Dzienniki** > **Aktualizacje serwera**.
2. Informacje o składnikach, które nie zostały zaktualizowane, zawiera kolumna **Wynik**.
3. Aby zapisać dzienniki w formacie `CSV` (plik z tekstem oddzielanym przecinkami), kliknij opcję **Eksportuj do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Aktualizacje zintegrowanego serwera Smart Protection

Zintegrowany Serwer Smart Protection pobiera dwa składniki, a mianowicie sygnatury Smart Scan i listę blokowania Web. Szczegółowe informacje o tych składnikach i sposobie ich aktualizowania zawiera temat *Zarządzanie zintegrowanym serwerem Smart Protection na stronie 4-19*.

Aktualizacje agenta OfficeScan

Aby zapewnić stałą ochronę agentów przed najnowszymi zagrożeniami, należy regularnie aktualizować składniki agenta.

Przed przeprowadzeniem aktualizacji agentów należy sprawdzić, czy źródło aktualizacji (serwer OfficeScan lub niestandardowe źródło aktualizacji) zawiera najnowsze wersje składników. Informacje na temat sposobu aktualizacji serwera OfficeScan znajdują się w części *Aktualizacje serwera OfficeScan na stronie 6-16*.

W poniższej tabeli wymieniono wszystkie składniki, które są instalowane na agentach przez źródła aktualizacji, oraz składniki, które są używane w przypadku korzystania z poszczególnych metod skanowania.

TABELA 6-5. Składniki programu OfficeScan instalowane na agentach

SKŁADNIK	DYSTRYBUCJA	
	AGENCI SKANOWANIA STANDARDOWEGO	AGENCI SMART SCAN
Antywirus		
Sygnatura Agenta Smart Scan	Nie	Tak
Sygnatura wirusów	Tak	Nie
Sygnatura IntelliTrap	Tak	Tak
Sygnatura wyjątków IntelliTrap	Tak	Tak
Silnik skanowania antywirusowego, 32-bitowe/64-bitowe	Tak	Tak
Sygnatura kontroli pamięci	Tak	Tak
Sygnatura wczesnego uruchamiania ochrony przed złośliwym oprogramowaniem (32/64-bitowe)	Tak	Tak
Silnik analizy kontekstowej (32/64 bity)	Tak	Tak
Sygnatura analizy kontekstowej	Tak	Tak
Mechanizm obsługi zapytań analizy kontekstowej (32/64 bity)	Tak	Tak
Silnik skanowania w poszukiwaniu zagrożeń zaawansowanych (32/64 bity)	Tak	Tak
Wzorzec korelacji zagrożeń zaawansowanych	Tak	Tak

Składnik	Dystrybucja	
	Agenci skanowania standardowego	Agenci Smart Scan
Oprogramowanie anty-spyware		
Sygnatura spyware/grayware	Tak	Tak
Sygnatura aktywnego monitorowania oprogramowania spyware	Tak	Nie
Silnik skanowania spyware/grayware (32/64-bitowe)	Tak	Tak
Usługi Usuwania Szkód Services		
Szablon usługi Usuwania Szkód	Tak	Tak
Silnik usług Usuwania Szkód (32-bitowy/64-bitowy)	Tak	Tak
Sterownik wczesnego czystego rozruchu (32/64-bitowe)	Tak	Tak
Usługi Web Reputation Services		
Silnik filtrowania adresów URL	Tak	Tak
Zapora		
Ogólna sygnatura zapory	Tak	Tak
Ogólny sterownik zapory (32/64-bitowe)	Tak	Tak
Składniki monitorowania zachowań		
Sygnatura wykrywania funkcji Monitorowanie zachowań (32-bitowa/64-bitowa)	Tak	Tak
Sterowniki głównego monitora zachowań, 32-bit/64-bit	Tak	Tak

Składnik	Dystrybucja	
	Agenci skanowania standardowego	Agenci Smart Scan
Główna usługa monitorowania zachowania, wersja 32-bitowa/64-bitowa	Tak	Tak
Sygnatura konfiguracji monitorowania zachowania	Tak	Tak
Sygnatura stosowania zasad	Tak	Tak
Sygnatura podpisu cyfrowego	Tak	Tak
Sygnatura Memory Scan Trigger Pattern (32/64-bitowe)	Tak	Tak
Sygnatura monitorowania inspekcji programów	Tak	Tak
Sygnatura przywracania po uszkodzeniach	Tak	Tak
Podejrzane połączenia		
Globalna lista numerów IP C&C	Tak	Tak
Sygnatura reguły istotności	Tak	Tak
Rozwiązanie luki w zabezpieczeniach przeglądarki		
Sygnatura zapobiegania wykorzystaniu przeglądarki	Tak	Tak
Ujednolicona sygnatura analizatora skryptów	Tak	Tak

Źródła aktualizacji agenta OfficeScan

agenci mogą pobierać aktualizacje ze standardowego źródła aktualizacji (serwera OfficeScan) lub określone składniki z niestandardowych źródeł aktualizacji, takich jak

serwer Trend Micro ActiveUpdate. Szczegółowe informacje zawiera sekcja *Standardowe źródła aktualizacji dla agentów OfficeScan na stronie 6-33* i *Niestandardowe źródło aktualizacji dla agentów OfficeScan na stronie 6-35*.

Obsługa protokołu IPv6 dla aktualizacji agenta OfficeScan

Agent wykorzystujący wyłącznie protokół IPv6 nie może wykonywać aktualizacji bezpośrednio ze źródeł wykorzystujących wyłącznie protokół IPv4, takich jak:

- Serwer OfficeScan wykorzystujący wyłącznie protokół IPv4
- Agent aktualizacji wykorzystujący wyłącznie protokół IPv4
- Dowolne niestandardowe źródło aktualizacji wykorzystujące wyłącznie protokół IPv4
- Trend Micro ActiveUpdate Server

Analogicznie, agent wykorzystujący wyłącznie protokół IPv4 nie może wykonywać aktualizacji bezpośrednio ze źródeł aktualizacji wykorzystujących wyłącznie protokół IPv6, takich jak serwer OfficeScan wykorzystujący wyłącznie protokół IPv6 lub agent aktualizacji.

Aby umożliwić agentom nawiązanie połączenia ze źródłami aktualizacji, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.

Standardowe źródła aktualizacji dla agentów OfficeScan

Standardowym źródłem aktualizacji agentów jest serwer OfficeScan.

Jeśli serwer OfficeScan będzie nieosiągalny, agenci nie będą mieć źródła zapasowego, przez co pozostaną nieaktualni. Aby zaktualizować agentów, którzy nie mogą osiągnąć serwera OfficeScan, firma Trend Micro zaleca użycie narzędzia Agent Packager. Za pomocą tego narzędzia można utworzyć pakiet z najnowszymi składnikami dostępnymi na serwerze, a następnie uruchomić pakiet na agentach.

Uwaga

Adres IP agenta (IPv4 lub IPv6) określa, czy można nawiązać połączenie z serwerem OfficeScan. Szczegółowe informacje o obsłudze protokołu IPv6 dla aktualizacji agentów zawiera temat *Obsługa protokołu IPv6 dla aktualizacji agenta OfficeScan na stronie 6-33*.

Konfigurowanie standardowego źródła aktualizacji agentów OfficeScan

Procedura

1. Przejdź do opcji **Aktualizacje** > **Agenci** > **Źródło aktualizacji**.
2. Wybierz opcję **Standardowe źródło aktualizacji (aktualizacja z serwera OfficeScan)**.
3. Kliknij polecenie **Powiadom wszystkich agentów**.

Proces aktualizacji agentów OfficeScan

Uwaga

W tym temacie omówiono proces aktualizacji agentów OfficeScan. Proces aktualizacji agentów aktualizacji omówiony w temacie *Standardowe źródła aktualizacji dla agentów OfficeScan na stronie 6-33*.

W przypadku skonfigurowania agentów OfficeScan do pobierania aktualizacji bezpośrednio z serwera OfficeScan proces aktualizacji przebiega następująco:

1. Agent OfficeScan pobiera aktualizacje z serwera OfficeScan.
2. Jeśli nie można wykonać aktualizacji z serwera OfficeScan, Agent OfficeScan próbuje nawiązać połączenie bezpośrednio z serwerem Trend Micro ActiveUpdate Server, gdy włączona jest opcja **Agenci OfficeScan pobierają aktualizacje z serwera Trend Micro ActiveUpdate Server** w sekcji **Agenci** > **Zarządzanie agentami**, kliknij kolejno **Ustawienia** > **Uprawnienia i inne ustawienia** > **Inne ustawienia (karta)** > **Ustawienia aktualizacji**.

Uwaga

Za pośrednictwem serwera ActiveUpdate można zaktualizować tylko składniki. Ustawienia domeny, programy i pakiety hot fix można pobierać tylko z serwera OfficeScan lub agentów aktualizacji. Proces aktualizacji można przyspieszyć, konfigurując agentów OfficeScan do pobierania tylko plików sygnatur z serwera ActiveUpdate. Aby uzyskać więcej informacji, patrz *Serwer ActiveUpdate jako źródło aktualizacji agentów OfficeScan na stronie 6-39*.

Niestandardowe źródło aktualizacji dla agentów OfficeScan

Agenci OfficeScan mogą pobierać aktualizacje nie tylko z serwera OfficeScan, lecz również z niestandardowych źródeł aktualizacji. Niestandardowe źródła aktualizacji ograniczają ruch sieciowy związany z przesyłaniem aktualizacji agentów OfficeScan na serwer OfficeScan i umożliwiają agentom OfficeScan, którzy nie łączą się z serwerem OfficeScan, pobieranie aktualizacji w oczekiwanym czasie. Informacje o niestandardowych źródłach aktualizacji są przechowywane na liście niestandardowych źródeł aktualizacji, która może zawierać maksymalnie 1024 wpisy.

Porada

Firma Trend Micro zaleca przypisanie niektórym agentom OfficeScan roli agentów aktualizacji, a następnie dodanie ich do listy.

Konfigurowanie niestandardowych źródeł aktualizacji dla agentów OfficeScan

Procedura

1. Przejdź do opcji **Aktualizacje** > **Agenci** > **Źródło aktualizacji**.
2. Wybierz opcję **Niestandardowe źródło aktualizacji** i kliknij przycisk **Dodaj**.
3. Na wyświetlonym ekranie wpisz adresy IP agentów. Można wpisać zakres adresów IPv4 i/lub prefiks IPv6 i długość.
4. Określ źródło aktualizacji. Można wybrać agenta aktualizacji, jeśli został już wyznaczony, lub wpisać adres URL wybranego źródła.

Uwaga

Upewnij się, że Agenci OfficeScan mogą nawiązać połączenie ze źródłem aktualizacji przy użyciu swoich adresów IP. Jeśli na przykład określono zakres adresów IPv4, źródło aktualizacji musi mieć adres IPv4. Jeśli określono prefiks IPv6 i długość, źródło aktualizacji musi mieć adres IPv6. Szczegółowe informacje o obsłudze protokołu IPv6 dla aktualizacji agentów zawiera temat *Źródła aktualizacji agenta OfficeScan na stronie 6-32*.

5. Kliknij przycisk **Zapisz**.

6. Na tym ekranie można wykonywać różne zadania.

   a. Wybierz jedno z następujących ustawień. Szczegółowe informacje o sposobie działania tych ustawień zawiera sekcja *Proces aktualizacji agentów OfficeScan na stronie 6-34*.

      - **Aktualizacja składników aktualizacji agentów, ustawień domeny oraz agentów i poprawek; wyłącznie z serwera OfficeScan**

      - Agenci OfficeScan aktualizują następujące składniki z serwera OfficeScan, jeśli wszystkie niestandardowe źródła są niedostępne lub nie zostały odnalezione:

        - **Składniki**

        - **Ustawienia domeny**

        - **Programy i poprawki agenta OfficeScan**

   b. Jeśli jako źródło określono co najmniej jednego agenta aktualizacji, kliknij opcję **Raport analityczny agenta aktualizacji**, aby wygenerować raport przedstawiający stan aktualizacji agentów. Szczegółowe informacje o raporcie zawiera temat *Raport analityczny agenta aktualizacji na stronie 6-66*.

   c. Zmodyfikuj źródło aktualizacji, klikając łącze zakresu adresów IP. Zmień ustawienia na ekranie, który zostanie wyświetlony, następnie kliknij przycisk **Zapisz**.

   d. Usuń źródło aktualizacji z listy, zaznaczając pole wyboru i klikając przycisk **Usuń**.

e. Aby przenieść źródło aktualizacji, kliknij przycisk strzałki w górę lub w dół. Jednocześnie można przenosić tylko jedno źródło.

7. Kliknij polecenie **Powiadom wszystkich agentów**.

Proces aktualizacji agentów OfficeScan

Uwaga

W tym temacie omówiono proces aktualizacji agentów OfficeScan. Proces aktualizacji agentów aktualizacji omówiony w temacie *Niestandardowe źródła aktualizacji dla agentów aktualizacji na stronie 6-62*.

Po skonfigurowaniu i zapisaniu listy niestandardowych źródeł aktualizacji proces aktualizacji przebiega następująco:

1. Agent OfficeScan pobiera aktualizacje z pierwszego źródła na liście.
2. Jeśli pobranie aktualizacji z pierwszego źródła nie jest możliwe, Agent OfficeScan pobiera aktualizacje z drugiego źródła itd.
3. Jeśli nie można pobrać aktualizacji z żadnego źródła, Agent OfficeScan sprawdza następujące ustawienia na ekranie **Źródło aktualizacji**:

TABELA 6-6. Dodatkowe ustawienia dla niestandardowych źródeł aktualizacji

USTAWIENIE	OPIS
Aktualizacja składników aktualizacji agentów, ustawień domeny oraz agentów i poprawek; wyłącznie z serwera OfficeScan	Jeśli to ustawienie jest włączone, agent aktualizacji pobiera aktualizacje bezpośrednio z serwera OfficeScan, ignorując listę Lista niestandardowych źródeł aktualizacji. Jeśli ustawienie jest wyłączone, agenci aktualizacji stosują niestandardowe ustawienia źródeł aktualizacji skonfigurowane dla zwykłych agentów.
Agenci OfficeScan aktualizują następujące składniki z serwera OfficeScan, jeśli wszystkie niestandardowe źródła są niedostępne lub nie zostały odnalezione:	

USTAWIENIE	OPIS
Składniki	Jeśli to ustawienie jest włączone, agent pobiera aktualizacje składników z serwera OfficeScan. Jeśli to ustawienie jest wyłączone, agent próbuje połączyć się bezpośrednio z serwerem Trend Micro ActiveUpdate, ale z uwzględnieniem następujących warunków: • W sekcji **Agenci** > **Zarządzanie agentami** kliknij kolejno **Ustawienia** > **Uprawnienia i inne ustawienia** > **Inne ustawienia (karta)** > **Ustawienia aktualizacji**, opcja **Agenci OfficeScan pobierają aktualizacje z serwera Trend Micro ActiveUpdate Server** jest włączona. • Serwer ActiveUpdate nie znajduje się na liście niestandardowych źródeł aktualizacji. **Uwaga** Za pośrednictwem serwera ActiveUpdate można zaktualizować tylko składniki. Ustawienia domeny, programy i pakiety hot fix można pobierać tylko z serwera OfficeScan lub agentów aktualizacji. Proces aktualizacji można przyspieszyć, konfigurując agentów OfficeScan do pobierania tylko plików sygnatur z serwera ActiveUpdate. Aby uzyskać więcej informacji, patrz *Serwer ActiveUpdate jako źródło aktualizacji agentów OfficeScan na stronie 6-39*.
Ustawienia domeny	Jeśli to ustawienie jest włączone, agent pobiera aktualizacje ustawień poziomu domeny z serwera OfficeScan.
Programy i poprawki agenta OfficeScan	Jeśli to ustawienie jest włączone, agent pobiera aktualizacje programów i pakietów Hot Fix z serwera OfficeScan.

4. Jeśli nie można pobrać aktualizacji z żadnego dostępnego źródła, agent zatrzymuje proces aktualizacji.

Serwer ActiveUpdate jako źródło aktualizacji agentów OfficeScan

Jeśli agenci OfficeScan pobierają aktualizacje bezpośrednio z serwera Trend Micro ActiveUpdate, pobieranie można ograniczyć do plików sygnatur, co spowoduje zmniejszenie wykorzystania przepustowości podczas aktualizacji i przyspieszenie procesu aktualizacji.

Silniki skanowania i inne składniki nie są aktualizowane tak często, jak pliki sygnatur, co jest kolejnym powodem, dla którego warto ograniczyć pobieranie tylko do plików sygnatur.

Agent wykorzystujący wyłącznie protokół IPv6 nie może wykonywać aktualizacji bezpośrednio z serwera Trend Micro ActiveUpdate Server. Aby umożliwić agentom OfficeScan nawiązanie połączenia z serwerem ActiveUpdate, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.

Ograniczanie pobieranie z serwera ActiveUpdate

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Kliknij kartę **System**.
3. Przejdź do sekcji **Aktualizacje**.
4. Wybierz opcję **Podczas przeprowadzania aktualizacji z serwera ActiveUpdate pobieraj tylko pliki sygnatur**.

Metody aktualizacji agenta OfficeScan

Agenci OfficeScan, którzy aktualizują składniki z serwera OfficeScan lub z niestandardowego źródła aktualizacji, mogą korzystać z następujących metod aktualizacji:

- **Aktualizacje automatyczne**: aktualizacje agentów są inicjowane automatycznie zgodnie z ustalonym harmonogramem lub gdy zostaną one wywołane przez

określone zdarzenie. Szczegółowe informacje zawiera sekcja *Aktualizacja automatyczna agentów OfficeScan na stronie 6-40*.

- **Aktualizacje ręczne**: gdy aktualizacja jest krytyczna, należy ją przeprowadzić ręcznie, aby niezwłocznie powiadomić agentów o konieczności aktualizacji składników. Szczegółowe informacje zawiera sekcja *Aktualizacja ręczna agentów OfficeScan na stronie 6-47*.

- **Aktualizacje zależne od uprawnień**: użytkownicy mający przypisane uprawnienia do aktualizacji mają większa kontrolę nad sposobem aktualizacji agenta OfficeScan zainstalowanego na komputerze. Szczegółowe informacje zawiera sekcja *Konfigurowanie uprawnień aktualizacji i innych ustawień na stronie 6-48*.

Aktualizacja automatyczna agentów OfficeScan

Przeprowadzanie aktualizacji automatycznych zwalnia z obowiązku powiadamiania wszystkich agentów o konieczności przeprowadzenia aktualizacji oraz eliminuje zagrożenie związane z występowaniem nieaktualnych składników na komputerach agentów.

Oprócz składników Agenci OfficeScan odbierają podczas automatycznej aktualizacji zaktualizowane pliki konfiguracji. Agenci potrzebują plików konfiguracji, aby zastosować nowe ustawienia. Pliki konfiguracji zmieniają się po każdej modyfikacji ustawień programu OfficeScan z poziomu konsoli Web. Informacje o określaniu częstości stosowania plików konfiguracyjnych na agentach znajdują się w punkcie 3 w temacie *Konfigurowanie automatycznych aktualizacji agenta OfficeScan na stronie 6-42*.

Uwaga

Agentów można skonfigurować tak, aby podczas aktualizacji automatycznej były używane ustawienia proxy. Szczegółowe informacje można znaleźć w części *Serwer proxy do aktualizacji składników agenta OfficeScan na stronie 6-52*.

Istnieją dwa typy automatycznych aktualizacji:

- *Aktualizacje wywołana zdarzeniem na stronie 6-41*
- *Aktualizacje w oparciu o harmonogram na stronie 6-42*

Aktualizacje wywołana zdarzeniem

Po pobraniu najnowszych składników serwer może powiadamiać o możliwości ich aktualizacji agentów online, a także agentów offline po ponownym uruchomieniu i połączeniu się z serwerem. Po aktualizacji można opcjonalnie zainicjować funkcję Skanuj teraz (skanowanie ręczne) na punktach końcowych Agent OfficeScan.

TABELA 6-7. Opcje aktualizacji wywołanej zdarzeniem

OPCJA	OPIS
Rozpocznij natychmiastową aktualizację składnika na agentach po jego pobraniu przez serwer OfficeScan	Serwer powiadamia agentów o konieczności zainstalowania aktualizacji natychmiast po jej pobraniu. Często aktualizowani agenci muszą tylko pobrać przyrostowe wzorce sygnatur, skracając w ten sposób czas potrzebny na dokonanie aktualizacji (szczegółowe informacje na temat przyrostowych wzorców sygnatur: *Duplikacja składników serwera OfficeScan na stronie 6-22*). Należy jednak pamiętać, że częste przeprowadzanie aktualizacji może negatywnie wpływać na wydajność serwera, zwłaszcza jeśli w tym samym czasie aktualizację wykonuje wielu agentów. Jeśli występują wymagający aktualizacji agenci działający w trybie niezależnym, należy zaznaczyć opcję **Uwzględnij agentów w trybie niezależnym i offline**. Szczegółowe informacje na temat trybu niezależnego zawiera rozdział *Uprawnienie trybu niezależnego Agent OfficeScan na stronie 15-19*.
Pozwól agentom rozpocząć aktualizację składnika po ponownym uruchomieniu i połączeniu się z serwerem OfficeScan (z wyłączeniem agentów w trybie niezależnym)	Agent, który nie przeprowadził aktualizacji, pobiera składniki natychmiast po ustanowieniu połączenia z serwerem. Agent może nie przeprowadzić aktualizacji, jeśli jest w trybie offline, lub gdy punkt końcowy, na którym jest zainstalowany, nie jest uruchomiony.

OPCJA	OPIS
Po aktualizacji przeprowadź operację Skanuj teraz (z wyłączeniem agentów w trybie niezależnym)	Serwer powiadamia agentów o konieczności przeprowadzenia skanowania po aktualizacji wywołanej zdarzeniem. Włączenie tej opcji należy rozważyć, jeśli określona aktualizacja została wykonana w odpowiedzi na zagrożenie bezpieczeństwa, które zdążyło się już rozprzestrzenić w sieci.

Uwaga

Jeśli serwer OfficeScan nie może pomyślnie przesłać do agentów powiadomienia o aktualizacji po pobraniu składników, po 15 minutach automatycznie przesyła powiadomienie ponownie. Serwer będzie w dalszym ciągu wysyłał powiadomienia maksymalnie pięciokrotnie, dopóki nie otrzyma odpowiedzi od agenta. Jeśli piąta próba nie powiedzie się, serwer przestanie wysyłać powiadomienia. Jeżeli wybrano opcję aktualizacji składników po ponownym uruchomieniu agenta, a następnie po połączeniu z serwerem, aktualizacja składników zostanie przeprowadzona.

Aktualizacje w oparciu o harmonogram

Przeprowadzanie aktualizacji zaplanowanych wymaga odpowiedniego uprawnienia. Należy najpierw wskazać agentów OfficeScan, którzy mają przypisane to uprawnienie. Będą oni mogli następnie uruchamiać aktualizacje zgodnie z ustalonym harmonogramem.

Uwaga

Informacje na temat aktualizacji opartej na harmonogramie z translacją adresu sieciowego znajdują się w części: *Konfigurowanie zaplanowanych aktualizacji agentów OfficeScan przy użyciu translatora NAT na stronie 6-44*.

Konfigurowanie automatycznych aktualizacji agenta OfficeScan

Procedura

1. Przejdź do opcji **Aktualizacje** > **Agenci** > **Aktualizacja automatyczna**.

2. Wybierz zdarzenia dla opcji **Aktualizacja wywołana zdarzeniem**:

   - **Rozpocznij natychmiastową aktualizację składnika na agentach po jego pobraniu przez serwer OfficeScan**

     - **Uwzględnij agentów w trybie niezależnym i offline**

   - **Pozwól agentom rozpocząć aktualizację składnika po ponownym uruchomieniu i połączeniu się z serwerem OfficeScan (z wyłączeniem agentów w trybie niezależnym)**

   - **Po aktualizacji przeprowadź operację Skanuj teraz (z wyłączeniem agentów w trybie niezależnym)**

   Szczegółowe informacje o dostępnych opcjach zawiera sekcja *Aktualizacje wywołana zdarzeniem na stronie 6-41*.

3. Skonfiguruj harmonogram dla ustawienia **Aktualizacja w oparciu o harmonogram**.

   - **Min** lub **Godz.**

     Opcja **Aktualizuj konfiguracje agenta tylko raz dziennie** jest dostępna podczas planowania aktualizacji opartej na godzinach lub minutach. Plik konfiguracyjny zawiera wszystkie ustawienia agenta OfficeScan skonfigurowane przy użyciu konsoli Web.

     Porada

     Firma Trend Micro często aktualizuje składniki, jednak ustawienia konfiguracji programu OfficeScan prawdopodobnie zmieniają się rzadziej. Aktualizacja plików konfiguracji wraz ze składnikami programu OfficeScan wymaga większej przepustowości i trwa dłużej. Z tego powodu firma Trend Micro zaleca aktualizowanie konfiguracji agenta OfficeScan tylko raz dziennie.

   - **Codziennie** lub **Co tydzień**

     Podaj godzinę aktualizacji i okres, przez jaki serwer OfficeScan będzie powiadamiał agentów o konieczności aktualizacji składników.

Porada

Ustawienie to zapobiega sytuacji, gdy wszyscy agenci online jednocześnie łączą się z serwerem o określonej godzinie, dzięki czemu zostaje znacznie ograniczony ruch sieciowy do serwera. Jeśli godzina rozpoczęcia to na przykład godzina 12, a okres jest równy 2 godzinom, program OfficeScan będzie losowo powiadamiać wszystkich agentów online o aktualizacji składników w godzinach od 12 do 14.

Uwaga

Po skonfigurowaniu harmonogramu aktualizacji włącz harmonogram na wybranych agentach.

Szczegółowe informacje o włączaniu aktualizacji opartych na harmonogramie zawiera krok 4 w sekcji *Konfigurowanie uprawnień aktualizacji i innych ustawień na stronie 6-48*.

4. Kliknij przycisk **Zapisz**.

   Program OfficeScan nie może natychmiast powiadomić agentów offline. Wybierz opcję **Pozwól agentom rozpocząć aktualizację składnika po ponownym uruchomieniu i połączeniu się z serwerem OfficeScan (z wyłączeniem agentów w trybie niezależnym)**, aby zaktualizować agentów offline, które przejdą do trybu online po upływie okresu. Agenci offline bez tego ustawienia zaktualizują składniki w następnym zaplanowanym czasie lub podczas aktualizacji ręcznej.

Konfigurowanie zaplanowanych aktualizacji agentów OfficeScan przy użyciu translatora NAT

Jeśli sieć lokalna wykorzystuje mechanizm translacji NAT, mogą się pojawić następujące problemy:

- Agenci OfficeScan mogą być wyświetlani w konsoli Web ze stanem offline.
- Serwer OfficeScan nie może pomyślnie powiadomić agentów o aktualizacjach i zmianach konfiguracji.

Tym problemom można zaradzić, pobierając najnowsze wersje składników i plików konfiguracyjnych z serwera na agenta ScanOffice i instalując je za pomocą mechanizmu zaplanowanych aktualizacji, zgodnie z poniższym opisem.

Procedura

- Przed zainstalowaniem agenta OfficeScan na komputerach agentów:

  a. Skonfiguruj harmonogram aktualizacji agentów w sekcji **Aktualizacja w oparciu o harmonogram** na stronie **Aktualizacje** > **Agenci** > **Aktualizacja automatyczna**.

  b. Nadaj agentom uprawnienie do włączania zaplanowanej aktualizacji w opcji **Agenci** > **Zarządzanie agentami**; kliknij kolejno **Ustawienia** > **Uprawnienia i inne ustawienia** > **Uprawnienia (karta)** > **Aktualizacje składników**.

- Jeśli Agenci OfficeScan są już zainstalowani na komputerach agent:

  a. Nadaj agentom uprawnienie do wykonywania funkcji „Aktualizuj teraz" w opcji **Agenci** > **Zarządzanie agentami**; kliknij kolejno **Ustawienia** > **Uprawnienia i inne ustawienia** > **Uprawnienia (karta)** > **Aktualizacje składników**.

  b. Poleć użytkownikom, aby ręcznie zaktualizowali składniki na punkcie końcowym (poprzez kliknięcie prawym przyciskiem myszy ikony agenta OfficeScan na pasku zadań, a następnie kliknięcie opcji „Aktualizuj teraz") w celu uzyskania zaktualizowanych ustawień konfiguracyjnych.

Gdy Agenci OfficeScan zostaną zaktualizowani, otrzymają zarówno uaktualnione składniki, jak i pliki konfiguracyjne.

Korzystanie z narzędzia aktualizacji harmonogramu domen

Harmonogram aktualizacji skonfigurowany dla automatycznych aktualizacji agentów jest stosowany wyłącznie do agentów z uprawnieniami do zaplanowanej aktualizacji. Dla innych agentów można ustawić oddzielny harmonogram aktualizacji. W tym celu należy skonfigurować harmonogram według domen drzewa agentów. Harmonogram będzie stosowany przez wszystkich agentów należących do domeny.

Uwaga

Nie jest możliwe skonfigurowanie harmonogramu aktualizacji dla określonego agenta lub poddomeny. Wszystkie poddomeny stosują harmonogram skonfigurowany dla ich domeny nadrzędnej.

Procedura

1. Zapisz nazwy domen drzewa agentów i harmonogramy aktualizacji.
2. Przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\DomainScheduledUpdate`.
3. Skopiuj następujące pliki do folderu `<Folder instalacji serwera>\PCCSRV`:
   - `DomainSetting.ini`
   - `dsu_convert.exe`
4. Otwórz plik `DomainSetting.ini` za pomocą edytora tekstu, np. Notatnika.
5. Określ domenę drzewa agentów, a następnie skonfiguruj harmonogram aktualizacji dla domeny. Powtórz ten krok, aby dodać więcej domen.

   Uwaga

   Szczegółowe instrukcje konfiguracji znajdują się w pliku `.ini`.
6. Zapisz plik `DomainSetting.ini`.
7. Otwórz wiersz polecenia i przejdź do folderu `PCCSRV`.
8. Wpisz poniższe polecenie i naciśnij klawisz `Enter`.

   ```
   dsuconvert.exe DomainSetting.ini
   ```
9. W konsoli Web przejdź do pozycji **Agenci** > **Ustawienia agenta globalnego**.
10. Kliknij przycisk **Zapisz**.

Aktualizacja ręczna agentów OfficeScan

Gdy składniki agenta OfficeScan są bardzo nieaktualne i każdorazowo podczas epidemii aktualizację należy przeprowadzać ręcznie. Składniki agenta OfficeScan stają się nieaktualne, kiedy Agent OfficeScan przez dłuższy czas nie może pobrać składników ze źródła aktualizacji.

Oprócz składników Agenci OfficeScan automatycznie odbierają podczas aktualizacji ręcznej zaktualizowane pliki konfiguracji. Agenci OfficeScan potrzebują plików konfiguracji, aby zastosować nowe ustawienia. Pliki konfiguracji zmieniają się po każdej modyfikacji ustawień programu OfficeScan z poziomu konsoli Web.

Uwaga

Oprócz inicjowania ręcznych aktualizacji, można przyznać użytkownikom uprawnienie do uruchamiania ręcznych aktualizacji (tzn. funkcji **Aktualizuj teraz**) na punktach końcowych agentów OfficeScan. Szczegółowe informacje zawiera sekcja *Konfigurowanie uprawnień aktualizacji i innych ustawień na stronie 6-48*.

Ręczna aktualizacja agentów OfficeScan

Procedura

1. Przejdź do opcji **Aktualizacje** > **Agenci** > **Aktualizacja ręczna**.
2. W górnej części ekranu zostaną wyświetlone składniki obecnie dostępne na serwerze OfficeScan oraz informacje o czasie ich ostatniej aktualizacji. Przed powiadomieniem agentów o konieczności aktualizacji sprawdź, czy składniki są aktualne.

   Uwaga

   Ręcznie zaktualizuj nieaktualne składniki na serwerze.

   Szczegółowe informacje można znaleźć w części *Aktualizacja ręczna agentów OfficeScan na stronie 6-47*.

3. Aby zaktualizować tylko agentów z nieaktualnymi składnikami:

a. Kliknij opcję **Wybierz agentów z nieaktualnymi składnikami**.

b. (Opcjonalnie) Wybierz opcję **Uwzględnij agentów w trybie niezależnym i offline**:

- Aby zaktualizować agentów w trybie niezależnym z działającym połączeniem z serwerem.
- Aby zaktualizować agentów offline w momencie ich przejścia w stan online.

c. Kliknij polecenie **Zainicjuj aktualizację**.

Uwaga

Serwer szuka agentów o składnikach w wersjach wcześniejszych niż wersje zapisane na serwerze, a następnie powiadamia tych agentów o konieczności aktualizacji. Aby sprawdzić stan powiadomień, przejdź do ekranu **Aktualizacje** > **Podsumowanie**.

4. Aby zaktualizować wybranych agentów:

a. Wybierz opcję **Wybierz ręcznie agentów**.

b. Kliknij przycisk **Wybierz**.

c. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.

d. Kliknij polecenie **Zainicjuj aktualizację**.

Uwaga

Serwer rozpocznie powiadamianie agentów o konieczności pobrania zaktualizowanych składników. Aby sprawdzić stan powiadomień, przejdź do ekranu **Aktualizacje** > **Podsumowanie**.

Konfigurowanie uprawnień aktualizacji i innych ustawień

Skonfiguruj ustawienia aktualizacji i przydziel różne uprawnienia użytkownikom agenta, takie jak uprawnienie do wykonywania funkcji „Aktualizuj teraz” lub do włączania aktualizacji zaplanowanych.

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Kliknij kartę **Inne ustawienia** i skonfiguruj następujące opcje w sekcji **Ustawienia aktualizacji**:

OPCJA	OPIS
Agenci OfficeScan pobierają aktualizacje z serwera Trend Micro ActiveUpdate Server	W przypadku rozpoczęcia aktualizacji Agenci OfficeScan w pierwszej kolejności uzyskują aktualizacje ze źródła aktualizacji określonego na ekranie **Aktualizacje** > **Agenci** > **Źródło aktualizacji**. W przypadku niepowodzenia aktualizacji agenci próbują pobrać aktualizację z serwera OfficeScan. Wybranie tej opcji umożliwia agentom pobieranie aktualizacji z serwera Trend Micro ActiveUpdate, jeśli próba aktualizacji z serwera OfficeScan zakończy się niepowodzeniem. **Uwaga** Agent wykorzystujący wyłącznie protokół IPv6 nie może wykonywać aktualizacji bezpośrednio z serwera Trend Micro ActiveUpdate. Aby umożliwić agentom OfficeScan nawiązanie połączenia z serwerem ActiveUpdate, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.
Włącz aktualizacje w oparciu o harmonogram na agentach OfficeScan	Wybranie tej opcji powoduje skonfigurowanie wszystkich agentów OfficeScan w celu domyślnego wykonywania aktualizacji w oparciu o harmonogram. Użytkownicy z uprawnieniem **Włącz/wyłącz aktualizacje w oparciu o harmonogram** mogą zmienić to ustawienie. Szczegółowe informacje na temat konfigurowania harmonogramu aktualizacji zawiera sekcja *Konfigurowanie automatycznych aktualizacji agenta OfficeScan na stronie 6-42*.

Opcja	Opis
Programy agentów mogą aktualizować składniki, ale nie mogą uaktualniać programu agenta ani instalować poprawek	Ta opcja zezwala na aktualizację składników, ale nie zezwala na instalowanie pakietów Hot Fix ani uaktualnianie agenta OfficeScan. **Uwaga** Wyłączenie tej opcji może mieć znaczący wpływ na wydajność serwera, ponieważ wszyscy agenci równocześnie łączą się z serwerem w celu uaktualnienia lub instalacji pakietu Hot Fix.

5. Kliknij kartę **Uprawnienia** i skonfiguruj następujące opcje w sekcji **Aktualizacje składników**:

Opcja	Opis
Wykonaj operację „Aktualizuj teraz”	Użytkownicy mający to uprawnienie mogą aktualizować składniki w dowolnej chwili, klikając ikonę agenta OfficeScan na pasku zadań prawym przyciskiem myszy i wybierając polecenie **Aktualizuj teraz**. **Uwaga** Użytkownicy agenta OfficeScan mogą korzystać z ustawień proxy podczas korzystania z funkcji „Aktualizuj teraz”. Szczegółowe informacje można znaleźć w części *Uprawnienia do konfiguracji proxy dla agentów na stronie 15-55*.
Włącz/wyłącz aktualizacje w oparciu o harmonogram	Wybranie tej opcji umożliwia użytkownikom agenta OfficeScan włączanie i wyłączanie zaplanowanych aktualizacji przy użyciu menu podręcznego agenta OfficeScan, co pozwala zmienić ustawienie **Włącz aktualizacje w oparciu o harmonogram**. **Uwaga** Administratorzy muszą najpierw wybrać ustawienie **Włącz aktualizacje w oparciu o harmonogram na agentach OfficeScan** na karcie **Inne ustawienie**, zanim ta pozycja menu pojawi się w menu agenta OfficeScan.

6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszlej domeny. Przyszle domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Konfigurowanie zarezerwowanego miejsca na dysku na potrzeby aktualizacji agentów OfficeScan

Program OfficeScan może przeznaczać pewną ilość miejsca na dysku agenta na pakiety Hot Fix, pliki sygnatur, silniki skanowania oraz aktualizacje programu. Program OfficeScan domyślnie rezerwuje 60 MB miejsca na dysku.

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Kliknij kartę **System**.
3. Przejdź do sekcji **Aktualizacje**.
4. Wybierz opcję **Zarezerwuj __ MB miejsca na dysku na uaktualnienia**.
5. Wybierz ilość miejsca na dysku.
6. Kliknij przycisk **Zapisz**.

Serwer proxy do aktualizacji składników agenta OfficeScan

Agenci OfficeScan używają ustawień proxy podczas automatycznej aktualizacji lub jeśli mają uprawnienie do wykonywania funkcji „Aktualizuj teraz”.

TABELA 6-8. Ustawienia proxy używane podczas aktualizacji składników agenta OfficeScan

METODA AKTUALIZACJI	UŻYWANE USTAWIENIA PROXY	UŻYWANIE
Aktualizacja automatyczna	• Automatyczne ustawienia proxy. Szczegółowe informacje zawiera sekcja *Automatyczne ustawienia proxy dla agenta OfficeScan na stronie 15-57*. • Ustawienia wewnętrznego serwera proxy. Szczegółowe informacje zawiera sekcja *Wewnętrzny serwer proxy dla agentów OfficeScan na stronie 15-52*.	1. Agenci OfficeScan będą w pierwszej kolejności używać do aktualizowania składników automatycznych ustawień proxy. 2. Jeśli automatyczne ustawienia proxy nie są włączone, będą używane ustawienia wewnętrznego serwera proxy. 3. Jeśli oba rodzaje ustawień są wyłączone, agenci nie będą używać żadnych ustawień proxy.

METODA AKTUALIZACJI	UŻYWANE USTAWIENIA PROXY	UŻYWANIE
Aktualizuj teraz	• Automatyczne ustawienia proxy. Szczegółowe informacje zawiera sekcja *Automatyczne ustawienia proxy dla agenta OfficeScan na stronie 15-57*. • Ustawienia proxy skonfigurowane przez użytkownika. Można przydzielać użytkownikom agenta uprawnienie do konfigurowania ustawień serwera proxy. Szczegółowe informacje zawiera sekcja *Uprawnienia do konfiguracji proxy dla agentów na stronie 15-55*.	1. Agenci OfficeScan będą w pierwszej kolejności używać do aktualizowania składników automatycznych ustawień proxy. 2. Jeśli automatyczne ustawienia proxy nie są włączone, będą używane ustawienia proxy skonfigurowane przez użytkownika. 3. Jeśli oba rodzaje ustawień są wyłączone, lub gdy automatyczne ustawienia proxy są wyłączone, a użytkownicy agenta nie mają wymaganego uprawnienia, agenci nie będą korzystać z serwera proxy podczas aktualizowania składników.

Konfigurowanie powiadomień dotyczących aktualizacji agenta OfficeScan

Program OfficeScan powiadamia użytkowników agenta, gdy występują zdarzenia związane z aktualizacją.

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Kliknij kartę **Kontrola agentów**.
3. Przejdź do sekcji **Ustawienia ostrzeżeń**.

4. Wybierz następujące opcje:

   - **Pokaż ikonę ostrzegawczą na pasku zadań systemu Windows, jeżeli plik sygnatur wirusów nie został uaktualniony w ciągu __ dni**: Na pasku zadań systemu Windows jest wyświetlana ikona ostrzeżenia przypominająca użytkownikowi o konieczności aktualizacji sygnatur wirusów, które nie były aktualizowane przez określoną liczbę dni. Aby zaktualizować sygnaturę, należy użyć dowolnych metod aktualizacji, które opisano w temacie *Metody aktualizacji agenta OfficeScan na stronie 6-39*.

     To ustawienie jest stosowane na wszystkich agentach zarządzanych przez serwer.

   - **Wyświetl powiadomienie, jeśli w celu wczytania sterownika trybu jądra jest konieczne ponowne uruchomienie punktu końcowego**: Po zainstalowaniu poprawki lub pakietu aktualizacyjnego zawierającego nową wersję sterownika jądra poprzednia wersja sterownika może nadal się znajdować na punkt końcowy. Jedynym sposobem na odinstalowanie poprzedniej wersji i załadowanie nowej jest ponowne uruchomienie punktu końcowego. Po ponownym uruchomieniu punktu końcowego nowa wersja jest automatycznie instalowana i nie ma potrzeby kolejnego uruchamiania.

     Po zainstalowaniu pakietu Hot Fix lub pakietu uaktualniającego na punkcie końcowym agenta jest natychmiast wyświetlane powiadomienie.

5. Kliknij przycisk **Zapisz**.

Wyświetlanie dzienników aktualizacji agenta OfficeScan

Dzienniki aktualizacji agentów zawierają informacje umożliwiające sprawdzenie, czy podczas aktualizowania sygnatur wirusów na agentach nie wystąpiły problemy.

Uwaga

W tej wersji produktu z poziomu konsoli Web można przeszukiwać tylko dzienniki dotyczące aktualizacji sygnatur wirusów.

Aby dzienniki nie zajmowały zbyt dużo miejsca na dysku twardym, można je ręcznie usunąć lub skonfigurować harmonogram ich usuwania. Dodatkowe informacje dotyczące dzienników zarządzania zawiera sekcja *Zarządzanie dziennikiem na stronie 14-41*.

Procedura

1. Przejdź do opcji **Dzienniki** > **Agenci** > **Aktualizacja składnika agenta**.
2. Aby wyświetlić liczbę aktualizacji agentów, kliknij przycisk **Wyświetl** w kolumnie **Postęp**. Na ekranie **Postęp aktualizacji składnika** jest wyświetlana liczba agentów zaktualizowanych w każdym 15-minutowym przedziale czasu oraz łączna liczba zaktualizowanych agentów.
3. Aby wyświetlić agentów, na których zaktualizowano sygnatury wirusów, kliknij przycisk **Wyświetl** w kolumnie **Szczegóły**.
4. Aby zapisać dzienniki w formacie CSV (plik z tekstem oddzielanym przecinkami), kliknij opcję **Eksportuj do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Wymuszanie aktualizacji agentów OfficeScan

Aby zapewnić, że agenci pobierają najnowsze składniki, należy użyć funkcji Zgodność z zabezpieczeniami. Funkcja Zgodność z zabezpieczeniami umożliwia wykrycie niezgodności składników między serwerem OfficeScan a agentami agenci. Niezgodności pojawiają się zwykle wtedy, gdy agenci nie mogą połączyć się z serwerem w celu aktualizacji składników. Jeżeli agent pobierze aktualizację z innego źródła (na przykład z serwera ActiveUpdate), może dojść do sytuacji, kiedy składnik na agencie jest nowszy niż ten na serwerze.

Aby uzyskać więcej informacji, patrz *Zgodność z zabezpieczeniami dla agentów zarządzanych na stronie 15-61*.

Wycofywanie składników agentów OfficeScan

Wycofywanie dotyczy przywracania poprzedniej wersji Sygnatury wirusa, sygnatura Agenta Smart Scan oraz Silnika skanowania antywirusowego. Jeżeli składniki te nie

funkcjonują właściwie, należy je wycofać do ich poprzednich wersji. Program OfficeScan zachowuje bieżącą i poprzednie wersje silnika skanowania antywirusowego oraz ostatnie pięć wersji sygnatury wirusa oraz sygnatura Agenta Smart Scan.

Uwaga

Wycofanie jest możliwe tylko w przypadku wymienionych wyżej składników.

Program OfficeScan używa różnych silników skanowania dla agentów wykorzystujących platformy 32- i 64-bitowe. Powyższe typy silników skanowania należy wycofywać niezależnie. Procedura wycofywania wszystkich typów silników skanowania jest jednakowa.

Procedura

1. Przejdź do opcji **Aktualizacje** > **Wycofywanie**
2. Kliknij opcję **Synchronizuj z serwerem** w odpowiednim obszarze.
   a. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
   b. Kliknij opcję **Wycofywanie**.
   c. Kliknij opcję **Wyświetl dzienniki aktualizacji**, aby sprawdzić wynik, lub przycisk **Wstecz**, aby wrócić do ekranu Wycofywanie.
3. Jeśli na serwerze istnieje starsza wersja pliku sygnatur, kliknij opcję **Wycofaj wersje serwera i agenta**, aby wycofać plik sygnatur zarówno z agenta, jak i serwera.

Uruchamianie narzędzia Touch Tool dla pakietów Hot Fix agenta OfficeScan

Narzędzie Touch Tool umożliwia synchronizację sygnatury czasowej jednego pliku z sygnaturą innego pliku lub czasem systemowym punktu końcowego. Jeśli próba instalacji pakietu hot fix na serwerze OfficeScan zakończy się niepowodzeniem, do zmiany sygnatury czasowej pakietu hot fix należy użyć narzędzia Touch Tool. Spowoduje

to, że program OfficeScan zinterpretuje plik pakietu hot fix jako nowy, dzięki czemu serwer spróbuje ponownie automatycznie zainstalować ten pakiet.

Procedura

1. Na serwerze OfficeScan przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\Touch`.

2. Skopiuj plik `TMTouch.exe` do folderu, w którym znajduje się plik do zmiany. Aby zsynchronizować sygnaturę czasową pliku z sygnaturą innego pliku, umieść oba pliki w tym samym miejscu co narzędzie Touch Tool.

3. Otwórz wiersz polecenia i przejdź do lokalizacji narzędzia Touch Tool.

4. Wpisz poniższy tekst:

   ```
   TmTouch.exe <nazwa pliku docelowego> <nazwa pliku źródłowego>
   ```

   Gdzie:

   - `<nazwa pliku docelowego>` to nazwa pliku Hot Fix, którego sygnatura czasowa ma zostać zmieniona
   - `<nazwa pliku źródłowego>` to nazwa pliku, którego sygnatura czasowa ma zostać skopiowana

   Uwaga

   Jeżeli nazwa pliku źródłowego nie zostanie określona, narzędzie ustawi sygnaturę czasową pliku docelowego zgodnie z czasem systemowym punktu końcowego. Użyj symbolu wieloznacznego * (gwiazdka) w przypadku pliku docelowego, ale nie pliku źródłowego.

5. Aby sprawdzić zmianę sygnatury czasowej, wpisz `dir` w wierszu polecenia lub sprawdź właściwości pliku w programie Eksplorator Windows.

Agenci aktualizacji

Aby przypisać zadanie instalowania składników, ustawień domeny, programów agenta oraz pakietów Hot Fix agentom OfficeScan, należy przydzielić niektórym agentom OfficeScan rolę agentów aktualizacji, czyli źródeł aktualizacji dla innych agentów. Dzięki temu agenci będą pobierać aktualizacje w odpowiednim czasie bez generowania nadmiernego ruchu sieciowego do serwera OfficeScan.

Jeśli sieć jest podzielona na segmenty według lokalizacji, a połączenie między segmentami jest obciążone dużym ruchem, należy ustanowić co najmniej jednego agenta lokalizacji w każdej lokalizacji.

Uwaga

Agenci OfficeScan wyznaczeni do aktualizacji składników z agenta aktualizacji otrzymują tylko zaktualizowane składniki i ustawienia z agenta aktualizacji. Wszyscy Agenci OfficeScan w dalszym ciągu zgłaszają swój stan do serwera OfficeScan.

Wymagania systemowe Agenta aktualizacji

Pełna lista wymagań systemowych jest dostępna pod adresem:

http://docs.trendmicro.com/pl-pl/enterprise/officescan.aspx

Konfiguracja Agenta aktualizacji

Konfiguracja agenta aktualizacji to proces dwuetapowy:

1. Wybierz agenta OfficeScan, który będzie pełnić rolę agenta aktualizacji określonych składników.
2. Wybierz agentów, którzy będą aktualizować składniki za pomocą tego agenta aktualizacji.

Uwaga

Liczba równoczesnych połączeń agentów, które mogą być obsługiwane przez jednego agenta aktualizacji, zależy od konfiguracji sprzętowej punktu końcowego.

Przydzielanie agentów OfficeScan jako agentów aktualizacji

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów wybierz agentów, którzy zostaną wyznaczeni jako agenci aktualizacji.

Uwaga

Nie jest możliwe wybranie ikony domeny głównej, ponieważ spowodowałoby to wyznaczenie wszystkich agentów jako agentów aktualizacji. Agent aktualizacji wykorzystujący wyłącznie protokół IPv6 nie umożliwia rozsyłania aktualizacji bezpośrednio do agentów wykorzystujących wyłącznie protokół IPv4. Analogicznie, agent aktualizacji wykorzystujący wyłącznie protokół IPv4 nie umożliwia rozsyłania aktualizacji bezpośrednio do agentów wykorzystujących wyłącznie protokół IPv6. Aby umożliwić agentowi aktualizacji rozsyłanie aktualizacji do agentów, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.

3. Kliknij polecenie **Ustawienia** > **Ustawienia agenta aktualizacji**.
4. Wybierz elementy, które mogą udostępniać agenty aktualizacji.
   - Aktualizacje składników
   - Ustawienia domeny
   - Programy i poprawki agenta OfficeScan
5. Kliknij przycisk **Zapisz**.

Określanie agentów OfficeScan, którzy pobierają aktualizację od agenta aktualizacji

Procedura

1. Przejdź do opcji **Aktualizacje** > **Agenci** > **Źródło aktualizacji**.
2. W sekcji **Lista niestandardowych źródeł aktualizacji** kliknij przycisk **Dodaj**.
3. Na wyświetlonym ekranie wpisz adresy IP agentów. Można wpisać zakres adresów IPv4 i/lub prefiks IPv6 i długość.
4. W polu **Agent aktualizacji** wybierz agenta aktualizacji, którego chcesz przydzielić agentom.

   Uwaga

   Upewnij się, że agenci mogą nawiązać połączenie z agentem aktualizacji przy użyciu swoich adresów IP. Jeśli na przykład określono zakres adresów IPv4, agent aktualizacji musi mieć adres IPv4. Jeśli określono prefiks IPv6 i długość, agent aktualizacji musi mieć adres IPv6.

5. Kliknij przycisk **Zapisz**.

Źródła aktualizacji dla agentów aktualizacji

Agenty aktualizacji mogą pobierać aktualizacje z różnych źródeł, takich jak serwer OfficeScan czy niestandardowe źródła aktualizacji. Źródło aktualizacji można skonfigurować w konsoli Web na ekranie Źródło aktualizacji.

Obsługa protokołu IPv6 dla agentów aktualizacji

Agent aktualizacji wykorzystujący wyłącznie protokół IPv6 nie może wykonywać aktualizacji bezpośrednio ze źródeł wykorzystujących wyłącznie protokół IPv4, takich jak:

- Serwer OfficeScan wykorzystujący wyłącznie protokół IPv4

- Dowolne niestandardowe źródło aktualizacji wykorzystujące wyłącznie protokół IPv4
- Trend Micro ActiveUpdate Server

Analogicznie, agent aktualizacji wykorzystujący wyłącznie protokół IPv4 nie może wykonywać aktualizacji bezpośrednio ze źródeł aktualizacji wykorzystujących wyłącznie protokół IPv6, takich jak serwer OfficeScan wykorzystujący wyłącznie protokół IPv6.

Aby umożliwić agentowi aktualizacji nawiązanie połączenia ze źródłami aktualizacji, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.

Standardowe źródła aktualizacji dla agentów aktualizacji

Standardowym źródłem aktualizacji agentów aktualizacji jest serwer OfficeScan. W przypadku skonfigurowania agentów do pobierania aktualizacji bezpośrednio z serwera OfficeScan proces aktualizacji przebiega następująco:

1. Agent aktualizacji pobiera aktualizacje z serwera OfficeScan.
2. Jeśli pobranie aktualizacji z serwera OfficeScan nie jest możliwe, agent próbuje się połączyć bezpośrednio z serwerem Trend Micro ActiveUpdate Server, jeśli są spełnione następujące warunki:
   - W **Agenci** > **Zarządzanie agentami** kliknij opcję **Ustawienia** > **Uprawnienia i inne ustawienia** > **Inne ustawienia** > **Ustawienia aktualizacji**, opcja **Agenci OfficeScan pobierają aktualizacje z serwera Trend Micro ActiveUpdate Server** jest włączona.
   - Serwer ActiveUpdate stanowi pierwszy wpis na liście niestandardowych źródeł aktualizacji.

Porada

Serwer ActiveUpdate należy umieścić na samej górze listy, tylko jeśli występują problemy z pobieraniem aktualizacji z serwera OfficeScan. Gdy agenty aktualizacji pobierają aktualizacje bezpośrednio z serwera ActiveUpdate, łącze między siecią a Internetem jest bardzo obciążone.

3. Jeśli nie można pobrać aktualizacji z żadnego dostępnego źródła, agent aktualizacji zatrzymuje proces aktualizacji.

Niestandardowe źródła aktualizacji dla agentów aktualizacji

Agenty aktualizacji mogą pobierać aktualizacje nie tylko z serwera OfficeScan, lecz również z niestandardowych źródeł aktualizacji. Niestandardowe źródła aktualizacji ograniczają ruch sieciowy związany z przesyłaniem aktualizacji agenta na serwer OfficeScan. Informacje o niestandardowych źródłach aktualizacji są przechowywane na liście niestandardowych źródeł aktualizacji, która może zawierać maksymalnie 1024 wpisy. Opis poszczególnych etapów konfiguracji listy znajduje się w *Niestandardowe źródło aktualizacji dla agentów OfficeScan na stronie 6-35*.

Uwaga

Upewnij się, że opcja **Aktualizacja składników aktualizacji agentów, ustawień domeny oraz agentów i poprawek; wyłącznie z serwera OfficeScan** jest wyłączona na ekranie **Źródło aktualizacji agentów** (**Aktualizacje** > **Agenci** > **Źródło aktualizacji**), aby agenci aktualizacji mogli łączyć się z niestandardowymi źródłami aktualizacji.

Po skonfigurowaniu i zapisaniu listy proces aktualizacji przebiega następująco:

1. Agent aktualizacji pobiera aktualizacje z pierwszej pozycji listy.
2. Jeśli pobranie aktualizacji z pierwszej pozycji nie jest możliwe, agent pobiera aktualizacje z drugiej pozycji itd.
3. Jeśli nie można pobrać aktualizacji z żadnego źródła określonego na liście, agent sprawdza następujące opcje pod nagłówkiem **Agenci OfficeScan aktualizują następujące składniki z serwera OfficeScan, jeśli wszystkie niestandardowe źródła są niedostępne lub nie zostały odnalezione**:

    - **Składniki**: Jeśli ta opcja jest włączona, agent pobiera aktualizacje z serwera OfficeScan.

      Jeśli ta opcja jest wyłączona, agent próbuje połączyć się bezpośrednio z serwerem Trend Micro ActiveUpdate Server, ale z uwzględnieniem następujących warunków:

Uwaga

Składniki można aktualizować tylko z serwera Active Update. Ustawienia domeny, programy i pakiety hot fix można pobierać tylko z serwera lub agentów aktualizacji.

- W **Agenci** > **Zarządzanie agentami** kliknij opcję **Ustawienia** > **Uprawnienia i inne ustawienia** > **Inne ustawienia** > **Ustawienia aktualizacji**, opcja **Agenci pobierają aktualizacje z serwera Trend Micro ActiveUpdate Server** jest włączona.
- Serwer ActiveUpdate nie znajduje się na liście niestandardowych źródeł aktualizacji.

- **Ustawienia domeny**: Jeśli ta opcja jest włączona, agent pobiera aktualizacje z serwera OfficeScan.
- **Programy i poprawki agenta OfficeScan**: Jeśli ta opcja jest włączona, agent pobiera aktualizacje z serwera OfficeScan.

4. Jeśli nie można pobrać aktualizacji z żadnego dostępnego źródła, agent aktualizacji zatrzymuje proces aktualizacji.

Proces aktualizacji przebiega inaczej, jeśli jest włączona opcja **Standardowe źródło aktualizacji (aktualizacja z serwera OfficeScan)**, a serwer OfficeScan powiadamia agenta o konieczności aktualizacji składników. Proces przebiega następująco:

1. Agent pobiera aktualizacje bezpośrednio z serwera OfficeScan, ignorując listę źródeł aktualizacji.
2. Jeśli pobranie aktualizacji z serwera nie jest możliwe, agent próbuje się połączyć bezpośrednio z serwerem Trend Micro ActiveUpdate Server, jeśli są spełnione następujące warunki:

   - W **Agenci** > **Zarządzanie agentami** kliknij opcję **Ustawienia** > **Uprawnienia i inne ustawienia** > **Inne ustawienia** > **Ustawienia aktualizacji**, opcja **Agenci OfficeScan pobierają aktualizacje z serwera Trend Micro ActiveUpdate Server** jest włączona.
   - Serwer ActiveUpdate stanowi pierwszy wpis na liście niestandardowych źródeł aktualizacji.

Porada

Serwer ActiveUpdate należy umieścić na samej górze listy, tylko jeśli występują problemy z pobieraniem aktualizacji z serwera OfficeScan. Gdy Agenci OfficeScan pobierają aktualizacje bezpośrednio z serwera ActiveUpdate, łącze między siecią a Internetem jest bardzo obciążone.

3. Jeśli nie można pobrać aktualizacji z żadnego dostępnego źródła, agent aktualizacji zatrzymuje proces aktualizacji.

Konfigurowanie źródła aktualizacji dla agenta aktualizacji

Procedura

1. Przejdź do opcji **Aktualizacje** > **Agenci** > **Źródło aktualizacji**.
2. Ustal, czy aktualizacje mają być pobierane ze standardowego źródła aktualizacji dla agentów aktualizacji (z serwera OfficeScan) czy z niestandardowego źródła aktualizacji dla agentów aktualizacji.
3. Kliknij polecenie **Powiadom wszystkich agentów**.

Duplikacja składnika agenta aktualizacji

Agenci aktualizacji, podobnie jak serwer OfficeScan, także korzystają z procedury duplikowania składników podczas pobierania. W *Duplikacja składników serwera OfficeScan na stronie 6-22* można znaleźć więcej informacji na temat sposobów powielania składników przez serwer.

Proces duplikacji składników agentów aktualizacji przebiega następująco:

1. Agent aktualizacji porównuje swoją bieżącą kompletną wersję wzorca sygnatur z najnowszą wersją dostępną w źródle aktualizacji. Jeśli różnica między obiema wersjami wynosi 14 lub mniej, agent aktualizacji pobiera przyrostowy wzorzec sygnatur, który odpowiada różnicy między obiema wersjami.

Uwaga

Jeśli różnica jest większa niż 14, agent aktualizacji automatycznie pobiera pełną wersję pliku sygnatur.

2. Agent aktualizacji scala pobrany przyrostowy wzorzec sygnatur ze swoim bieżącym kompletnym wzorcem sygnatur, aby utworzyć najnowszy kompletny wzorzec sygnatur.
3. Agent aktualizacji pobiera pozostałe przyrostowe wzorce sygnatur ze źródła aktualizacji.
4. Najnowszy kompletny wzorzec sygnatur i wszystkie przyrostowe wzorce sygnatur zostają udostępnione agentom.

Metody aktualizacji za pomocą Agentów aktualizacji

Agenci aktualizacji korzystają z takich samych metod aktualizacji, jakie są dostępne dla zwykłych agentów. Szczegółowe informacje zawiera sekcja *Metody aktualizacji agenta OfficeScan na stronie 6-39*.

Jeśli agent aktualizacji został zainstalowany za pomocą narzędzia Agent Packager, zaplanowane aktualizacje można włączyć i skonfigurować za pomocą Narzędzia konfiguracji zaplanowanej aktualizacji.

Uwaga

To narzędzie nie jest dostępne, jeśli agenta aktualizacji zainstalowano za pomocą innej metody. Patrz *Uwagi dotyczące instalacji na stronie 5-13* Aby uzyskać więcej informacji.

Korzystanie z narzędzia konfiguracji zaplanowanej aktualizacji

Procedura

1. Na punkcie końcowym agenta aktualizacji przejdź do lokalizacji <*Folder instalacji agenta*>.

2. Kliknij dwukrotnie plik `SUCTool.exe`, aby uruchomić narzędzie. Zostanie otwarta konsola Narzędzie konfiguracji zaplanowanej aktualizacji.
3. Wybierz polecenie **Włącz zaplanowaną aktualizację**.
4. Określ częstotliwość oraz datę i godzinę przeprowadzania aktualizacji.
5. Kliknij **Zastosuj**.

Raport analityczny agenta aktualizacji

Można wygenerować raport analityczny agenta aktualizacji, aby przeprowadzić analizę infrastruktury aktualizacji oraz ustalić, którzy agenci pobierają aktualizacje częściowe z agentów aktualizacji i innych źródeł aktualizacji.

Uwaga

W tym raporcie uwzględnieni są wszyscy Agenci OfficeScan skonfigurowani do odbierania częściowych aktualizacji od agentów aktualizacji. Jeśli zadanie zarządzania jedną lub kilkoma domenami zostało przekazane innym administratorom, wszyscy Agenci OfficeScan skonfigurowani do odbierania częściowych aktualizacji od agentów aktualizacji należących do zarządzanych przez nich domen będą widoczni również dla nich.

Program OfficeScan eksportuje Raport analityczny agenta aktualizacji do pliku rozdzielanego przecinkami (`.csv`).

Raport ten zawiera następujące informacje:

- Agent OfficeScan punkt końcowy
- Adres IP
- Ścieżka drzewa agentów
- Źródło aktualizacji
- Jeśli agenci pobierają z agentów aktualizacji następujące elementy:
    - Składniki

- Ustawienia domeny
- Programy i pakiety Hot Fix agenta OfficeScan

Ważne

Raport analityczny agenta aktualizacji uwzględnia tylko agentów OfficeScan skonfigurowanych do odbierania częściowych aktualizacji od agenta aktualizacji. Agenci OfficeScan, którzy zostali skonfigurowani do odbierania częściowych aktualizacji od agenta aktualizacji (łącznie ze składnikami, ustawieniami domeny oraz programami agenta OfficeScan i pakietami Hot Fix), nie są wyświetlani w raporcie.

Szczegółowe informacje dotyczące generowania raportu zawiera temat *Niestandardowe źródło aktualizacji dla agentów OfficeScan na stronie 6-35*.

Podsumowanie aktualizacji składników

Konsola Web zapewnia dostęp do ekranu **Podsumowanie aktualizacji** (opcja **Aktualizacje** > **Podsumowanie**), który zawiera informacje o ogólnym stanie aktualizacji składników oraz umożliwia aktualizację nieaktualnych składników. Jeśli są włączone zaplanowane aktualizacje serwera, na tym ekranie jest również widoczny harmonogram kolejnych aktualizacji.

Aby mieć dostęp do najnowszych informacji dotyczących stanu aktualizacji składników, należy okresowo odświeżać ekran.

Uwaga

Aby wyświetlić informacje o aktualizacjach składników na zintegrowanym serwerze Smart Protection, przejdź do opcji **Administracja** > **Smart Protection** > **Zintegrowany serwer**.

Stan aktualizacji agentów OfficeScan

Jeśli zainicjowano aktualizację składników na agentach, w tej sekcji można wyświetlić następujące informacje:

- Liczba agentów powiadomionych o aktualizacji składników.
- Liczba agentów jeszcze niepowiadomionych, ale będących w kolejce do powiadomienia. Aby anulować powiadomienia tych agentów, kliknij przycisk **Anuluj powiadomienie**.

Składniki

W tabeli **Stan aktualizacji** są widoczne stany aktualizacji poszczególnych składników pobieranych i rozpowszechnianych przez serwer OfficeScan.

W przypadku każdego składnika można wyświetlić jego bieżącą wersję i datę ostatniej aktualizacji. Można również wyświetlić agentów z nieaktualnymi składnikami, klikając łącze z numerem. Agentów z nieaktualnymi składnikami można następnie ręcznie zaktualizować.

Rozdział 7

Skanowanie w poszukiwaniu zagrożeń bezpieczeństwa

W tym rozdziale przedstawiono sposób ochrony punktów końcowych przed zagrożeniami bezpieczeństwa przy użyciu skanowania opartego na plikach.

Rozdział składa się z następujących tematów:

Zagrożenia bezpieczeństwa — informacje

Zagrożenie bezpieczeństwa to ogólne pojęcie określające wirusy/złośliwe oprogramowanie oraz oprogramowanie spyware/grayware. W celu ochrony punktów końcowych przed zagrożeniami program OfficeScan skanuje pliki i wykonuje określone czynności przy każdym wykrytym zagrożeniu bezpieczeństwa. Bardzo duża liczba zagrożeń bezpieczeństwa wykrytych w krótkim przedziale czasu sugeruje epidemię. Program OfficeScan może powstrzymać epidemię, stosując reguły ochrony przed epidemią i izolując zarażone punkty końcowe, aż do ich całkowitego wyleczenia. W celu zapewnienia możliwości podejmowania natychmiastowych działań można śledzić zagrożenia bezpieczeństwa i alerty za pomocą powiadomień i dzienników.

Wirusy i złośliwe oprogramowanie

Istnieją dziesiątki tysięcy wirusów i złośliwych programów, a z każdym dniem ich przybywa. O ile w przeszłości wirusy komputerowe najczęściej występowały w systemach DOS lub Windows, dziś mogą powodować poważne szkody, wykorzystując słabości sieci korporacyjnych, systemów pocztowych i witryn internetowych.

TABELA 7-1. Rodzaje wirusów/złośliwych programów

TYP WIRUSA/ ZŁOŚLIWEGO OPROGRAMO WANIA	OPIS
Program-żart	Programy-żarty to podobne do wirusów programy, które często zmieniają wygląd elementów wyświetlanych na monitorze punktu końcowego.
Inne	“Inne” dotyczy wirusów i złośliwych programów nieskategoryzowanych jako żaden z rodzajów wirusów lub złośliwego oprogramowania.
Narzędzie do kompresji	Samorozpakowujące się archiwum to skompresowany i (lub) zaszyfrowany program wykonywalny systemu Windows lub Linux™, często trojan. Kompresja plików wykonywalnych utrudnia wykrywanie wirusów przez programy antywirusowe.

Typ wirusa/ złośliwego oprogramowania	Opis
Oprogramowanie typu rootkit	Oprogramowanie typu rootkit to program (lub zbiór programów), który instaluje w systemie kod i wykonuje go bez zgody i wiedzy użytkownika. Wykorzystuje mechanizmy maskujące, które umożliwiają stałą obecność na komputerze, niemożliwą do wykrycia. Programy typu rootkit nie zarażają komputerów, lecz raczej stanowią niewykrywalne środowisko pozwalające wykonywać złośliwy kod. Programy typu rootkit są instalowane z wykorzystaniem metod inżynierii społecznej, w wyniku uruchomienia złośliwego oprogramowania lub po prostu podczas przeglądania złośliwych witryn sieci Web. Po zainstalowaniu osoba atakująca może wykonywać w systemie niemal każdą funkcję, w tym m.in. zdalny dostęp, podsłuchiwanie, jak również ukrywanie procesów, plików, kluczy rejestru i kanałów komunikacji.
Wirus testowy	Wirus testowy to obojętny plik, który działa jak prawdziwy wirus i jest wykrywalny przez oprogramowanie antywirusowe. Do sprawdzania, czy zainstalowane oprogramowanie antywirusowe prawidłowo wykonuje skanowanie, można używać wirusów testowych, takich jak skrypt testowy EICAR.
Koń trojański	Trojany często wykorzystują porty, aby uzyskać dostęp do komputerów lub programów wykonywalnych. Programy typu „koń trojański” nie replikują się, lecz rezydują w systemach, aby prowadzić złośliwe działania, np. otwierać porty w celu umożliwienia ingerencji hakerom. Tradycyjne programy antywirusowe potrafią wykryć i usunąć wirusy, lecz nie trojany, szczególnie te, które są już aktywne w systemie.

Typ wirusa/ złośliwego oprogramowania	Opis
Wirus	Wirusy to programy powielające się. W tym celu wirus musi dołączyć się do innych plików programów i jest wykonywany po uruchomieniu programu, do którego jest dołączony, m.in.: • **Szkodliwy kod formantu ActiveX**: kod rezydujący na stronach internetowych korzystających z formantów ActiveX™. • **Wirus sektora rozruchowego**: wirus, który zaraża sektor rozruchowy partycji lub dysku. • **Zarażające pliki COM i EXE**: Programy wykonywalne z rozszerzeniami `.com` i `.exe`. • **Szkodliwy kod Java**: Niezależny od systemu operacyjnego kod wirusa, napisany lub osadzony w języku Java™. • **Wirus makr**: wirus zakodowany jako makro aplikacji i często dołączony do dokumentów. • Wirus **VBScript**, **JavaScript** lub **HTML**: wirus rezydujący na stronach internetowych i pobierany przez przeglądarkę. • **Robak**: Niezależny program lub zestaw programów, zdolny do rozpowszechniania swoich działających kopii lub ich segmentów na innych komputerach, często za pośrednictwem poczty e-mail.
Wirus sieciowy	Wirus rozpowszechniający się przez sieć nie jest, ściśle rzecz biorąc, wirusem sieciowym. Jedynie kilka typów wirusów / złośliwego oprogramowania, takich jak robaki, jest zaliczanych do wirusów sieciowych. Wirusy sieciowe używają do replikacji protokołów sieciowych, takich jak TCP, FTP, UDP, HTTP, i protokołów e-mail. Często nie zmieniają one plików systemowych czy sektorów rozruchowych twardych dysków. Wirusy sieciowe zarażają natomiast pamięć komputerów, zmuszając je do obciążenia sieci ruchem, który może spowodować opóźnienia, a nawet awarię sieci. Ponieważ wirusy sieciowe pozostają w pamięci, często są niewykrywalne przez konwencjonalne metody skanowania plików działające na zasadzie badania danych wejściowych i wyjściowych.

TYP WIRUSA/ ZŁOŚLIWEGO OPROGRAMOWANIA	OPIS
Możliwy wirus/ złośliwe oprogramowanie	Możliwe wirusy/złośliwe oprogramowanie to podejrzane pliki mające niektóre cechy charakterystyczne dla wirusa/złośliwego oprogramowania. Szczegółowe informacje zawiera Encyklopedia zagrożeń firmy Trend Micro: http://about-threats.trendmicro.com/us/threatencyclopedia#malware **Uwaga** Operacji czyszczenia nie można przeprowadzać na prawdopodobnym wirusie/złośliwym oprogramowaniu, ale można konfigurować tę operację skanowania.

Oprogramowanie spyware i grayware

Zagrożeniem dla urządzeń typu Punkty końcowe są nie tylko wirusy/złośliwe oprogramowanie. Nazwa spyware/grayware odnosi się do aplikacji lub plików niesklasyfikowanych jako wirusy lub trojany, lecz mogących mieć negatywny wpływ na wydajność urządzeń typu punkty końcowe w sieci i wprowadzających znaczne ryzyko naruszenia bezpieczeństwa, poufności i prawa w organizacji. Oprogramowanie typu spyware/grayware często wykonuje niepożądane i niebezpieczne operacje wpływające na pracę użytkownika, takie jak wyświetlanie wyskakujących okienek, rejestrowanie naciśnięć klawiszy czy narażenie urządzenia typu punkt końcowy na atak.

W przypadku znalezienia aplikacji lub pliku niewykrywanego przez program OfficeScan jako oprogramowanie grayware, ale mogącego być typem oprogramowania grayware, plik lub aplikację należy przesłać do firmy Trend Micro, korzystając z poniższego adresu:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Typ	Opis
Spyware	gromadzi dane, takie jak nazwy kont użytkowników i hasła, a następnie przysyła je do osób trzecich.
Adware	wyświetlają reklamy i gromadzą dane, takie jak preferencje dotyczące przeglądanych witryn Web, w celu kierowania do użytkownika reklam za pomocą przeglądarki internetowej.
Moduł telefoniczny	Zmieniają ustawienia internetowe urządzenia typu punkt końcowy i mogą wymusić wybieranie wstępnie określonych numerów telefonu przez modem urządzenia typu punkt końcowy. Są to zazwyczaj numery typu „pay-per-call” lub numery międzynarodowe, połączenie przez nie oznacza dla organizacji znaczne koszty.
Program-żart	Powoduje nietypowe zachowanie urządzenia typu punkt końcowy, takie jak zamykanie i otwieranie tacy napędu CD-ROM lub wyświetlanie licznych okien komunikatów.
Narzędzie hakerskie	ułatwia hakerom uzyskiwanie dostępu do komputerów.
Narzędzie zdalnego dostępu	ułatwia hakerom uzyskiwanie dostępu do komputerów i przejmowanie nad nimi kontroli.
Aplikacja do łamania haseł	ułatwia hakerom rozszyfrowywanie nazw kont i haseł użytkowników.
Inne	inne typy potencjalne złośliwych programów.

Jak oprogramowanie spyware/grayware dostaje się do sieci

Programy spyware/grayware często dostają się do sieci firmowej, gdy użytkownicy pobierają legalne programy, które zawierają aplikacje grayware dołączone do pakietu instalacyjnego. Większość oprogramowania zawiera Umowę Licencyjną Użytkownika Końcowego Oprogramowania (EULA), którą należy zaakceptować przed rozpoczęciem pobierania. Umowa licencyjna użytkownika końcowego oprogramowania (EULA) zawiera często informacje na temat takiej aplikacji i jej przeznaczenia do gromadzenia danych osobistych, jednak użytkownicy zazwyczaj nie zauważają tego typu informacji lub nie rozumieją używanego w takich przypadkach prawniczego żargonu.

Potencjalne ryzyko oraz zagrożenia

Obecność oprogramowania spyware i innych typów grayware w sieci może mieć następujące skutki:

TABELA 7-2. Potencjalne ryzyko oraz zagrożenia

RYZYKO LUB ZAGROŻENIE	OPIS
Zmniejszenie wydajności punktu końcowego	W celu realizacji swoich funkcji aplikacje spyware/grayware często nadmiernie wykorzystują zasoby procesora i pamięci systemowej.
Zwiększenie częstotliwości awarii związanych z przeglądarką sieci Web	Niektóre typy oprogramowania grayware, takie jak adware, często wyświetlają informacje w ramce lub oknie przeglądarki. W zależności od tego, jak kod aplikacji wpływa na procesy systemowe, aplikacje typu grayware mogą czasami powodować awarie przeglądarki lub blokować ją, w wyniku czego konieczne może być ponowne uruchomienie punktu końcowego.
Zmniejszenie wydajności pracy użytkownika	Z uwagi na konieczność zamykania często wyskakujących okienek reklamowych i reagowania na negatywne efekty programów-żartów użytkownicy są niepotrzebnie odrywani od swoich podstawowych zadań i obowiązków.
Zmniejszenie przepustowości sieci	Aplikacje spyware/grayware często regularnie przesyłają gromadzone dane do innych aplikacji uruchomionych w sieci lub poza nią.
Utrata informacji osobistych i firmowych	Nie wszystkie dane gromadzone przez aplikacje spyware i grayware są tak nieszkodliwe, jak lista odwiedzonych przez użytkownika witryn internetowych. Programy spyware/grayware mogą także gromadzić poświadczenia użytkowników w celu uzyskania dostępu do kont bankowych i sieci firmowych.
Wyższe ryzyko odpowiedzialności prawnej	W przypadku przejęcia zasobów punktu końcowego w sieci hakerzy mogą mieć możliwość wykorzystania komputerów agenta w celu przeprowadzenia ataków na komputery znajdujące się poza siecią lub w celu zainstalowania na nich oprogramowania spyware/grayware. Udział zasobów sieci firmowej w tego typu działaniach może narazić firmę na odpowiedzialność prawną w zakresie szkód spowodowanych przez osoby trzecie.

Ochrona przed oprogramowaniem spyware/grayware i innymi zagrożeniami

Istnieje wiele sposobów na to, aby zapobiec instalacji oprogramowania spyware/grayware na urządzeniu typu punkt końcowy. Firma Trend Micro zaleca przestrzeganie następujących zasad:

- Skonfiguruj wszystkie typy skanowania (Skanowanie ręczne, Skanowanie w czasie rzeczywistym, Skanowanie zaplanowane oraz Skanuj teraz), aby wyszukiwać oraz usuwać pliki i aplikacje spyware i inne typy grayware. Patrz *Rodzaje skanowania na stronie 7-15* Aby uzyskać więcej informacji.
- Należy poinformować użytkowników urządzeń typu agent o konieczności wykonywania następujących czynności:
  - Czytanie Umowy Licencyjnej Użytkownika Oprogramowania (EULA) i dokumentacji dołączonej do pobieranych i instalowanych aplikacji.
  - Klikanie przycisku **Nie** we wszystkich monitach o autoryzację pobierania i instalowania oprogramowania, chyba że użytkownicy urządzeń typu agent ufają twórcy oprogramowania i wyświetlanej witryny internetowej.
  - Odrzucanie niezapowiedzianej, komercyjnej poczty e-mail (spamu), szczególnie jeśli w treści wiadomości znajduje się prośba o kliknięcie przycisku lub łącza.
- Ustawienia zabezpieczeń przeglądarki sieci Web powinny być skonfigurowane tak, aby zapewniać wysoki poziom ochrony. Firma Trend Micro zaleca ustawienie w przeglądarkach internetowych opcji wyświetlania monitów przed instalowaniem formantów ActiveX.
- Jeśli używany jest program Microsoft Outlook, należy tak skonfigurować ustawienia zabezpieczeń, aby program Outlook nie pobierał automatycznie elementów HTML, takich jak obrazy wysyłane w spamie.
- Zabronienie udostępniania plików za pomocą usług i oprogramowania peer-to-peer. Aplikacje spyware i grayware mogą być maskowane jako inne typy plików pobieranych przez użytkowników, takich jak pliki muzyczne MP3.
- Należy okresowo sprawdzać oprogramowanie zainstalowane na komputerach agentach i wyszukiwać aplikacje, które mogą być programami spyware lub innym typem grayware.

- Aktualizowanie systemów operacyjnych Windows za pomocą najnowszych poprawek z firmy Microsoft. Szczegółowe informacje można znaleźć w witrynie internetowej firmy Microsoft.

Typy metod skanowania

Agenci OfficeScan podczas skanowania zagrożeń bezpieczeństwa mogą korzystać z dwóch metod skanowania: skanowania Smart Scan i skanowania standardowego.

- **Smart Scan**

  Agenci, którzy używają skanowania Smart Scan, są w tym dokumencie nazywani **agentami Smart Scan**. Agenci Smart Scan korzystają z funkcji skanowania lokalnego i zapytań w chmurze obsługiwanych przez usługi File Reputation Services.

- **Skanowanie standardowe**

  Agenci, którzy nie używają skanowania Smart Scan, są nazywani **agentami skanowania standardowego**. Agent skanowania standardowego zapisuje wszystkie składniki programu OfficeScan na punkcie końcowym agenta i skanuje wszystkie pliki lokalnie.

Domyślna metoda skanowania

Domyślna metoda skanowania w tej wersji OfficeScan w przypadku nowych instalacji to Smart Scan. Oznacza to, że po wykonaniu nowej instalacji serwera OfficeScan bez zmiany metody skanowania w konsoli Web na wszystkich agentach obsługiwanych przez serwer zostanie zastosowana metoda Smart Scan.

W przypadku uaktualnienia serwera OfficeScan z wcześniejszej wersji i po włączeniu automatycznego uaktualnienia agenta na wszystkich agentach obsługiwanych przez ten serwer zostanie zastosowana metoda skanowania ustawiona przed uaktualnieniem. Na przykład w przypadku uaktualnienia z programu OfficeScan 11.0, który obsługuje skanowanie Smart Scan i skanowanie standardowe, wszyscy uaktualnieni agenci Smart Scan będą w dalszym ciągu używać skanowania Smart Scan, podczas gdy wszyscy agenci skanowania standardowego będą kontynuować użycie skanowania standardowego.

Porównanie metod skanowania

Poniższa tabela przedstawia porównanie tych dwóch metod skanowania:

TABELA 7-3. Porównanie skanowania standardowego i skanowania Smart Scan

PODSTAWA PORÓWNANIA	SKANOWANIE STANDARDOWE	SMART SCAN
Dostępność	Dostępne w tej i wszystkich poprzednich wersjach programu OfficeScan	Możliwe uruchomienia w OfficeScan 10
Zachowanie skanowania	Skanowanie jest wykonywane przez agenta skanowania standardowego na lokalnym punkcie końcowym.	• Skanowanie jest wykonywane przez agenta skanowania Smart Scan na lokalnym punkcie końcowym. • Jeśli w trakcie skanowania agent nie może określić ryzyka, jest ono sprawdzane przez agenta przez przesłanie zapytania o skanowanie do źródła programu Smart Protection. • Agent „buforuje” wynik zapytania o skanowanie, aby zwiększyć wydajność skanowania.
Używane i aktualizowane składniki	Wszystkie elementy dostępne w źródle aktualizacji poza sygnatura Agenta Smart Scan.	Wszystkie składniki dostępne w źródle aktualizacji poza sygnaturą wirusa i sygnaturą aktywnego monitorowania oprogramowania spyware.
Typowe źródło aktualizacji	Serwer OfficeScan	Serwer OfficeScan

Zmiana metody skanowania

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Ustawienia skanowania** > **Metody skanowania**.
4. Wybierz opcję **Skanowanie standardowe** lub **Smart Scan**.
5. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Przełączanie ze skanowania Smart Scan na skanowanie standardowe

Podczas przełączania agentów na skanowanie standardowe należy wziąć pod uwagę następujące kwestie:

1. Liczba przełączanych agentów

   W celu zapewnienia optymalnego wykorzystania zasobów serwera OfficeScan i serwera Smart Protection jednorazowo należy przełączać względnie małą liczbę agentów. Podczas przełączania metody skanowania agentów serwery takie mogą wykonywać inne ważne zadania.

2. Synchronizacja

   Podczas ponownego przełączania na skanowanie standardowe agenci będą prawdopodobnie pobierać z serwera OfficeScan pełną wersję sygnatury wirusów oraz sygnaturę aktywnego monitorowania oprogramowania spyware. Te pliki sygnatur są używane wyłącznie w przypadku agentów skanowania standardowego.

   Należy wziąć pod uwagę, że pobieranie będzie trwać krócej, jeśli zostanie wykonane poza godzinami największego ruchu w sieci. Pod uwagę należy również wziąć wybranie takiego momentu przełączenia, podczas którego żaden agent nie będzie pobierać z serwera zaplanowanych aktualizacji. Należy również tymczasowo wyłączyć na agentach dostęp do funkcji „Aktualizuj teraz", a następnie ponownie go umożliwić po przełączeniu agentów na skanowanie Smart Scan.

3. Ustawienia drzewa agentów

   Metoda skanowania to szczegółowe ustawienie, które można skonfigurować na poziomie głównym, domeny oraz indywidualnego agenta. Podczas przełączania na skanowanie standardowe można:

   - Można utworzyć nową domenę drzewa agentów i jako metodę skanowania wybrać skanowanie standardowe. Każdy agent przeniesiony do tej domeny będzie korzystać ze skanowania standardowego. Podczas przenoszenia agenta można włączyć ustawienie **Zastosuj ustawienia nowej domeny do wybranych agentów**.
   - wybrać domenę i skonfigurować ją do korzystania ze skanowania standardowego. Agenci Smart Scan należący do tej domeny przełączą się na skanowanie standardowe.
   - Można wybrać jednego lub kilku agentów Smart Scan z domeny i przełączyć ich na skanowanie standardowe.

Uwaga

Wszelkie zmiany metody skanowania elementów domeny zastępują metodę skanowania skonfigurowaną na poszczególnych agentach.

Przełączanie ze skanowania standardowego na skanowanie Smart Scan

Podczas przełączania agentów ze skanowania standardowego na skanowanie Smart Scan należy upewnić się, że skonfigurowano usługi Smart Protection.

Szczegółowe informacje zawiera sekcja *Konfigurowanie usług Smart Protection na stronie 4-13*.

Poniższa tabela przedstawia inne uwagi dotyczące przełączania na skanowanie Smart Scan.

TABELA 7-4. Uwagi dotyczące przełączania na skanowanie Smart Scan

UWAGA	SZCZEGÓŁY
Licencja produktu	W celu korzystania ze skanowania Smart Scan należy się upewnić, że aktywowano licencje poniższych usług oraz że nie są one przeterminowane: • Antywirus • Usługi Web Reputation i Anti-spyware
Serwer OfficeScan	Należy się upewnić, że agenci mogą się połączyć z serwerem OfficeScan. O przejściu na skanowanie Smart Scan są powiadamiani wyłącznie agenci online. Agenci offline otrzymają powiadomienie po przejściu do trybu online. Agenci w trybie niezależnym są powiadamiani, gdy przejdą do trybu online lub, jeśli mają uprawnienia do zaplanowanych aktualizacji, gdy zostanie przeprowadzona aktualizacja zaplanowana. Ponieważ agenci Smart Scan muszą pobierać z serwera sygnaturę Smart Scan Agent Pattern, należy się również upewnić, że serwer OfficeScan zawiera najnowsze składniki. Aby zaktualizować składniki, patrz: *Aktualizacje serwera OfficeScan na stronie 6-16*.
Liczba przełączanych agentów	W celu zapewnienia optymalnego wykorzystania zasobów serwera OfficeScan jednorazowo należy przełączać względnie małą liczbę agentów. Podczas przełączania metody skanowania agentów serwer OfficeScan może wykonywać inne ważne zadania.

Uwaga	Szczegóły
Synchronizacja	Podczas pierwszego przełączania na skanowanie Smart Scan agenci muszą pobrać z serwera OfficeScan pełną wersję sygnatury Smart Scan Agent Pattern. Sygnatura Smart Scan Pattern jest używana wyłącznie przez agentów Smart Scan. Należy wziąć pod uwagę, że pobieranie będzie trwać krócej, jeśli zostanie wykonane poza godzinami największego ruchu w sieci. Pod uwagę należy również wziąć wybranie takiego momentu przełączenia, podczas którego żaden agent nie będzie pobierać z serwera zaplanowanych aktualizacji. Należy również tymczasowo wyłączyć na agentach dostęp do funkcji „Aktualizuj teraz”, a następnie ponownie go umożliwić po przełączeniu agentów na skanowanie Smart Scan.
Ustawienia drzewa agentów	Metoda skanowania to szczegółowe ustawienie, które można skonfigurować na poziomie głównym, domeny oraz indywidualnego agenta. Podczas przełączania na skanowanie Smart Scan można: • utworzyć nową domenę drzewa agentów i jako metodę skanowania wybrać Smart Scan. Każdy agent przeniesiony do tej domeny będzie korzystać ze skanowania Smart Scan. podczas przenoszenia agenta można włączyć ustawienie **Zastosuj ustawienia nowej domeny do wybranych agentów**. • wybrać domenę i skonfigurować ją do korzystania ze skanowania Smart Scan. Agenci skanowania standardowego należący do tej domeny przełączą się na skanowanie Smart Scan. • wybrać jednego lub wielu agentów skanowania standardowego z domeny i przełączyć ich na skanowanie Smart Scan. **Uwaga** Wszelkie zmiany metody skanowania elementów domeny zastępują metodę skanowania skonfigurowaną na poszczególnych agentach.

Uwaga	Szczegóły
Obsługa IPv6	Agenci Smart Scan mogą wysyłać żądania skanowania do źródeł Smart Protection. Agent Smart Scan wykorzystujący wyłącznie protokół IPv6 nie może wysyłać żądań bezpośrednio do źródeł wykorzystujących wyłącznie protokół IPv4, takich jak: • Serwer Smart Protection 2.0 (zintegrowany lub oddzielny) **Uwaga** Obsługa protokołu IPv6 została wprowadzona w wersji 2.5 serwera Smart Protection. • Trend Micro Smart Protection Network Analogicznie, agent Smart Scan wykorzystujący wyłącznie protokół IPv4 nie może wysyłać żądań bezpośrednio do serwerów Smart Protection wykorzystujących wyłącznie protokół IPv6. Aby umożliwić agentom Smart Scan nawiązanie połączenia ze źródłami, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.

Rodzaje skanowania

Program OfficeScan w celu ochrony komputerów Agent OfficeScanów przed zagrożeniami bezpieczeństwa zapewnia funkcje skanowania następujących typów:

Tabela 7-5. Rodzaje skanowania

Typ skanowania	Opis
Skanowanie w czasie rzeczywistym	Automatyczne skanowanie plików na punkcie końcowym po ich odebraniu, otwarciu, pobraniu, skopiowaniu lub zmodyfikowaniu. Szczegółowe informacje można znaleźć w części *Skanowanie w czasie rzeczywistym na stronie 7-16*.

Typ skanowania	Opis
Skanowanie ręczne	Inicjowane przez użytkownika skanowanie pliku lub zestawu plików Szczegółowe informacje można znaleźć w części *Skanowanie ręczne na stronie 7-19*.
Skanowanie zaplanowane	Automatyczne skanowanie plików na punkcie końcowym zgodnie z harmonogramem ustalonym przez administratora lub użytkownika.<--punkt końcowy--> Szczegółowe informacje można znaleźć w części *Skanowanie zaplanowane na stronie 7-22*.
Skanuj teraz	Inicjowane przez administratora skanowanie plików przechowywanych na jednym lub wielu komputerach docelowych. Szczegółowe informacje można znaleźć w części *Skanuj teraz na stronie 7-25*.

Skanowanie w czasie rzeczywistym

Skanowanie w czasie rzeczywistym zapewnia stałą ochronę. Zawsze gdy plik jest odbierany, otwierany, pobierany, kopiowany i modyfikowany, następuje skanowanie w czasie rzeczywistym w poszukiwaniu zagrożeń bezpieczeństwa. Jeśli program OfficeScan nie wykryje zagrożenia bezpieczeństwa, plik pozostaje w swojej lokalizacji i użytkownicy mogą uzyskać do niego dostęp. Jeśli program OfficeScan wykryje zagrożenie bezpieczeństwa lub potencjalnego wirusa / złośliwe oprogramowanie, jest wyświetlane powiadomienie zawierające nazwę zarażonego pliku i określonego zagrożenia bezpieczeństwa.

Skanowanie w czasie rzeczywistym zachowuje trwałą pamięć podręczną skanowania, która jest ładowana ponownie po każdym uruchomieniu agenta OfficeScan. Agent OfficeScan śledzi wszystkie zmiany w plikach lub folderach, które wystąpiły od momentu zamknięcia agenta OfficeScan oraz usuwa te pliki z pamięci podręcznej.

Uwaga

Aby zmodyfikować powiadomienie programu, należy otworzyć konsolę Web i przejść do sekcji **Administracja** > **Powiadomienia** > **Agent**.

Ustawienia skanowania w czasie rzeczywistym można konfigurować i stosować na jednym lub wielu agentach i domenach albo na wszystkich agentach zarządzanych przez serwer.

Konfigurowanie ustawień skanowania w czasie rzeczywistym

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Ustawienia skanowania** > **Ustawienia skanowania w czasie rzeczywistym**.
4. Wybierz następujące opcje:
   - **Włącz skanowanie wirusów / złośliwego oprogramowania**
   - **Włącz skanowanie oprogramowania spyware/grayware**

   Uwaga

   W przypadku wyłączenia skanowania w poszukiwaniu wirusów / złośliwego oprogramowania, jest również wyłączane skanowanie w poszukiwaniu oprogramowania spyware/grayware. Podczas epidemii wirusów skanowania w czasie rzeczywistym nie można wyłączyć (jest ono automatycznie włączane, nawet jeśli początkowo było wyłączone). Dzięki temu wirusy nie mogą modyfikować ani usuwać plików oraz folderów na komputerach agentów.
5. Na karcie **Cel** skonfiguruj następujące opcje:
   - *Działania użytkownika na plikach na stronie 7-30*
   - *Pliki do skanowania na stronie 7-30*
   - *Ustawienia skanowania na stronie 7-31*

6. Kliknij kartę **Operacja** i skonfiguruj następujące opcje:

TABELA 7-6. Operacje skanowania

OPERACJA	REFERENCJE
Operacja dla wirusa/ złośliwego oprogramowania	Operacja podstawowa (wybierz jedną): • *Zastosuj funkcję ActiveAction na stronie 7-42* • *Wykonaj te same operacje dla wszystkich typów wirusów/złośliwego oprogramowania na stronie 7-44* • *Użyj konkretnego działania w przypadku wirusa/ złośliwego oprogramowania każdego typu na stronie 7-44* **Uwaga** Szczegółowe informacje o różnych operacjach zawiera temat *Operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania na stronie 7-40*. Dodatkowe operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania: • *Katalog kwarantanny na stronie 7-45* • *Utwórz kopie przed wyczyszczeniem na stronie 7-47* • *Usługi Usuwania Szkód Services na stronie 7-48* • *Wyświetl powiadomienie, jeśli wykryty zostanie wirus/złośliwe oprogramowanie na stronie 7-49* • *Wyświetl powiadomienie, jeśli wykryty zostanie potencjalny wirus/złośliwe oprogramowanie na stronie 7-49*

OPERACJA	REFERENCJE
Operacja dla oprogramowania spyware/grayware	Operacja podstawowa: • *Operacje skanowania w poszukiwaniu oprogramowania spyware/grayware na stronie 7-55* Dodatkowa operacja skanowania w poszukiwaniu spyware/grayware: • *Wyświetl powiadomienie programu po wykryciu spyware/grayware na stronie 7-56*

7. Na karcie **Wykluczenia skanowania** można skonfigurować katalogi, pliki i rozszerzenia, które mają być wykluczone ze skanowania.

   Szczegółowe informacje zawiera sekcja *Wykluczenia skanowania na stronie 7-35*.

8. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.

   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Skanowanie ręczne

Skanowanie ręczne jest inicjowane na żądanie użytkownika i rozpoczyna się natychmiast po uruchomieniu tej funkcji z konsoli agenta OfficeScan. Czas skanowania zależy od liczby przeznaczonych do skanowania plików oraz od zasobów sprzętowych punktu końcowego agenta OfficeScan.

Ustawienia skanowania ręcznego można konfigurować i stosować na jednym lub wielu agentach i domenach albo na wszystkich agentach zarządzanych przez serwer.

Konfigurowanie ustawień skanowania ręcznego

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Ustawienia skanowania** > **Ustawienia skanowania ręcznego**.
4. Na karcie **Cel** skonfiguruj następujące opcje:
   - *Pliki do skanowania na stronie 7-30*
   - *Ustawienia skanowania na stronie 7-31*
   - *Wykorzystanie procesora na stronie 7-33*
5. Kliknij kartę **Operacja** i skonfiguruj następujące opcje:

TABELA 7-7. Operacje skanowania

OPERACJA	REFERENCJE
Operacja dla wirusa/ złośliwego oprogramowania	Operacja podstawowa (wybierz jedną): • *Zastosuj funkcję ActiveAction na stronie 7-42* • *Wykonaj te same operacje dla wszystkich typów wirusów/złośliwego oprogramowania na stronie 7-44* • *Użyj konkretnego działania w przypadku wirusa/ złośliwego oprogramowania każdego typu na stronie 7-44* **Uwaga** Szczegółowe informacje o różnych operacjach zawiera temat *Operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania na stronie 7-40*. Dodatkowe operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania: • *Katalog kwarantanny na stronie 7-45* • *Utwórz kopie przed wyczyszczeniem na stronie 7-47* • *Usługi Usuwania Szkód Services na stronie 7-48*
Operacja dla oprogramowania spyware/grayware	Operacja podstawowa: • *Operacje skanowania w poszukiwaniu oprogramowania spyware/grayware na stronie 7-55*

6. Na karcie **Wykluczenia skanowania** można skonfigurować katalogi, pliki i rozszerzenia, które mają być wykluczone ze skanowania.

   Szczegółowe informacje zawiera sekcja *Wykluczenia skanowania na stronie 7-35*.

7. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

- **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Skanowanie zaplanowane

Skanowanie zaplanowane jest uruchamiane automatycznie zgodnie z datą i godziną ustawioną w harmonogramie. Funkcja Skanowanie zaplanowane pozwala zwiększyć wydajność zarządzania skanowaniem i zautomatyzować procesy regularnego skanowania na agencie.

Ustawienia skanowania zaplanowanego można konfigurować i stosować na jednym lub wielu agentach i domenach albo na wszystkich agentach zarządzanych przez serwer.

Konfigurowanie ustawień skanowania zaplanowanego

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Ustawienia skanowania** > **Ustawienia skanowania zaplanowanego**.
4. Wybierz następujące opcje:
   - **Włącz skanowanie wirusów / złośliwego oprogramowania**
   - **Włącz skanowanie oprogramowania spyware/grayware**

Uwaga

W przypadku wyłączenia skanowania w poszukiwaniu wirusów / złośliwego oprogramowania, jest również wyłączane skanowanie w poszukiwaniu oprogramowania spyware/grayware.

5. Na karcie **Cel** skonfiguruj następujące opcje:
   - *Harmonogram na stronie 7-34*
   - *Pliki do skanowania na stronie 7-30*
   - *Ustawienia skanowania na stronie 7-31*
   - *Wykorzystanie procesora na stronie 7-33*
6. Kliknij kartę **Operacja** i skonfiguruj następujące opcje:

TABELA 7-8. Operacje skanowania

OPERACJA	REFERENCJE
Operacja dla wirusa/ złośliwego oprogramowania	Operacja podstawowa (wybierz jedną): • *Zastosuj funkcję ActiveAction na stronie 7-42* • *Wykonaj te same operacje dla wszystkich typów wirusów/złośliwego oprogramowania na stronie 7-44* • *Użyj konkretnego działania w przypadku wirusa/ złośliwego oprogramowania każdego typu na stronie 7-44* **Uwaga** Szczegółowe informacje o różnych operacjach zawiera temat *Operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania na stronie 7-40*. Dodatkowe operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania: • *Katalog kwarantanny na stronie 7-45* • *Utwórz kopie przed wyczyszczeniem na stronie 7-47* • *Usługi Usuwania Szkód Services na stronie 7-48* • *Wyświetl powiadomienie, jeśli wykryty zostanie wirus/złośliwe oprogramowanie na stronie 7-49* • *Wyświetl powiadomienie, jeśli wykryty zostanie potencjalny wirus/złośliwe oprogramowanie na stronie 7-49*

OPERACJA	REFERENCJE
Operacja dla oprogramowania spyware/grayware	Operacja podstawowa: • *Operacje skanowania w poszukiwaniu oprogramowania spyware/grayware na stronie 7-55* Dodatkowa operacja skanowania w poszukiwaniu spyware/grayware: • *Wyświetl powiadomienie programu po wykryciu spyware/grayware na stronie 7-56*

7. Na karcie **Wykluczenia skanowania** można skonfigurować katalogi, pliki i rozszerzenia, które mają być wykluczone ze skanowania.

   Szczegółowe informacje zawiera sekcja *Wykluczenia skanowania na stronie 7-35*.

8. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Skanuj teraz

Funkcja Skanuj teraz jest zdalnie inicjowana przez administratora programu OfficeScan z poziomu konsoli Web i może być stosowana na jednym lub kilku komputerach agentów.

Ustawienia funkcji Skanuj teraz można konfigurować i stosować na jednym lub kilku agentach i domenach albo na wszystkich agentach zarządzanych przez serwer.

Konfigurowanie ustawień Skanuj teraz

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Ustawienia skanowania** > **Ustawienia funkcji Skanuj teraz**.
4. Wybierz następujące opcje:
   - **Włącz skanowanie wirusów / złośliwego oprogramowania**
   - **Włącz skanowanie oprogramowania spyware/grayware**

   Uwaga

   W przypadku wyłączenia skanowania w poszukiwaniu wirusów / złośliwego oprogramowania, jest również wyłączane skanowanie w poszukiwaniu oprogramowania spyware/grayware.
5. Na karcie **Cel** skonfiguruj następujące opcje:
   - *Pliki do skanowania na stronie 7-30*
   - *Ustawienia skanowania na stronie 7-31*
   - *Wykorzystanie procesora na stronie 7-33*
6. Kliknij kartę **Operacja** i skonfiguruj następujące opcje:

TABELA 7-9. Operacje skanowania

OPERACJA	REFERENCJE
Operacja dla wirusa/ złośliwego oprogramowania	Operacja podstawowa (wybierz jedną): • *Zastosuj funkcję ActiveAction na stronie 7-42* • *Wykonaj te same operacje dla wszystkich typów wirusów/złośliwego oprogramowania na stronie 7-44* • *Użyj konkretnego działania w przypadku wirusa/ złośliwego oprogramowania każdego typu na stronie 7-44* **Uwaga** Szczegółowe informacje o różnych operacjach zawiera temat *Operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania na stronie 7-40*. Dodatkowe operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania: • *Katalog kwarantanny na stronie 7-45* • *Utwórz kopie przed wyczyszczeniem na stronie 7-47* • *Usługi Usuwania Szkód Services na stronie 7-48*
Operacja dla oprogramowania spyware/grayware	Operacja podstawowa: • *Operacje skanowania w poszukiwaniu oprogramowania spyware/grayware na stronie 7-55*

7. Na karcie **Wykluczenia skanowania** można skonfigurować katalogi, pliki i rozszerzenia, które mają być wykluczone ze skanowania.

   Szczegółowe informacje zawiera sekcja *Wykluczenia skanowania na stronie 7-35*.

8. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

- **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Uruchamianie Skanuj teraz

Funkcję Skanuj teraz należy inicjować na komputerach, które są prawdopodobnie zarażone.

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, albo wybierz określone domeny lub agentów.
3. Kliknij kolejno opcje **Zadania** > **Skanuj teraz**.
4. Aby zmienić skonfigurowane wstępnie ustawienia funkcji **Skanuj teraz** przed zainicjowaniem skanowania, kliknij polecenie **Ustawienia**.

   Zostanie wyświetlony ekran **Ustawienia funkcji Skanuj teraz**. Szczegółowe informacje można znaleźć w części *Skanuj teraz na stronie 7-25*.
5. W drzewie agentów wybierz agentów, które wykonają skanowanie, a następnie kliknij polecenie **Uruchom funkcję Skanuj teraz**.

   Serwer wyśle powiadomienie do agentów.
6. Sprawdź stan powiadomienia oraz czy powiadomienia dotarły do wszystkich agentów.
7. Kliknij polecenie **Wybierz niepowiadomione punkty końcowe**, a następnie kliknij polecenie **Uruchom funkcję Skanuj teraz**, aby natychmiast wysłać

ponowne powiadomienie do agentów, do których takie powiadomienie nie zostało jeszcze wysłane.

Przykład: łączna liczba agentów: 50

TABELA 7-10. Scenariusze związane z niepowiadomionymi agentami

WYBÓR DRZEWA AGENTÓW	POWIADOMIENI AGENCI (PO KLIKNIĘCIU POLECENIA „URUCHOM FUNKCJĘ SKANUJ TERAZ”)	NIEPOWIADOMIENI AGENCI
Brak (automatyczne wybranie wszystkich 50 agentów)	35 z 50 agentów	15 agenci
Wybór ręczny (wybrano 45 z 50 agentów)	40 z 45 agentów	5 agentów + 5 innych agentów nieuwzględnionych w wyborze ręcznym

8. Kliknij polecenie **Zatrzymaj powiadamianie**, aby program OfficeScan przerwał działanie bieżącej operacji powiadamiania agentów. Powiadomieni Agenci oraz już przeprowadzający skanowanie zignorują to polecenie.

9. W przypadku agentów przeprowadzających skanowanie kliknij polecenie **Zatrzymaj funkcję Skanuj teraz** w celu powiadomienia ich o zaprzestaniu skanowania.

Ustawienia ogólne wszystkich typów skanowania

W przypadku skanowania każdego typu należy skonfigurować trzy zestawy ustawień: kryteria skanowania, wykluczenia skanowania i operacje skanowania. Ustawienia takie należy wdrożyć na jednym lub kilku agentach i domenach, albo na wszystkich agentach zarządzanych przez serwer.

Kryteria skanowania

Można skonfigurować opcje, takie jak typ pliku i rozszerzenie pliku, określające typ skanowania używany w odniesieniu do poszczególnych plików. Można również określić zdarzenia wywołujące skanowanie. Można na przykład tak skonfigurować ustawienia, aby plik był skanowany w czasie rzeczywistym po jego pobraniu na punkt końcowy.

Działania użytkownika na plikach

Wybierz działania na plikach, które mają wywoływać skanowanie w czasie rzeczywistym. Wybierz odpowiednie opcje:

- **Skanuj pliki tworzone/modyfikowane**: są skanowane nowe pliki zapisywane na punkcie końcowym (np. po pobraniu) oraz pliki modyfikowane.
- **Skanuj pliki pobierane**: pliki są skanowane w momencie ich otwierania.
- **Skanuj pliki tworzone/modyfikowane i pobierane**

Jeśli na przykład wybrano trzecią opcję, nowy plik pobrany na punkt końcowy zostanie przeskanowany i pozostanie w bieżącej lokalizacji, jeśli nie zostanie wykryte żadne zagrożenie bezpieczeństwa. Ten sam plik będzie skanowany w momencie jego otwarcia, wprowadzania modyfikacji oraz przed zapisaniem wprowadzonych modyfikacji.

Pliki do skanowania

Wybierz odpowiednie opcje:

- **Wszystkie pliki możliwe do skanowania**: skanowanie wszystkich plików.
- **Typy plików skanowane przez IntelliScan**: są skanowane tylko pliki znane jako potencjalnie przenoszące złośliwy kod, nawet takie, które mają nieszkodliwe rozszerzenie.

  Szczegółowe informacje można znaleźć w części *IntelliScan na stronie E-6*.
- **Pliki o następujących rozszerzeniach**: są skanowane tylko pliki o rozszerzeniach znajdujących się na liście rozszerzeń plików. Można dodawać nowe rozszerzenia lub usuwać dowolne istniejące rozszerzenia.

Ustawienia skanowania

Należy wybrać jedną lub wiele następujących opcji:

- **Skanuj dyskietkę podczas zamykania systemu**: Skanowanie w czasie rzeczywistym skanuje napęd dyskietek pod kątem wirusów sektora rozruchowego przed wyłączeniem punktu końcowego. Zapobiega to uruchomieniu wirusa/złośliwego oprogramowania po ponownym uruchomieniu punktu końcowego z dyskietki.

- **Skanuj foldery ukryte**: Podczas skanowania ręcznego umożliwia programowi OfficeScan wykrywanie, a następnie skanowanie ukrytych folderów na punkcie końcowym.

- **Skanuj dysk sieciowy**: Podczas skanowania ręcznego lub skanowania w czasie rzeczywistym skanuje napędy sieciowe i foldery mapowane na punkt końcowy Agent OfficeScan.

- **Skanuj sektor rozruchowy przenośnego urządzenia magazynującego USB po jego podłączeniu**: automatycznie skanuje tylko sektor rozruchowy urządzenia magazynującego USB za każdym razem, kiedy użytkownik je podłączy (skanowanie w czasie rzeczywistym).

- **Skanuj wszystkie pliki w wymiennych urządzeniach pamięci masowej po podłączeniu**: automatycznie skanuje wszystkie pliki na urządzeniu magazynującym USB za każdym razem, kiedy użytkownik je podłączy (skanowanie w czasie rzeczywistym).

- **Poddaj kwarantannie wykryte w pamięci warianty złośliwego oprogramowania**: Funkcja Monitorowanie zachowania skanuje pamięć systemu pod kątem podejrzanych procesów, a skanowanie w czasie rzeczywistym mapuje proces i skanuje go pod kątem zagrożeń ze strony złośliwego oprogramowania. Jeśli istnieje zagrożenie złośliwym oprogramowaniem, skanowanie w czasie rzeczywistym poddaje plik i/lub proces kwarantannie.

Uwaga

Ta funkcja wymaga włączenia przez administratorów usługi zapobiegania nieautoryzowanym zmianom i usługi zaawansowanej ochrony.

- **Skanuj pliki skompresowane**: Umożliwia programowi OfficeScan skanowanie określonej maksymalnej liczby warstw kompresji i pominięcie skanowania nadmiarowych warstw. Program OfficeScan może także czyścić lub usuwać zarażone pliki w plikach skompresowanych. Na przykład jeśli maksymalna określona liczba to dwie warstwy, a skompresowany plik przeznaczony do skanowania ma sześć warstw, program OfficeScan przeprowadzi skanowanie dwóch warstw i pominie pozostałe cztery. Jeśli skompresowany plik zawiera zagrożenia bezpieczeństwa, program OfficeScan czyści lub usuwa plik.

  Uwaga

  Program OfficeScan traktuje pliki pakietu Microsoft Office 2007 zapisane w formacie Office Open XML, jak pliki skompresowane. Office Open XML, format pliku aplikacji pakietu Office 2007, wykorzystuje technologię kompresji ZIP. Jeśli pliki utworzone za pomocą tych aplikacji mają zostać przeskanowane pod kątem wirusów/złośliwego oprogramowania, należy włączyć skanowanie plików skompresowanych.

- **Skanuj obiekty OLE**: Gdy plik zawiera wiele warstw OLE (Object Linking and Embedding), program OfficeScan wykona skanowanie określonej przez użytkownika liczby warstw i pominie pozostałe.

  Wszyscy agenci zarządzani przez serwer sprawdzają to ustawienie podczas skanowania ręcznego, skanowania w czasie rzeczywistym, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz. W poszukiwaniu wirusów / złośliwego oprogramowania oraz oprogramowania spyware/grayware jest skanowana każda warstwa kompresji.

  Na przykład:

  Określona liczba warstw to 2. W pliku jest osadzony dokument programu Microsoft Word (pierwsza warstwa), w jego wnętrzu jest osadzony skoroszyt programu Microsoft Excel (druga warstwa), a w jego wnętrzu znajduje się plik `.exe` (trzecia warstwa). Program OfficeScan przeprowadzi skanowanie dokumentu programu Word i skoroszytu programu Excel, ale pominie plik `.exe`.

  - **Wykrywanie kodu ataku w plikach OLE**: Wykrycie wykorzystania OLE heurystycznie identyfikuje złośliwe oprogramowanie, sprawdzając pliki pakietu Microsoft Office w poszukiwaniu kodu ataku.

Uwaga

Określona liczba warstw kompresji dotyczy zarówno opcji **Skanuj obiekty OLE**, jak i opcji **Wykryj kod ataku**.

- **Włącz mechanizm IntelliTrap**: Wykrywa i usuwa wirusy/złośliwe oprogramowanie w skompresowanych plikach wykonywalnych. Opcja ta jest dostępna wyłącznie dla skanowania w czasie rzeczywistym.

  Szczegółowe informacje można znaleźć w części *IntelliTrap na stronie E-7*.

- **Włącz skanowanie wykorzystania luki CVE w celu wyszukania plików pobranych z sieci Web oraz pocztą e-mail**: Blokuje procesy podejmujące próbę wykorzystania znanych luk w dostępnych komercyjnie produktach na podstawie systemu Common Vulnerabilities and Exposures (CVE). Opcja ta jest dostępna wyłącznie dla skanowania w czasie rzeczywistym.

- **Skanuj obszar rozruchowy**: Podczas skanowania ręcznego, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz skanuje sektor rozruchowy dysku twardego w poszukiwaniu wirusów/złośliwego oprogramowania.

Wykorzystanie procesora

Program OfficeScan może wstrzymywać działanie między skanowaniem kolejnych plików. To ustawienie jest stosowane podczas skanowania ręcznego, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz.

Wybierz odpowiednie opcje:

- **Wysokie**: brak przerw między kolejnymi operacjami skanowania.
- **Średnie**: wstrzymuje pracę podczas skanowania kolejnych plików, jeśli poziom wykorzystania procesora przekracza 50%. W przeciwnym razie skanuje bez przerw.
- **Niskie**: wstrzymuje pracę podczas skanowania kolejnych plików, jeśli poziom wykorzystania procesora przekracza 20%. W przeciwnym razie skanuje bez przerw.

W przypadku wybraniu poziomu Średnie lub Niskie, gdy po uruchomieniu skanowania wykorzystanie procesora mieści się w określonych granicach (50% lub 20%), program OfficeScan nie będzie wstrzymywać działania między operacjami skanowania, dzięki

czemu skanowanie będzie trwać krócej. Program OfficeScan wykorzystuje wtedy więcej zasobów procesora, ale ponieważ poziom wykorzystania jest optymalny, wydajność punktu końcowego nie jest nadmiernie ograniczana. Gdy wykorzystanie procesora przekroczy wartość graniczną, program OfficeScan wstrzyma działanie. Działanie zostanie wznowione, jeśli poziom wykorzystania procesora ponownie spadnie poniżej wartości granicznej.

W przypadku wybrania opcji Wysokie program OfficeScan nie sprawdza bieżącego wykorzystania procesora i skanuje pliki bez wstrzymywania działania.

Harmonogram

Określ, jak często (codziennie, co tydzień czy co miesiąc) i o której godzinie Skanowanie zaplanowane ma być uruchamiane.

Na potrzeby comiesięcznego Skanowania zaplanowanego można wybrać albo konkretny dzień miesiąca, albo dzień tygodnia oraz kolejność występowania.

- **Konkretny dzień miesiąca**: Wybierz dzień od 1. do 31. Jeśli wybrano 29., 30. lub 31. dzień, a w danym miesiącu go nie ma, program OfficeScan uruchamia skanowanie zaplanowane w ostatnim dniu miesiąca. W związku z tym:
  - Jeśli wybrano 29. dzień, Skanowanie zaplanowane jest uruchamiane 28 lutego (z wyjątkiem roku przestępnego) oraz 29. dnia pozostałych miesięcy.
  - Jeśli wybrano 30. dzień, Skanowanie zaplanowane jest uruchamiane 28 lub 29 lutego oraz 30. dnia pozostałych miesięcy.
  - Jeśli wybrano 31. dzień, Skanowanie zaplanowane jest uruchamiane 28 lub 29 lutego, 30 kwietnia, 30 czerwca, 30 września, 30 listopada oraz 31. dnia pozostałych miesięcy.
- **Dzień tygodnia i kolejność występowania**: Dany dzień tygodnia występuje cztery lub pięć razy w miesiącu. Przykładowo w miesiącu są zwykle cztery poniedziałki. Określ dzień tygodnia i kolejność, w jakiej występuje w ciągu miesiąca. Wybierz na przykład uruchamianie Skanowania zaplanowanego w drugi poniedziałek każdego miesiąca. Jeśli wybierzesz piąte wystąpienie dnia, a nie będzie go w danym miesiącu, skanowanie zostanie przeprowadzone przy czwartym wystąpieniu.

Wykluczenia skanowania

Aby zwiększyć wydajność skanowania i pomijać skanowanie plików powodujących fałszywe alarmy, można skonfigurować wykluczenia skanowania. Gdy jest wykonywane skanowanie określonego typu, program OfficeScan sprawdza lista wykluczeń skanowania, aby określić, które pliki punktu końcowego nie będą skanowanie w poszukiwaniu wirusów/złośliwego oprogramowania oraz oprogramowania spyware/grayware.

Po włączeniu wykluczenia skanowania program OfficeScan nie skanuje pliku, jeśli:

- plik znajduje się w określonym katalogu (lub w dowolnym z jego podkatalogów),
- nazwa pliku pasuje do dowolnej nazwy znajdującej się na liście wykluczeń,
- rozszerzenie pliku pasuje do dowolnego rozszerzenia znajdującego się na liście wykluczeń.

Porada

Lista produktów niezalecanych przez firmę Trend Micro do uwzględniania w ramach skanowania w czasie rzeczywistym znajduje się na stronie:

http://esupport.trendmicro.com/solution/en-US/1059770.aspx

Wyjątki z symbolami wieloznacznymi

Lista wykluczeń plików i katalogów ze skanowania obsługuje wykorzystanie symboli wieloznacznych. Można użyć znaku „?” do zastąpienia jednego znaku oraz użyć znaku „*” do zastąpienia kilku znaków.

Podczas korzystania z symboli wieloznacznych należy zachować ostrożność. Użycie niewłaściwego symbolu może spowodować wykluczenie niewłaściwych plików lub katalogów. Na przykład, dodanie ciągu `C:\*` do Lista wykluczeń skanowania (pliki) spowoduje wykluczenie ze skanowania całego dysku `C:\`.

TABELA 7-11. Wykluczenia skanowania zawierające symbole wieloznaczne

WARTOŚĆ	WYKLUCZONE	NIEWYKLUCZONE

`c:\director*\fil\*.txt`	`c:\directory\fil\doc.txt`
	`c:\directories\fil\files\document.txt`
		`c:\directory\file\`
		`c:\directories\files\`
		`c:\directory\file\doc.txt`
		`c:\directories\files\document.txt`

`c:\director?\file\*.txt`	`c:\directory\file\doc.txt`	`c:\directories\file\document.txt`
`c:\director?\file\?.txt`	`c:\directory\file\1.txt`	`c:\directory\file\doc.txt` `c:\directories\file\document.txt`
`c:\*.txt`	Wszystkie pliki `.txt` w katalogu `C:\`	Wszystkie inne typy plików w katalogu `C:\`
`[]`	Nieobsługiwane	Nieobsługiwane

Lista wykluczeń skanowania (katalogi)

Program OfficeScan pomija skanowanie wszystkich plików znajdujących się w określonym katalogu na komputerze. Można określić maksymalnie 256 katalogów.

Uwaga

Wykluczając katalog ze skanowania, program OfficeScan automatycznie wyklucza ze skanowania również wszystkie jego podkatalogi.

Można także wybrać opcję **Wyklucz katalogi, w których zainstalowano produkty firmy Trend Micro**. W przypadku wybrania tej opcji program OfficeScan automatycznie wyklucza ze skanowania katalogi następujących produktów firmy Trend Micro:

- <*Folder instalacji serwera*>

Uwaga

Podczas skanowania ręcznego program OfficeScan kontynuuje skanowanie folderu instalacji serwera.

- Zabezpieczenia wiadomości błyskawicznych
- InterScan eManager 3.5x
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall
- ScanMail eManager™ 3.11, 5.1, 5.11, 5.12
- ScanMail for Lotus Notes™ eManager NT
- ScanMail™ for Microsoft Exchange

W przypadku posiadania produktu Trend Micro, który NIE został wymieniony poniżej, należy ręcznie dodać katalogi produktu do lista wykluczeń skanowania

Należy również skonfigurować w programie OfficeScan opcję wykluczenia katalogów programu Microsoft Exchange 2000/2003, przechodząc do sekcji **Ustawienia skanowania** opcji **Agenci** > **Ustawienia agenta globalnego** na karcie **Ustawienia zabezpieczeń**. W przypadku korzystania z programu Microsoft Exchange 2007 lub nowszego należy ręcznie dodać jego katalog do lista wykluczeń skanowania. Szczegółowe informacje na temat wykluczenia skanowania znajdują się w witrynie:

http://technet.microsoft.com/en-us/library/bb332342.aspx

Podczas konfigurowania listy plików można wybrać spośród następujących opcji:

- **Zachowanie bieżącej listy** (domyślna): Program OfficeScan udostępnia tę opcję, aby zapobiec przypadkowemu zastąpieniu istniejącej listy wykluczeń agenta. Aby zapisać i zastosować zmiany dokonane na liście wykluczeń, należy wybrać jedną z pozostałych opcji.

- **Zastąpienie**: Ta opcja powoduje usunięcie całej listy wykluczeń na agencie i zastąpienie jej bieżącą listą. Po kliknięciu polecenia **Zastosuj dla wszystkich agentów** program OfficeScan wyświetla komunikat ostrzeżenia w celu potwierdzenia.
- **Dodanie ścieżek do**: Ta opcja powoduje dodanie elementów znajdujących się na aktualnej liście do istniejącej listy wykluczeń agenta. Jeśli element już znajduje się na liście wykluczeń agenta, agent zignoruje ten element.
- **Usunięcie ścieżek z**: Ta opcja powoduje usunięcie elementów znajdujących się na aktualnej liście z istniejącej listy wykluczeń agenta, jeśli zostaną znalezione.

Lista wykluczeń skanowania (pliki)

Program OfficeScan nie skanuje pliku, jeśli jego nazwa pasuje do nazwy znajdującej się na liście wykluczeń. W przypadku zamiaru wykluczenia pliku znajdującego się w określonej lokalizacji punktu końcowego można wprowadzić ścieżkę tego pliku, na przykład `C:\Temp\sample.jpg`.

Można określić maksymalnie 256 plików.

Podczas konfigurowania listy plików można wybrać spośród następujących opcji:

- **Zachowanie bieżącej listy** (domyślna): Program OfficeScan udostępnia tę opcję, aby zapobiec przypadkowemu zastąpieniu istniejącej listy wykluczeń agenta. Aby zapisać i zastosować zmiany dokonane na liście wykluczeń, należy wybrać jedną z pozostałych opcji.
- **Zastąpienie**: Ta opcja powoduje usunięcie całej listy wykluczeń na agencie i zastąpienie jej bieżącą listą. Po kliknięciu polecenia **Zastosuj dla wszystkich agentów** program OfficeScan wyświetla komunikat ostrzeżenia w celu potwierdzenia.
- **Dodanie ścieżek do**: Ta opcja powoduje dodanie elementów znajdujących się na aktualnej liście do istniejącej listy wykluczeń agenta. Jeśli element już znajduje się na liście wykluczeń agenta, agent zignoruje ten element.
- **Usunięcie ścieżek z**: Ta opcja powoduje usunięcie elementów znajdujących się na aktualnej liście z istniejącej listy wykluczeń agenta, jeśli zostaną znalezione.

Lista wykluczeń skanowania (rozszerzenia plików)

Program OfficeScan nie skanuje pliku, jeśli jego rozszerzenie pasuje do rozszerzenia znajdującego się na liście wykluczeń. Można określić maksymalnie 256 rozszerzeń plików. Przed rozszerzeniem nie trzeba wpisywać kropki (.).

W przypadku skanowania ręcznego, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz, jako symbol wieloznaczny można zastosować pytajnik (?) lub gwiazdkę (*). Na przykład, aby skanować wszystkie pliki z rozszerzeniem rozpoczynającym się literą D, takie jak `DOC`, `DOT` lub `DAT`, należy wpisać `D*` lub `D?`.

Uwaga

Skanowanie w czasie rzeczywistym nie obsługuje użycia symboli wieloznacznych podczas określania rozszerzeń.

Zastosuj ustawienia wykluczenia skanowania do wszystkich typów skanowania

Program OfficeScan umożliwia skonfigurowanie ustawień wykluczenia skanowania w odniesieniu do skanowania określonego typu, a następnie zastosowanie takich samych ustawień do innych typów skanowania. Na przykład:

Pierwszego stycznia administrator programu OfficeScan o imieniu Piotr stwierdził, że na komputerach agentów znajduje się dużo plików typu `JPG` oraz że nie stanowią one zagrożenia bezpieczeństwa. Piotr dodał rozszerzenie `JPG` do listy wykluczeń plików ze skanowania ręcznego i zastosował to ustawienie do pozostałych typów skanowania. Dzięki temu pliki `.jpg` są teraz pomijane również w przypadku skanowania w czasie rzeczywistym, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz.

Tydzień później Piotr usunął rozszerzenie `JPG` z listy wykluczeń ze skanowania w czasie rzeczywistym, ale nie zastosował tego ustawienia do pozostałych typów skanowania. Pliki `JPG` nie są od tej pory skanowane tylko w przypadku skanowania w czasie rzeczywistym.

Operacje skanowania

Można określić, jaką operację wykonuje program OfficeScan, gdy podczas skanowania określonego typu zostanie wykryte zagrożenie bezpieczeństwa. Program OfficeScan

używa innych zestawów operacji skanowania w poszukiwaniu wirusów/złośliwego oprogramowania oraz spyware/grayware.

Operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania

Operacja skanowania wykonywana przez program OfficeScan zależy od typu wirusa / złośliwego oprogramowania oraz typu skanowania używanego do szukania wirusów / złośliwego oprogramowania. Przykładowo, w przypadku wykrycia przez program OfficeScan programu typu „koń trojański" (typ wirusa/złośliwego oprogramowania) podczas skanowania ręcznego (typ skanowania) zarażony plik zostanie wyczyszczony (operacja).

Informacje na temat różnych rodzajów wirusów/złośliwego oprogramowania można znaleźć w *Wirusy i złośliwe oprogramowanie na stronie 7-2*.

Program OfficeScan wykonuje względem wirusów/złośliwego oprogramowania następujące operacje:

TABELA 7-12. Operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania

OPERACJA	OPIS
Usuń	Program OfficeScan usuwa zarażony plik.

OPERACJA	OPIS
Poddaj kwarantannie	Program OfficeScan zmienia nazwę zainfekowanego pliku, szyfruje go, a następnie przenosi do tymczasowego katalogu kwarantanny na punkcie końcowym agenta w lokalizacji <*Folder instalacji agenta*>`\Suspect`. Agent OfficeScan przesyła następnie pliki poddane kwarantannie do wyznaczonego katalogu kwarantanny. Szczegółowe informacje można znaleźć w części *Katalog kwarantanny na stronie 7-45*. Domyślny katalog kwarantanny znajduje się na serwerze OfficeScan w lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Virus`. W razie potrzeby przywrócenia plików poddanych kwarantannie należy użyć funkcji Centralne przywracanie kwarantanny. Szczegółowe informacje zawiera sekcja *Przywracanie plików poddanych kwarantannie na stronie 7-50*.
Wyczyść	Przed zapewnieniem pełnego dostępu do danego pliku Program OfficeScan czyści zarażony plik. Jeśli nie ma możliwości wyczyszczenia pliku, program OfficeScan jako drugą operację wykonuje jedną z następujących czynności: Poddaj kwarantannie, Usuń, Zmień nazwę, Zezwól. Aby skonfigurować drugą operację, przejdź do opcji **Agenci** > **Zarządzanie agentami**. Kliknij kartę **Ustawienia** > **Ustawienia skanowania** > **{typ skanowania}** > **Operacja**. Operację można przeprowadzać na wszystkich typach złośliwego oprogramowania z wyjątkiem prawdopodobnego wirusa/złośliwego oprogramowania.
Zmień nazwę	Program OfficeScan zmienia rozszerzenie zainfekowanego pliku na „`vir`”. Użytkownicy początkowo nie mogą otworzyć pliku, którego nazwa została zmieniona; mogą to zrobić po skojarzeniu pliku z aplikacją. Wirus/złośliwe oprogramowanie mogą zostać uruchomione podczas otwierania zarażonego pliku o zmienionej nazwie.

Operacja	Opis
Pomiń	Program OfficeScan może wykonywać tę operację tylko wówczas, jeśli wirus dowolnego typu zostanie wykryty podczas skanowania ręcznego, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz. Ta operacja skanowania nie może być używana podczas skanowania w czasie rzeczywistym, ponieważ niewykonanie żadnej czynności po wykryciu próby otwarcia lub uruchomienia wykrytego zarażonego pliku umożliwi uruchomienie wirusa/złośliwego oprogramowania. Wszystkie pozostałe operacje skanowania można wykorzystywać podczas skanowania w czasie rzeczywistym.
Odmów dostępu	Tę operację skanowania można wykonać tylko podczas skanowania w czasie rzeczywistym. Po wykryciu przez program OfficeScan próby otwarcia lub wykonania zarażonego pliku ta operacja jest natychmiast blokowana. Użytkownicy mogą ręcznie usunąć zarażony plik.

Zastosuj funkcję ActiveAction

Różne typy wirusów/złośliwego oprogramowania wymagają różnych operacji skanowania. Dostosowywanie operacji skanowania wymaga znajomości wirusów/złośliwego oprogramowania i może być czasochłonnym zadaniem. Program OfficeScan używa funkcji ActiveAction w celu rozwiązania tych problemów.

Usługa ActiveAction to zestaw wstępnie skonfigurowanych operacji skanowania w poszukiwaniu wirusów/złośliwego oprogramowania. Jeśli użytkownik nie jest zaznajomiony z operacjami skanowania lub nie ma pewności, czy operacja skanowania jest odpowiednia dla danego typu wirusa/złośliwego oprogramowania, firma Trend Micro zaleca użycie funkcji ActiveAction.

Korzystanie z funkcji ActiveAction zapewnia następujące korzyści:

- W usłudze ActiveAction zastosowano operacje skanowania zalecane przez firmę Trend Micro. Nie trzeba poświęcać czasu na skonfigurowanie operacji skanowania.
- Twórcy wirusów stale zmieniają sposoby atakowania komputerów wirusami/złośliwym oprogramowaniem. Ustawienia funkcji ActiveAction są aktualizowane, aby zapewnić ochronę przed najnowszymi zagrożeniami i metodami ataków wirusów/złośliwego oprogramowania.

Uwaga

Usługa ActiveAction nie obsługuje skanowania w poszukiwaniu oprogramowania spyware/grayware.

Poniższa tabela ilustruje sposób działania usługi ActiveAction w odniesieniu do każdego typu wirusa/złośliwego oprogramowania:

TABELA 7-13. Operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania zalecane przez firmę Trend Micro

TYP WIRUSA/ ZŁOŚLIWEGO OPROGRAMOWANIA	SKANOWANIE W CZASIE RZECZYWISTYM		SKANOWANIE RĘCZNE/ SKANOWANIE ZAPLANOWANE/ SKANUJ TERAZ	
	PIERWSZA OPERACJA	DRUGA OPERACJA	PIERWSZA OPERACJA	DRUGA OPERACJA
Program wykorzystujący luki CVE	Odmów dostępu	nd.	nd.	nd.
Program-żart	Poddaj kwarantannie	nd.	Poddaj kwarantannie	nd.
Trojany	Poddaj kwarantannie	nd.	Poddaj kwarantannie	nd.
Wirus	Wyczyść	Poddaj kwarantannie	Wyczyść	Poddaj kwarantannie
Wirus testowy	Odmów dostępu	nd.	Pomiń	nd.
narzędzie do kompresji	Poddaj kwarantannie	nd.	Poddaj kwarantannie	nd.
Prawdopodobne złośliwe oprogramowanie	Odmów dostępu lub operacja skonfigurowana przez użytkownika	nd.	Pomiń lub operacja skonfigurowana przez użytkownika	nd.

Typ wirusa/ złośliwego oprogramowania	Skanowanie w czasie rzeczywistym		Skanowanie ręczne/ Skanowanie zaplanowane/ Skanuj teraz	
	Pierwsza operacja	Druga operacja	Pierwsza operacja	Druga operacja
Inne złośliwe oprogramowanie	Wyczyść	Poddaj kwarantannie	Wyczyść	Poddaj kwarantannie

W przypadku prawdopodobnego złośliwego oprogramowania domyślana operacja to „Odmów dostępu" podczas skanowania w czasie rzeczywistym lub „Pomiń" podczas skanowania ręcznego, skanowania zaplanowanego lub operacji Skanuj teraz. Jeśli nie są to preferowane operacje, można zmienić je na Poddaj kwarantannie, Usuń lub Zmień nazwę.

Wykonaj te same operacje dla wszystkich typów wirusów/ złośliwego oprogramowania

Tę opcję należy wybrać, jeśli w przypadku wirusów/złośliwego oprogramowania wszystkich typów (z wyjątkiem prawdopodobnego wirusa/złośliwego oprogramowania) ma być wykonywana taka sama operacja. Jeśli jako pierwszą operację wybrano „Wyczyść", wybierz drugą operację, którą program OfficeScan wykona po pomyślnym zakończeniu czyszczenia. Jeśli pierwszą operacją nie jest „Wyczyść", nie można skonfigurować drugiej operacji.

Jeśli jako pierwsza operacja zostanie wybrana operacja „Wyczyść", program OfficeScan wykona drugą operację po wykryciu prawdopodobnego wirusa/złośliwego oprogramowania.

Użyj konkretnego działania w przypadku wirusa/złośliwego oprogramowania każdego typu

Należy ręcznie wybrać operację skanowania stosowaną względem wirusa / złośliwego oprogramowania każdego typu.

Dostępne są wszystkie operacje skanowania dla wszystkich typów wykrytych wirusów/ złośliwego oprogramowania z wyjątkiem prawdopodobnego wirusa/złośliwego

oprogramowania. Jeśli jako pierwszą operację wybrano „Wyczyść”, wybierz drugą operację, którą program OfficeScan wykona po pomyślnym zakończeniu czyszczenia. Jeśli pierwszą operacją nie jest „Wyczyść”, nie można skonfigurować drugiej operacji.

W przypadku prawdopodobnego wirusa/złośliwego oprogramowania dostępne są wszystkie operacje skanowania z wyjątkiem operacji „Wyczyść”.

Katalog kwarantanny

Jeśli operacją wykonywaną na zarażonym pliku jest „Poddaj kwarantannie”, Agent OfficeScan zakoduje plik i przeniesie go do tymczasowego katalogu kwarantanny w lokalizacji <*Folder instalacji agentar*>\SUSPECT, a następnie wyśle plik do wyznaczonego katalogu kwarantanny.

Uwaga

W przypadku konieczności uzyskania dostępu do zaszyfrowanych plików kwarantanny, można je przywrócić.

Szczegółowe informacje zawiera sekcja *Przywracanie zaszyfrowanych plików na stronie 7-51*.

Należy zaakceptować domyślny katalog kwarantanny, który jest zlokalizowany na komputerze serwera OfficeScan. Katalog jest podawany w formie adresu URL i zawiera nazwę hosta lub adres IP serwera.

- Jeśli serwer zarządza agentami IPv4 i IPv6, należy użyć nazwy hosta, aby wszyscy agenci mogli wysyłać na serwer pliki poddane kwarantannie.
- Jeśli serwer ma tylko adres IPv4 lub jest identyfikowany przy użyciu takiego adresu, tylko agenci wykorzystujący wyłącznie protokół IPv4 i agenci z dwoma stosami będą mogli wysyłać na serwer pliki poddane kwarantannie.
- Jeśli serwer ma tylko adres IPv6 lub jest identyfikowany przy użyciu takiego adresu, tylko agenci wykorzystujący wyłącznie protokół IPv6 i agenci z dwoma stosami będą mogli wysyłać na serwer pliki poddane kwarantannie.

Można także podać alternatywny katalog kwarantanny, wpisując lokalizację w postaci adresu URL, ścieżki UNC lub bezwzględnej ścieżki pliku. Agenci powinni mieć możliwość połączenia się z tym katalogiem alternatywnym. Na przykład katalog alternatywny powinien mieć adres IPv6, jeśli będzie odbierać pliki poddane

kwarantannie z agentów z dwoma stosami i agentów wykorzystujących wyłącznie protokół IPv6. Firma Trend Micro zaleca wyznaczenie katalogu alternatywnego z dwoma stosami poprzez identyfikację katalogu według nazwy hosta i użycie ścieżki UNC podczas wpisywania katalogu.

Wskazówki na temat okoliczności korzystania z adresu URL, ścieżki UNC i bezwzględnej ścieżki dostępu znajdują się w poniższej tabeli:

TABELA 7-14. Katalog kwarantanny

KATALOG KWARANTANNY	AKCEPTOWALNY FORMAT	PRZYKŁAD	UWAGI
Katalog na serwerze OfficeScan	URL	`http://<osceserver>`	Jest to katalog domyślny. Należy skonfigurować ustawienia katalogu, takie jak jego rozmiar. Szczegółowe informacje zawiera sekcja *Menedżer kwarantanny na stronie 14-63*.
	Ścieżka UNC	`\\<osceserver>\ofcscan\Virus`	

KATALOG KWARANTANNY	AKCEPTOWALNY FORMAT	PRZYKŁAD	UWAGI
Katalog na innym komputerze serwera OfficeScan (jeśli w sieci działają inne serwery OfficeScan)	URL	`http://<osceserver2>`	Należy się upewnić, że agenci mają dostęp do tego katalogu. W przypadku podania nieprawidłowego katalogu Agent OfficeScan przechowuje pliki kwarantanny w folderze SUSPECT, aż do momentu określenia prawidłowego katalogu kwarantanny. W dziennikach wirusów/złośliwego oprogramowania serwera wynik skanowania wpisywany jest jako „Nie można przesłać pliku poddanego kwarantannie do wskazanego folderu kwarantanny”. W razie użycia ścieżki UNC należy się upewnić, że folder kwarantanny jest udostępniony grupie „Wszyscy”, i że grupie tej przyznano uprawnienia do odczytu i zapisu.
	Ścieżka UNC	`\\<osceserver2>\ofcscan\Virus`	
Inny punkt końcowy w sieci	Ścieżka UNC	`\\<nazwa_komputera>\temp`	
Inny katalog na agencie OfficeScan	Ścieżka bezwzględna	`C:\temp`	

Utwórz kopie przed wyczyszczeniem

Jeśli program OfficeScan skonfigurowano tak, aby zarażone pliki były czyszczone, można włączyć opcję tworzenia ich kopii zapasowych. Dzięki temu w razie potrzeby plik będzie można w przyszłości przywrócić. Program OfficeScan koduje plik kopii zapasowej, by zabezpieczyć ją przed otwarciem, a następnie zachowuje plik w katalogu <*Folder instalacji agenta*>`\Backup`.

Aby przywrócić zakodowane pliki kopii zapasowej, patrz *Przywracanie zaszyfrowanych plików na stronie 7-51*.

Usługi Usuwania Szkód Services

Usługi Usuwania Szkód Services oczyszczają komputery z wirusów sieciowych oraz opartych na plikach, a także pozostałości wirusów i robaków (trojanów, wpisów w rejestrze, zainfekowanych plików).

Agent uruchamia Usługi Usuwania Szkód Services przed rozpoczęciem skanowania w poszukiwaniu wirusów/złośliwego oprogramowania lub po jego zakończeniu, w zależności od typu skanowania.

- Po uruchomieniu funkcji Skanowanie ręczne, Skanowanie zaplanowane lub Skanuj teraz Agent OfficeScan uruchamiania Usługi Usuwania Szkód Services, a następnie wykonuje skanowanie w poszukiwaniu wirusów/złośliwego oprogramowania. Podczas skanowania w poszukiwaniu wirusów/złośliwego oprogramowania agent może ponownie uruchomić Usługi Usuwania Szkód Services, jeśli wymagane jest czyszczenie.

- Podczas skanowania w czasie rzeczywistym Agent OfficeScan wykonuje najpierw skanowanie w poszukiwaniu wirusów/złośliwego oprogramowania, a następnie uruchamia Usługi Usuwania Szkód Services, jeśli jest to konieczne.

Można wybrać typ czyszczenia podczas działania usług Usuwania Szkód Services:

- **Czyszczenie standardowe**: Agent OfficeScan wykonuje następujące operacje podczas czyszczenia standardowego:
  - Wykrywa i usuwa aktywne trojany
  - Przerywa procesy tworzone przez trojany
  - Naprawia pliki systemowe, zmodyfikowane przez trojany
  - Usuwa pliki i aplikacje pozostawione przez trojany
- **Czyszczenie zaawansowane**: oprócz operacji czyszczenia standardowego, Agent OfficeScan powstrzymuje operacje fałszywego oprogramowania zabezpieczającego, nazywanego także FakeAV, a także niektóre warianty oprogramowania typu rootkit. Agent OfficeScan używa także reguł czyszczenia zaawansowanego, aby aktywnie wykrywać i zatrzymywać aplikacje wykazujące zachowanie oprogramowania FakeAV i oprogramowania typu rootkit.

Uwaga

Funkcja czyszczenia zaawansowanego zapewnia aktywną ochronę, ale powoduje zgłoszenie dużej liczby fałszywych alarmów.

Usługi Usuwania Szkód Services nie wykonują czyszczenia dla prawdopodobnego wirusa/złośliwego oprogramowania, chyba że wybrano opcję **Uruchom czyszczenie w przypadku wykrycia potencjalnego wirusa/złośliwego oprogramowania**. Tę opcję można wybrać tylko wtedy, gdy w przypadku prawdopodobnego wirusa/złośliwego oprogramowania nie wybrano opcji **Pomiń** ani **Odmów dostępu**. Jeśli na przykład Agent OfficeScan wykryje prawdopodobnego wirusa/złośliwe oprogramowanie podczas skanowania w czasie rzeczywistym, a wybrana operacja to Poddaj kwarantannie, Agent OfficeScan najpierw poddaje kwarantannie zarażony plik, a następnie wykonuje czyszczenie, jeśli to konieczne. Typ czyszczenia (standardowy lub zaawansowany) jest zależny od dokonanego wyboru.

Wyświetl powiadomienie, jeśli wykryty zostanie wirus/złośliwe oprogramowanie

Gdy program OfficeScan wykryje wirusa / złośliwe oprogramowanie podczas skanowania w czasie rzeczywistym lub skanowania zaplanowanego, może o tym poinformować użytkownika, wyświetlając odpowiednie powiadomienie.

Aby zmodyfikować powiadomienie programu, wybierz opcję **Wirus/złośliwe oprogramowanie** z listy rozwijanej **Typ** w obszarze **Administracja** > **Powiadomienia** > **Agent**.

Wyświetl powiadomienie, jeśli wykryty zostanie potencjalny wirus/złośliwe oprogramowanie

Gdy program OfficeScan wykryje prawdopodobnego wirusa/złośliwe oprogramowanie podczas skanowania w czasie rzeczywistym lub skanowania zaplanowanego, może o tym poinformować użytkownika, wyświetlając odpowiednie powiadomienie.

Aby zmodyfikować powiadomienie programu, wybierz opcję **Wirus/złośliwe oprogramowanie** z listy rozwijanej **Typ** w obszarze **Administracja** > **Powiadomienia** > **Agent**.

Przywracanie plików poddanych kwarantannie

Istnieje możliwość przywrócenia plików poddanych kwarantannie przez program OfficeScan, jeśli podejrzewasz, że wykrycie było nieprawidłowe. Funkcja centralnego przywracania kwarantanny umożliwia wyszukanie plików w katalogu kwarantanny i wykonanie weryfikacji SHA1 w celu upewnienia się, że pliki do przywrócenia nie zostały zmodyfikowane w żaden sposób.

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów wybierz domenę lub dowolnego agenta.
3. Kliknij opcje **Zadania** > **Centralne przywracanie kwarantanny**.

   Zostanie wyświetlony ekran **Centralne przywracanie kwarantanny**.
4. Wpisz nazwę pliku danych do przywrócenia w polu **Zarażony plik/obiekt**.
5. Opcjonalnie podaj okres, nazwę zagrożenia bezpieczeństwa i ścieżkę pliku danych.
6. Kliknij przycisk **Wyszukaj**.

   Zostanie wyświetlony ekran **Centralne przywracanie kwarantanny** z wynikami wyszukiwania.
7. Wybierz opcję **Dodaj przywrócony plik do listy wykluczeń na poziomie domeny**, aby wszyscy Agenci OfficeScan w domenach, w których są przywracane pliki, dodali plik do lista wykluczeń skanowania.

   Dzięki temu program OfficeScan nie wykryje pliku jako zagrożenia podczas skanowania w przyszłości.
8. Opcjonalnie wpisz wartość SHA1 pliku w celu weryfikacji.
9. Wybierz na liście pliki do przywrócenia i kliknij polecenie **Przywróć**.

Porada

Aby wyświetlić poszczególnych agentów OfficeScan, którzy przywracają plik, kliknij łącze w kolumnie **Punkty końcowe**.

10. Kliknij przycisk **Zamknij** w oknie dialogowym potwierdzenia.

    Aby sprawdzić, czy program OfficeScan pomyślnie przywrócił plik poddany kwarantannie, przejdź do sekcji *Wyświetlanie dzienników centralnego przywracania kwarantanny na stronie 7-110*.

Przywracanie zaszyfrowanych plików

W celu zapobiegania otwieraniu zarażonych plików program OfficeScan szyfruje je w następujących przypadkach:

- przed poddaniem pliku kwarantannie,
- podczas tworzenia kopii zapasowej pliku przed jego wyczyszczeniem.

Program OfficeScan zapewnia narzędzie, które odszyfrowuje, a następnie przywraca plik, gdy jest wymagany dostęp do zapisanych w nim informacji. Program OfficeScan może odszyfrowywać następujące pliki:

TABELA 7-15. Pliki, które program OfficeScan może odszyfrowywać i przywracać

PLIK	OPIS
Pliki poddane kwarantannie na punkcie końcowym agenta	Te pliki są przechowywane w folderze <*Folder instalacji agenta*>`\SUSPECT\Backup` i są automatycznie usuwane po 7 dniach. Są one również przesyłane do wyznaczonego katalogu kwarantanny znajdującego się na serwerze OfficeScan.
Pliki poddane kwarantannie w wyznaczonym katalogu kwarantanny	Domyślnie ten katalog jest zlokalizowany na komputerze serwera OfficeScan. Szczegółowe informacje zawiera sekcja *Katalog kwarantanny na stronie 7-45*.

PLIK	OPIS
Kopie zapasowe zaszyfrowanych plików	Są to kopie zapasowe zarażonych plików, których program OfficeScan nie mógł wyczyścić. Te pliki są przechowywane w lokalizacji `<Folder instalacji agenta>\Backup`. Aby przywrócić te pliki, należy je przenieść do folderu `<Folder instalacji agenta>\SUSPECT\Backup`. Program OfficeScan tworzy kopie zapasowe i szyfruje pliki przed wyczyszczeniem tylko w przypadku wybrania opcji **Przed czyszczeniem utwórz kopię zapasową** przez przejście do ekranu **Agenci** > **Zarządzanie agentami** i kliknięcie karty **Ustawienia** > **Ustawienia skanowania** > **{typ skanowania}** > **Operacja**.

OSTRZEŻENIE!

Przywracanie zarażonego pliku może spowodować przeniesienie wirusa / złośliwego oprogramowania na inne pliki i komputery. Przed przywróceniem pliku należy odizolować zarażony punkt końcowy i przenieść ważne pliki z tego punktu końcowego do lokalizacji zapasowej.

Odszyfrowywanie i przywracanie plików

Procedura

- Jeśli plik jest zapisany na punkt końcowy Agent OfficeScan:
  a. Otwórz wiersz polecenia i przejdź do lokalizacji <*Folder instalacji agenta*>.
  b. Uruchom program `VSEncode.exe`, klikając dwukrotnie plik lub wpisując następujący ciąg w wierszu polecenia:

     ```
     VSEncode.exe /u
     ```

     Zastosowanie tego parametru powoduje wyświetlenie ekranu z listą plików przechowywanych w lokalizacji `<Folder instalacji agenta>\SUSPECT\Backup`.
  c. Zaznacz plik przeznaczony do przywrócenia i kliknij polecenie **Przywróć**. Narzędzie może jednocześnie przywrócić tylko jeden plik.

d. Na wyświetlonym ekranie określ folder, do którego ma zostać przywrócony plik.

e. Kliknij przycisk **Ok**. Plik zostanie przywrócony do wskazanego folderu.

Uwaga

Może się zdarzyć, że program OfficeScan ponownie przeskanuje plik i uzna go za zarażony natychmiast po jego przywróceniu. Aby uniemożliwić skanowanie pliku, należy go dodać do lista wykluczeń skanowania. Szczegółowe informacje można znaleźć w części *Wykluczenia skanowania na stronie 7-35*.

f. Po zakończeniu przywracania plików kliknij polecenie **Zakończ**.

- Jeśli plik jest zapisany na serwerze OfficeScan lub w niestandardowym katalogu kwarantanny:

  a. Jeśli plik jest zapisany na komputerze serwera OfficeScan, otwórz wiersz polecenia i przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\VSEncrypt`.

  Jeśli plik jest zapisany w niestandardowym katalogu kwarantanny, przejdź do lokalizacji `<Folder instalacji serwera>\PCCSRV\Admin\Utility` i skopiuj folder `VSEncrypt` na punkt końcowy, na którym znajduje się niestandardowy katalog kwarantanny.

  b. Utwórz plik tekstowy i wpisz pełną ścieżkę plików, które chcesz zaszyfrować lub odszyfrować.

  Aby na przykład przywrócić pliki znajdujące się w lokalizacji `C:\Moje dokumenty\Raporty`, w pliku tekstowym należy wpisać `C:\Moje dokumenty\Raporty\*.*`.

  Pliki poddane kwarantannie na komputerze serwera OfficeScan są przechowywane w lokalizacji `<Folder instalacji serwera>\PCCSRV\Virus`.

  c. Zapisz plik tekstowy z rozszerzeniem `INI` lub `TXT`. Plik można na przykład zapisać na dysku `C:` pod nazwą `DoZaszyfrowania.ini`.

  d. Otwórz wiersz polecenia i przejdź do katalogu, w którym znajduje się folder `VSEncrypt`.

e. Uruchom plik `VSEncode.exe`, wpisując:

```
VSEncode.exe /d /i <lokalizacja pliku INI lub TXT>
```

Gdzie:

`<lokalizacja pliku INI lub TXT>` jest ścieżką pliku `INI` lub `TXT`, który utworzono (np. `C:\DoZaszyfrowania.ini`).

f. Użyj innych parametrów do wydawania różnych poleceń.

TABELA 7-16. Parametry przywracania

PARAMETR	OPIS
Brak (brak parametru)	Szyfruj pliki
/d	Odszyfruj pliki
/debug	Utwórz dziennik diagnostyczny i zapisz go na punkcie końcowym. Na punkcie końcowym agenta OfficeScan dziennik diagnostyki `VSEncrypt.log` jest tworzony w lokalizacji `<Folder instalacji agenta>`.
/o	Zastąp zaszyfrowany lub odszyfrowany plik, jeżeli już istnieje
/f <nazwa pliku>	Szyfruj lub odszyfruj pojedynczy plik
/nr	Nie przywracaj oryginalnej nazwy pliku
/v	Wyświetl informacje o narzędziu
/u	Uruchom interfejs użytkownika narzędzia
/r <Folder docelowy>	Folder, do którego ma zostać przywrócony plik
/s <Oryginalna nazwa pliku>	Nazwa oryginalnego zaszyfrowanego pliku

Można na przykład wpisać `VSEncode [/d] [/debug]`, aby odszyfrować pliki w folderze `Suspect` (folder z podejrzanymi plikami) i utworzyć dziennik diagnostyczny. W przypadku szyfrowania lub odszyfrowywania pliku program OfficeScan tworzy zaszyfrowany lub odszyfrowany plik w tym samym

katalogu. Przed szyfrowaniem i odszyfrowaniem pliku należy się upewnić, że nie jest on zablokowany.

Operacje skanowania w poszukiwaniu oprogramowania spyware/grayware

Operacja skanowania wykonywana przez program OfficeScan zależy od typu skanowania, podczas którego wykryto oprogramowanie spyware/grayware. Szczególne operacje można konfigurować dla każdego rodzaju wirusa/złośliwego oprogramowania, ale dla wszystkich rodzajów spyware/grayware może zostać skonfigurowana tylko jedna operacja. Przykładowo, w przypadku wykrycia przez program OfficeScan oprogramowania spyware/grayware podczas skanowania ręcznego (typ skanowania) zagrożone zasoby systemowe zostaną wyczyszczone (operacja).

Informacje na temat różnych rodzajów oprogramowania spyware/grayware można znaleźć w części *Oprogramowanie spyware i grayware na stronie 7-5*.

Uwaga

Operacje skanowania w poszukiwaniu spyware/grayware można konfigurować tylko z poziomu konsoli Web. Konsola agenta OfficeScan nie umożliwia dostępu do tych ustawień.

Program OfficeScan wykonuje względem oprogramowania spyware/grayware operacje podane w poniższej tabeli.

TABELA 7-17. Operacje skanowania w poszukiwaniu oprogramowania spyware/grayware

OPERACJA	OPIS
Wyczyść	Program OfficeScan kończy działanie procesu lub usuwa wpisy rejestru, pliki, pliki cookie i skróty. Po wyczyszczeniu oprogramowania spyware/grayware Agenci OfficeScan tworzą kopie zapasowe danych spyware/grayware, które można przywrócić, gdy dostęp do tych danych będzie bezpieczny. Szczegółowe informacje można znaleźć w części *Przywracanie spyware/grayware na stronie 7-59*.
Pomiń	Program OfficeScan nie wykonuje żadnej operacji na wykrytych składnikach spyware/grayware, ale w dziennikach tworzy wpisy o wykryciu oprogramowania spyware/grayware. Ta operacja może być wykonywana tylko w przypadku skanowania ręcznego, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz. Podczas funkcji Skanowanie w czasie rzeczywistym operacją tą jest „Odmów dostępu”. Jeśli wykryte oprogramowanie spyware/grayware znajduje się na liście elementów dozwolonych program OfficeScan nie wykonuje żadnej operacji. Szczegółowe informacje można znaleźć w części *Lista dozwolonych spyware/grayware na stronie 7-57*.
Odmów dostępu	Program OfficeScan odmawia dostępu (kopiowania, otwierania) do wykrytych składników spyware/grayware. Tę operację można wykonać tylko podczas skanowania w czasie rzeczywistym. Podczas skanowania ręcznego, skanowania zaplanowanego i używania funkcji Skanuj teraz, operacją tą jest „Pomiń”.

Wyświetl powiadomienie programu po wykryciu spyware/grayware

Gdy program OfficeScan wykryje oprogramowanie spyware/grayware podczas skanowania w czasie rzeczywistym lub skanowania zaplanowanego, może o tym poinformować użytkownika, wyświetlając odpowiednie powiadomienie.

Aby zmodyfikować powiadomienie programu, wybierz opcję **Oprogramowanie spyware/grayware** z listy rozwijanej **Typ** w obszarze **Administracja** > **Powiadomienia** > **Agent**.

Lista dozwolonych spyware/grayware

Program OfficeScan prowadzi listę dozwolonych programów spyware/grayware, na której znajdują się pliki lub aplikacje, które nie mają być traktowane jako spyware lub grayware. Gdy określony program typu spyware/grayware zostanie wykryty podczas skanowania, program OfficeScan sprawdza listę elementów dozwolonych i nie wykonuje żadnej operacji, jeśli znajdzie dopasowanie.

Listę dozwolonych można stosować na jednym lub wielu agentach i domenach albo na wszystkich agentach zarządzanych przez serwer. Lista elementów dozwolonych dotyczy wszystkich typów skanowania, co oznacza, że taka sama lista jest stosowana podczas skanowania ręcznego, skanowania w czasie rzeczywistym, skanowania zaplanowanego oraz skanowania za pomocą funkcji Skanuj teraz.

Dodawanie wcześniej wykrytego oprogramowania spyware/grayware do listy Dozwolone

Procedura

1. Przejdź do jednej z następujących opcji:
   - **Agenci** > **Zarządzanie agentami**
   - **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa**
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, albo wybierz określone domeny lub agentów.
3. Kliknij polecenie **Dzienniki** > **Dzienniki spyware/grayware** lub **Wyświetl dzienniki** > **Dzienniki spyware/grayware**.
4. Określ kryteria dziennika i kliknij przycisk **Wyświetl dzienniki**.
5. Wybierz dzienniki i kliknij opcję **Dodaj do listy dozwolonych**.

6. Zastosuj listę dozwolonych programów spyware/grayware wyłącznie na wybranych komputerach agentów lub w określonych domenach.

7. Kliknij przycisk **Zapisz**. Wybrani agenci zastosują ustawienie, a serwer OfficeScan doda oprogramowanie spyware/grayware do listy elementów dozwolonych w sekcji **Agenci** > **Zarządzanie agentami** > **Ustawienia** > **Lista dozwolonych spyware/grayware**.

Uwaga

Program OfficeScan obsługuje do 1024 wpisów spyware/grayware na liście dozwolonych.

Zarządzanie listą dozwolonych spyware/grayware

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Lista dozwolonych spyware/grayware**.
4. W tabeli **Nazwy spyware/grayware** wskaż nazwę oprogramowania spyware/grayware. Aby zaznaczyć wiele nazw, podczas wybierania przytrzymaj naciśnięty klawisz CTRL.
   - Można również wpisać słowo kluczowe w polu **Wyszukaj** i kliknąć przycisk **Wyszukaj**. Program OfficeScan odświeży tabelę, wyświetlając nazwy odpowiadające wprowadzonemu słowu kluczowemu.
5. Kliknij przycisk **Dodaj**.

   Nazwy zostaną przeniesione do tabeli **Lista dozwolonych**.
6. Aby usunąć nazwy z listy dozwolonych, wybierz nazwy i kliknij przycisk **Usuń**. Aby zaznaczyć wiele nazw, podczas wybierania przytrzymaj naciśnięty klawisz CTRL.
7. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

- **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Przywracanie spyware/grayware

Po usunięciu oprogramowania spyware/grayware Agenci OfficeScan tworzą jego kopie zapasowe. Jeśli usunięte dane są uważane za nieszkodliwe, można powiadomić agenta online o chęci ich przywrócenia. Wybierz dane spyware/grayware do przywrócenia na podstawie tego, kiedy kopia zapasowa została wykonana.

Uwaga

Użytkownicy agentów OfficeScan nie mogą inicjować przywracania spyware/grayware i nie są powiadamiani o tym, jakie dane kopii zapasowej agent mógł przywrócić.

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów otwórz domenę, a następnie wybierz agenta.

   Uwaga

   Jednocześnie przywracanie spyware/grayware może wykonywać tylko jeden agent.

3. Kliknij kolejno opcje **Zadania** > **Przywracanie spyware/grayware**.
4. Aby zobaczyć elementy do przywrócenia dla każdego segmentu danych, należy kliknąć polecenie **Widok**.

   Zostanie wyświetlony nowy ekran. Kliknij przycisk **Wstecz**, aby powrócić do poprzedniego ekranu.

5. Wybierz segmenty danych, które mają zostać przywrócone.
6. Kliknij przycisk **Przywróć**.

   Program OfficeScan powiadomi o stanie przywracania. Sprawdź dzienniki przywracania oprogramowania spyware/grayware w celu uzyskania pełnego raportu. Szczegółowe informacje można znaleźć w części *Wyświetlanie dzienników przywracania po usunięciu oprogramowania spyware/grayware na stronie 7-115*.

Lista zaufanych programów

Program OfficeScan można tak skonfigurować, aby pomijał skanowanie zaufanych procesów w trakcie skanowania w czasie rzeczywistym lub w ramach monitorowania zachowań. Po dodaniu programu do listy zaufanych programów program OfficeScan nie poddaje skanowaniu w czasie rzeczywistym takiego programu ani żadnych procesów przez niego zainicjowanych. Dodanie zaufanych programów do listy zaufanych programów pozwala poprawić wydajność skanowania na punktach końcowych.

Uwaga

Pliki można dodać do listy zaufanych programów, jeśli są spełnione następujące warunki:

- Plik nie znajduje się w katalogu systemowym Windows.
- Plik ma ważny podpis cyfrowy.

Po dodaniu programu do listy zaufanych programów program OfficeScan automatycznie wyłącza go z następujących rodzajów skanowania:

- Sprawdzanie plików podczas skanowania w czasie rzeczywistym
- Monitorowanie zachowań
- Skanowanie procesów w czasie rzeczywistym

Konfigurowanie listy zaufanych programów

Lista zaufanych programów powoduje wykluczenie ze skanowania w czasie rzeczywistym i skanowania w ramach monitorowania zachowań programów i wszystkich procesów podrzędnych wywoływanych przez program.

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij kolejno **Ustawienia** > **Lista zaufanych programów**.
4. Wpisz pełną ścieżkę programu, który ma być wykluczony z listy.
5. Kliknij opcję **Dodaj do listy zaufanych programów**.
6. Aby usunąć program z listy, kliknij ikonę **Usuń**.
7. Aby wyeksportować listę zaufanych programów, kliknij przycisk **Eksportuj** i wybierz lokalizację pliku.

   Uwaga

   Program OfficeScan zapisuje listę w formacie `DAT`.

8. Aby zaimportować listę zaufanych programów, kliknij przycisk **Importuj** i wybierz lokalizację pliku.
   a. Kliknij przycisk **Przeglądaj** i wybierz lokalizację pliku `DAT`.
   b. Kliknij przycisk **Importuj**.
9. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.

- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Uprawnienia do skanowania i inne ustawienia

Użytkownicy mający przypisane uprawnienia do skanowania mają większą kontrolę nad sposobem skanowania plików przechowywanych na ich komputerach. Uprawnienia do skanowania umożliwiają użytkownikom lub agentowi OfficeScan wykonywanie następujących zadań:

- Użytkownicy mogą konfigurować ustawienia skanowania ręcznego, skanowania zaplanowanego i skanowania w czasie rzeczywistym. Szczegółowe informacje zawiera sekcja *Uprawnienia typu skanowania na stronie 7-62*.
- Użytkownicy mogą odłożyć, zatrzymać lub pominąć skanowanie zaplanowane. Szczegółowe informacje zawiera sekcja *Uprawnienia do skanowania zaplanowanego i inne ustawienia na stronie 7-65*.
- Użytkownicy mogą włączyć skanowanie wiadomości poczty POP3 w poszukiwaniu wirusów/złośliwego oprogramowania. Szczegółowe informacje zawiera sekcja *Uprawnienia do skanowania poczty i inne ustawienia na stronie 7-71*.
- Agent OfficeScan może używać ustawień pamięci podręcznej w celu zwiększenia wydajności skanowania. Szczegółowe informacje zawiera sekcja *Ustawienia pamięci podręcznej skanowania na stronie 7-73*.
- Użytkownicy mogą dostosowywać poszczególne listy zaufanych programów. Szczegółowe informacje zawiera sekcja *Uprawnienie do listy zaufanych programów na stronie 7-78*.

Uprawnienia typu skanowania

Użytkownikom można umożliwić konfigurowanie własnych ustawień skanowania ręcznego, skanowania w czasie rzeczywistym i skanowania zaplanowanego.

Przyznawanie uprawnień typu skanowania

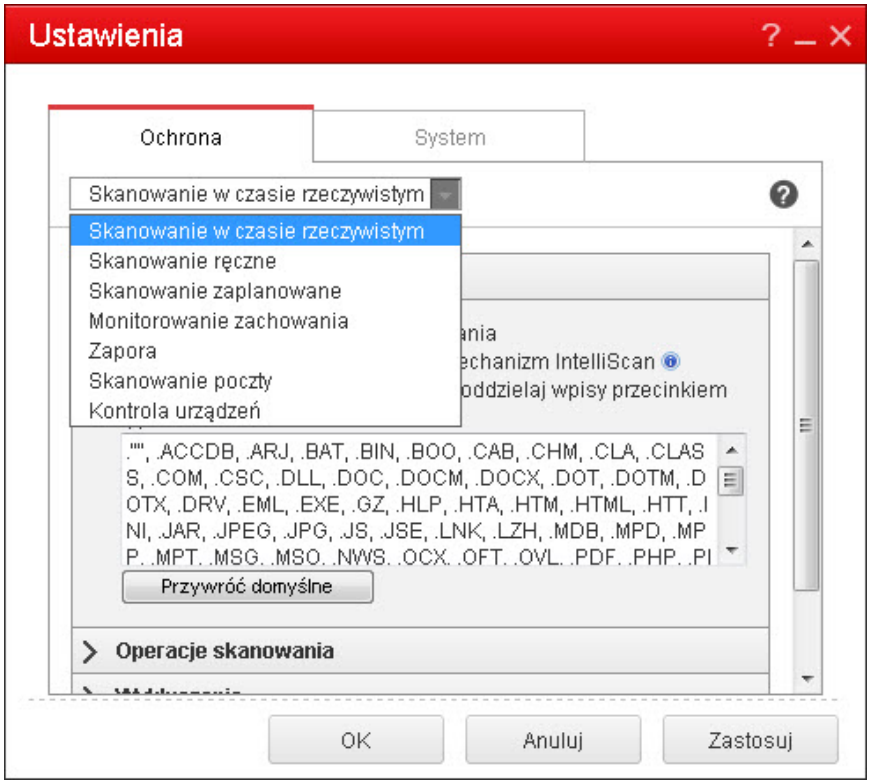
Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Na karcie **Uprawnienia** przejdź do sekcji **Skanowanie**.
5. Wybierz typy skanowania, które użytkownicy mogą konfigurować.
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Konfigurowanie ustawień skanowania agenta OfficeScan

Procedura

1. Kliknij prawym przyciskiem myszy ikonę agenta OfficeScan na pasku zadań i wybierz opcję **Otwórz konsolę agenta OfficeScan**.
2. Kliknij polecenie **Ustawienia** > **{Typ skanowania}**.



ILUSTRACJA 7-1. Ustawienia skanowania na konsoli agenta OfficeScan

3. Skonfiguruj następujące ustawienia:

   - Ustawienia skanowania w czasie rzeczywistym: Działania użytkownika na plikach, Pliki do skanowania, Ustawienia skanowania, Wykluczenia skanowania, Operacje skanowania
   - Ustawienia skanowania ręcznego: Pliki do skanowania, Ustawienia skanowania, Wykorzystanie procesora, Wykluczenia skanowania, Operacje skanowania
   - Ustawienia skanowania zaplanowanego: Harmonogram, Pliki do skanowania, Ustawienia skanowania, Wykorzystanie procesora, Wykluczenia skanowania, Operacje skanowania

4. Kliknij przycisk **OK**.

Uprawnienia do skanowania zaplanowanego i inne ustawienia

Jeśli skonfigurowano uruchamianie skanowania zaplanowanego na agencie, użytkownicy mogą odłożyć oraz pominąć lub zatrzymać skanowanie zaplanowane.

Odłóż skanowanie zaplanowane

Użytkownicy z uprawnieniami do uruchomienia funkcji „Odłóż skanowanie zaplanowane" mogą wykonać następujące działania:

- Odłóż skanowanie zaplanowane zanim się rozpocznie, a następnie określ czas, na jaki skanowanie ma zostać odłożone. Skanowanie zaplanowane można odłożyć tylko raz.
- Jeśli skanowanie zaplanowane jest uruchomione, można je zatrzymać i ponownie uruchomić w późniejszym czasie. Użytkownicy mogą następnie określić czas, który minie przed ponownym uruchomieniem skanowania. Gdy skanowanie zostanie ponownie uruchomione, wszystkie przeskanowane wcześniej pliki zostaną przeskanowane powtórnie. Skanowanie zaplanowane może zostać zatrzymane, a następnie uruchomione ponownie tylko raz.

Uwaga

Minimalny czas odłożenia dostępny dla użytkownika wynosi 15 minut. Maksymalny czas wynosi 12 godzin i 45 minut.

Czas odłożenia można zmienić, przechodząc do opcji **Agenci** > **Ustawienia agenta globalnego** na karcie **Ustawienia zabezpieczeń**. W sekcji **Ustawienia skanowania zaplanowanego** zmień ustawienie opcji **Odłóż skanowanie zaplanowane na __ godz. i __ min**.

Pomiń i zatrzymaj skanowanie zaplanowane

To uprawnienie pozwala użytkownikom podejmować następujące działania:

- Odkładać skanowanie zaplanowane zanim się rozpocznie.
- Zatrzymywać wykonywanie skanowania zaplanowanego.

Uwaga

Użytkownicy nie mogą pominąć ani zatrzymać skanowania zaplanowanego więcej niż jeden raz. Nawet po ponownym uruchomieniu systemu skanowanie zaplanowane wznawia skanowanie zgodnie z następnym zaplanowanym terminem.

Powiadomienie o uprawnieniach do skanowania zaplanowanego

Aby umożliwić użytkownikom korzystanie z uprawnień do skanowania zaplanowanego, należy im o nich przypomnieć, konfigurując program OfficeScan tak, aby przed rozpoczęciem skanowania zaplanowanego było wyświetlane odpowiednie powiadomienie.

Przyznawanie uprawnienia do skanowania zaplanowanego i wyświetlanie powiadomienia

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Na karcie **Uprawnienia** przejdź do sekcji **Skanowanie zaplanowane**.
5. Wybierz następujące opcje:
   - **Odłóż skanowanie zaplanowane**
   - **Pomiń i zatrzymaj skanowanie zaplanowane**
6. Kliknij kartę **Inne ustawienia** i przejdź do sekcji **Ustawienia skanowania zaplanowanego**.

7. Wybierz opcję **Wyświetl powiadomienie przed przeprowadzeniem skanowania zaplanowanego**.

   Po włączeniu tej opcji na punkcie końcowym agenta kilka minut przed rozpoczęciem skanowania zaplanowanego jest wyświetlane powiadomienie programu. Użytkownicy są powiadamiani o harmonogramie skanowania (dacie i godzinie) oraz o uprawnieniach do przeprowadzenia skanowania zaplanowanego, takich jak odkładanie, pomijanie lub zatrzymywanie.

   Uwaga

   Liczbę minut można określić. Aby określić liczbę minut, przejdź do opcji **Agenci** > **Ustawienia agenta globalnego** na karcie **Ustawienia zabezpieczeń**. W sekcji **Ustawienia skanowania zaplanowanego** zmień ustawienie opcji **Przypominaj użytkownikom o Skanowaniu zaplanowanym __ min przez rozpoczęciem skanowania**.

8. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

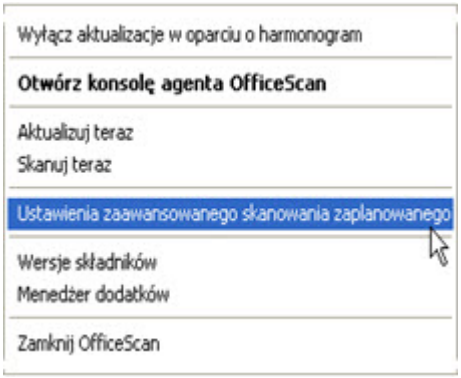
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Odkładanie/pomijanie i zatrzymywanie skanowania zaplanowanego na agencie

Procedura

- Jeżeli skanowanie zaplanowane nie rozpoczęło się:

  a. Kliknij prawym przyciskiem myszy ikonę agenta OfficeScan znajdującą się na pasku zadań i wybierz opcję **Ustawienia zaawansowanego skanowania zaplanowanego**.



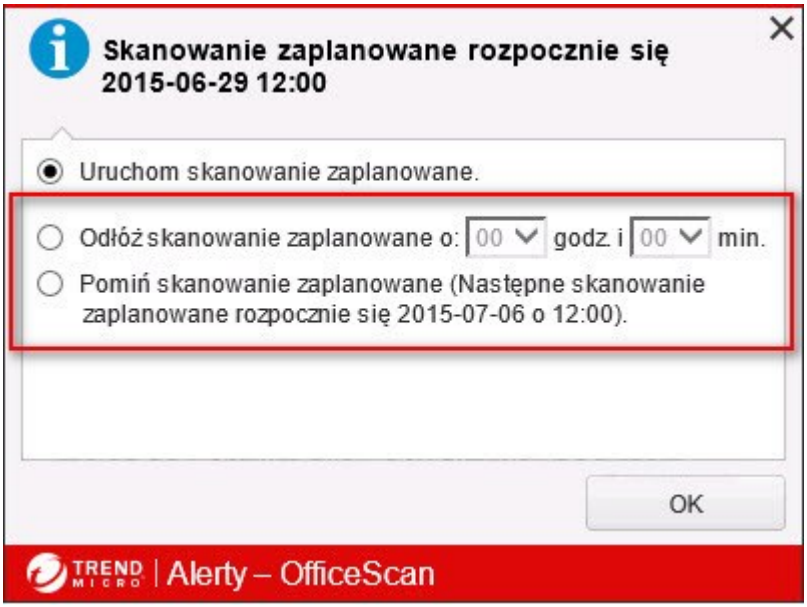
ILUSTRACJA 7-2. Opcja Zaawansowane ustawienia skanowania zaplanowanego

Uwaga

Użytkownicy nie muszą wykonywać tej czynności, jeśli powiadomienia programu są włączone, a komunikat wyświetla się kilka minut przed rozpoczęciem skanowania zaplanowanego. Szczegółowe informacje o powiadomieniach programu zawiera sekcja *Powiadomienie o uprawnieniach do skanowania zaplanowanego na stronie 7-66*.

b. Zostanie wyświetlone okno powiadomienia, na którym należy wybrać następujące opcje:

- **Odłóż skanowanie na __ godz. i __ min.**
- **Pomiń to skanowanie zaplanowane. Następne skanowanie zaplanowane zostanie uruchomione w dniu: <date> o <time>.**



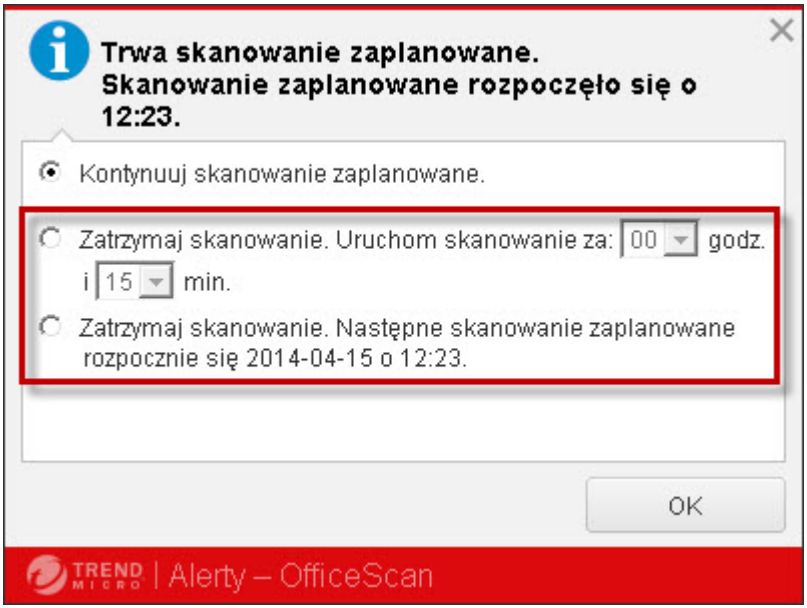
ILUSTRACJA 7-3. Uprawnienia do skanowania zaplanowanego na punkcie końcowym agenta OfficeScan

- Jeżeli skanowanie zaplanowane jest w toku:

  a. Kliknij prawym przyciskiem myszy ikonę agenta OfficeScan znajdującą się na pasku zadań i wybierz pozycję **Zaawansowane ustawienia skanowania zaplanowanego**.

  b. Zostanie wyświetlone okno powiadomienia, na którym należy wybrać następujące opcje:

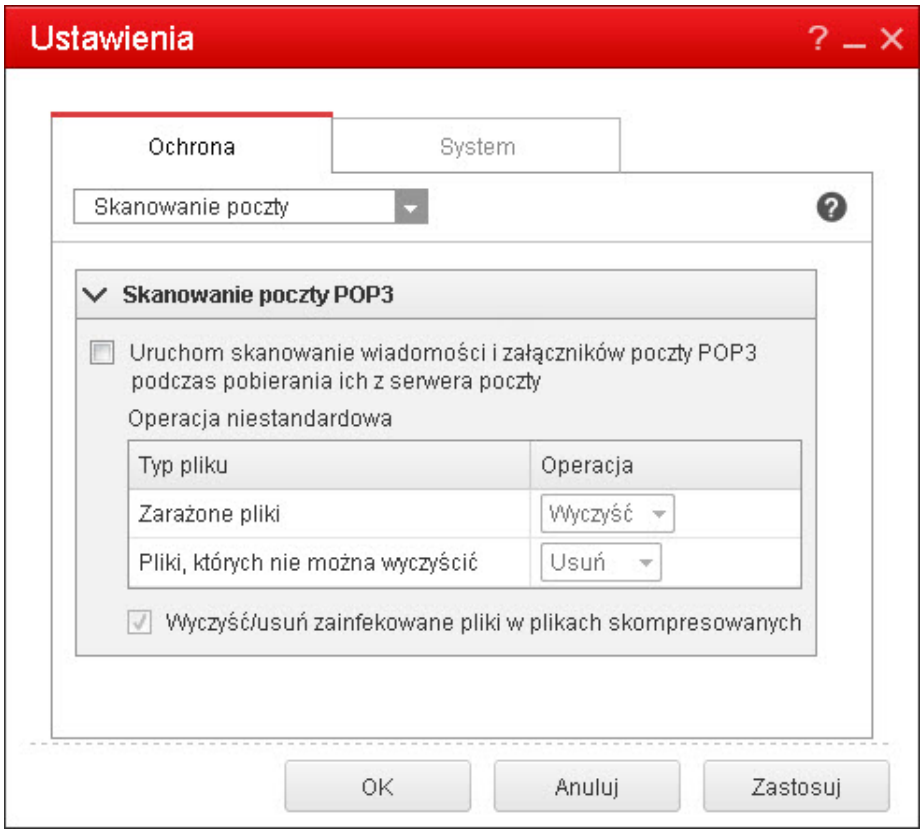
     - **Zatrzymaj skanowanie. Rozpocznij ponownie skanowanie po __ godz. i __ min.**
     - **Zatrzymaj skanowanie. Następne skanowanie zaplanowane zostanie uruchomione w dniu: <date> o <time>.**



ILUSTRACJA 7-4. Uprawnienia do skanowania zaplanowanego na punkcie końcowym agenta OfficeScan

Uprawnienia do skanowania poczty i inne ustawienia

Jeśli agenci ma przydzielone uprawnienie do skanowania poczty, w konsoli agenta OfficeScan jest wyświetlana opcja **Skanowanie poczty**. Opcja **Skanowanie poczty** powoduje wyświetlenie programu Skanowanie poczty POP3.



ILUSTRACJA 7-5. Ustawienia skanowania poczty na konsoli agenta OfficeScan

Poniższa tabela przedstawia program Skanowanie poczty POP3.

TABELA 7-18. Programy do skanowania poczty

SZCZEGÓŁY	OPIS
Przeznaczenie	Umożliwia skanowanie wiadomości e-mail POP3 w poszukiwaniu wirusów/złośliwego oprogramowania
Wymagania wstępne	• Musi zostać włączony przez administratorów w konsoli Web, zanim będzie możliwe jego użycie przez użytkowników **Uwaga** Aby włączyć skanowanie poczty POP3, patrz *Przyznawanie uprawnienia do skanowania poczty i włączanie skanowanie poczty POP3 na stronie 7-73*. • Operacja dla wirusów/złośliwego oprogramowania jest konfigurowana w konsoli agenta OfficeScan, a nie w konsoli Web
Obsługiwane typy skanowania	Skanowanie w czasie rzeczywistym Skanowanie jest wykonywane podczas pobierania wiadomości e-mail z serwera poczty POP3.
Wyniki skanowania	• Informacje o wykrytych zagrożeniach bezpieczeństwa są dostępne po zakończeniu skanowania • Wyniki skanowania nie są rejestrowane na ekranie **Dzienniki** konsoli agenta OfficeScan. • Wyniki skanowania nie są wysyłane do serwera
Inne szczegóły	Udostępnia usługę proxy OfficeScan NT (`TMProxy.exe`) wraz z funkcją Web Reputation

Przyznawanie uprawnienia do skanowania poczty i włączanie skanowanie poczty POP3

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Na karcie **Uprawnienia** przejdź do sekcji **Skanowanie poczty**.
5. Patrz **Wyświetl ustawienia Skanowanie poczty w konsoli agenta OfficeScan**.
6. Kliknij kartę **Inne ustawienia** i przejdź do sekcji **Ustawienia skanowania poczty POP3**.
7. Wybierz opcję **Skanuj pocztę POP3**.
8. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Ustawienia pamięci podręcznej skanowania

Agent OfficeScan może utworzyć pliki pamięci podręcznej podpisów cyfrowych i skanowania na żądanie, aby zwiększyć wydajność skanowania. Po uruchomieniu skanowania na żądanie agent OfficeScan sprawdza najpierw plik pamięci podręcznej podpisów cyfrowych, a następnie plik pamięci podręcznej skanowania na żądanie, aby

uzyskać informacje o plikach, które mają zostać wykluczone ze skanowania. Wykluczenie dużej liczby plików ze skanowania powoduje skrócenie czasu skanowania.

Pamięć podręczna podpisów cyfrowych

Plik pamięci podręcznej podpisów cyfrowych jest używany podczas skanowania ręcznego, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz. Agenci nie skanują plików, których sygnatury zostały dodane do pliku pamięci podręcznej podpisów cyfrowych.

Agent OfficeScan używa tej samej sygnatury podpisu cyfrowego, która jest używana przez monitorowanie zachowań, aby utworzyć plik pamięci podręcznej podpisów cyfrowych. Sygnatura Digital Signature Pattern zawiera listę plików uznanych przez firmę Trend Micro za wiarygodne, dzięki czemu można je wykluczyć ze skanowania.

Uwaga

Monitorowanie zachowań jest domyślnie wyłączone na platformach serwerowych Windows (obsługa nie jest dostępna w 64-bitowych systemach Windows XP, 2003 i Vista bez dodatku SP1). Jeśli jest włączona pamięć podręczna podpisów cyfrowych, Agenci OfficeScan na tych platformach pobierają sygnaturę podpisu cyfrowego w celu użycia w pamięci podręcznej i nie pobierają innych składników monitorowania zachowań.

Agenci tworzą plik pamięci podręcznej podpisów cyfrowych zgodnie z harmonogramem, który jest konfigurowany z poziomu konsoli Web. Agenci wykonują tę operację w celu:

- Dodania sygnatur nowych plików, które pojawiły się w systemie od momentu utworzenia poprzedniego pliku pamięci podręcznej.
- Usunięcia sygnatur plików, które zostały zmodyfikowane lub usunięte z systemu.

Podczas procesu budowania pamięci podręcznej agenci sprawdzają następujące foldery w poszukiwaniu wiarygodnych plików, a następnie dodają sygnatury tych plików do pliku pamięci podręcznej podpisów cyfrowych:

- `%PROGRAMFILES%`
- `%WINDIR%`

Proces tworzenia pamięci podręcznej nie wpływa na wydajność punktu końcowego, ponieważ agenci wykorzystują minimalną ilość zasobów systemowych w czasie tej operacji. Agenci mogą także wznowić zadanie tworzenia pamięci podręcznej, które zostało przerwane z jakiegoś powodu (na przykład po wyłączeniu hosta lub odłączeniu zasilacza bezprzewodowego punktu końcowego).

Pamięć podręczna skanowania na żądanie

Plik pamięci podręcznej skanowania na żądanie jest używany podczas skanowania ręcznego, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz. Agenci OfficeScan nie skanują plików, których pamięci podręczne zostały dodane do pliku pamięci podręcznej skanowania na żądanie.

Przy każdym uruchomieniu skanowania Agent OfficeScan sprawdza właściwości plików wolnych od zagrożeń. Jeśli plik wolny od zagrożeń nie został zmodyfikowany przez pewien czas (który można skonfigurować), Agent OfficeScan dodaje pamięć podręczną pliku do pliku pamięci podręcznej skanowania na żądanie. Podczas następnego skanowania plik nie będzie skanowany, jeśli jego pamięć podręczna nie wygasła.

Pamięć podręczna pliku wolnego od zagrożeń wygasa po określonej liczbie dni, którą także można skonfigurować. Kiedy skanowanie jest wykonywane w momencie wygaśnięcia pamięci podręcznej lub w późniejszym momencie, Agent OfficeScan usuwa wygasłą pamięć podręczną i skanuje plik w poszukiwaniu zagrożeń. Jeśli plik jest wolny od zagrożeń i nie został zmodyfikowany, pamięć podręczna pliku zostaje dodana z powrotem do pliku pamięci podręcznej skanowania na żądanie. Jeśli plik jest wolny od zagrożeń, ale został niedawno zmodyfikowany, pamięć podręczna pliku nie zostaje dodana do pamięci podręcznej i plik zostanie ponownie sprawdzony podczas następnego skanowania.

Pamięć podręczna pliku wolnego od zagrożeń wygasa, aby zapobiec wykluczeniu zarażonych plików ze skanowania, co przedstawiono w poniższych przykładach:

- Istnieje możliwość, że bardzo nieaktualny plik sygnatur spowodował potraktowanie zarażonego, niezmodyfikowanego pliku jako wolnego od zagrożeń. Gdyby pamięć podręczna nie wygasła, zarażony plik pozostawałby w systemie do momentu jego zmodyfikowania i wykrycia przez skanowanie w czasie rzeczywistym.
- Jeśli plik w pamięci podręcznej został zmodyfikowany, a skanowanie w czasie rzeczywistym nie było wykonywane podczas modyfikowania pliku, pamięć

podręczna musi wygasnąć, aby możliwe było przeskanowanie pliku w poszukiwaniu zagrożeń.

Liczba pamięci podręcznych dodanych do pliku pamięci podręcznej skanowania na żądanie jest zależna od typu skanowania i jego elementów docelowych. Na przykład liczba pamięci podręcznych może być mniejsza, jeśli Agent OfficeScan przeskanował tylko 200 z 1000 plików na punkcie końcowym podczas skanowania ręcznego.

Jeżeli skanowanie na żądanie jest uruchamiane często, plik pamięci podręcznej skanowania na żądanie powoduje znaczne skrócenie czasu skanowania. Jeśli zadanie skanowania jest wykonywane w sytuacji, gdy żadna pamięć podręczna nie wygasła, skanowanie zajmujące zwykle 12 minut może zostać skrócone do 1 minuty. Skrócenie liczby dni, przez jaką plik musi pozostawać niezmodyfikowany, oraz wydłużenie okresu wygaśnięcia pamięci podręcznej zwykle powoduje zwiększenie wydajności. Ponieważ pliki muszą pozostawać niezmodyfikowane przez relatywnie krótki czas, do pliku pamięci podręcznej można dodać więcej pamięci podręcznych. Pamięć podręczna wygasa także później, co oznacza pominięcie większej liczby plików podczas skanowania.

Jeżeli skanowanie na żądanie nie jest uruchamiane często, można wyłączyć pamięć podręczną skanowania na żądanie, ponieważ wygaśnie ona przed uruchomieniem następnego skanowania.

Konfigurowanie ustawień pamięci podręcznej skanowania

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Kliknij kartę **Inne ustawienia** i przejdź do sekcji **Ustawienia pamięci podręcznej skanowania**.
5. Skonfiguruj ustawienia pamięci podręcznej podpisów cyfrowych.

a. Wybierz opcję **Włącz pamięć podręczną podpisu cyfrowego**.

b. W polu **Kompiluj pamięć podręczną co __ dni** określ częstotliwość, z jaką agent agent będzie tworzyć pamięć podręczną.

6. Skonfiguruj ustawienia pamięci podręcznej skanowania na żądanie.

a. Wybierz opcję **Włącz pamięć podręczną skanowania na żądanie**.

b. W polu **Dodaj pamięć podręczną dla bezpiecznych plików niezmienionych przez __ dni** określ liczbę dni, przez jaką plik musi pozostawać niezmieniony, aby został umieszczony w pamięci podręcznej.

c. W polu **Pamięć podręczna dla każdego bezpiecznego pliku wygaśnie za __ dni** określ maksymalną liczbę dni, przez jaką pamięć podręczna będzie pozostawać w pliku pamięci podręcznej.

Uwaga

Aby zapobiec sytuacji, w której wszystkie pamięci podręczne dodane podczas skanowania wygasają w tym samym dniu, pamięci podręczne wygasają losowo w podanym okresie maksymalnej liczby dni. Jeśli na przykład 500 plików zostało dodanych do pamięci podręcznej dzisiaj, a maksymalna liczba dni wynosi 10, niewielka część pamięci podręcznych wygaśnie następnego dnia, a większość pamięci podręcznych wygaśnie w ciągu kolejnych dni. W dziesiątym dniu wygasną wszystkie pozostałe pamięci podręczne.

---

7. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

- **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.

- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Uprawnienie do listy zaufanych programów

Użytkownikom końcowym można przyznać uprawnienie do konfigurowania programu OfficeScan w taki sposób, aby pomijał skanowanie zaufanych procesów w trakcie skanowania w czasie rzeczywistym lub w ramach monitorowania zachowań. Po dodaniu programu do listy zaufanych programów program OfficeScan nie poddaje skanowaniu w czasie rzeczywistym takiego programu ani żadnych procesów przez niego zainicjowanych. Dodanie zaufanych programów do listy zaufanych programów pozwala poprawić wydajność skanowania na punktach końcowych.

Przyznawanie uprawnień do ustawień listy zaufanych programów.

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Na karcie **Uprawnienia** przejdź do sekcji **Lista zaufanych programów**.
5. Wybierz opcję **Wyświetl listę zaufanych programów w konsoli agenta OfficeScan**.
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Globalne ustawienia skanowania

Globalne ustawienia skanowania można zastosować na agentach OfficeScan, korzystając z różnych sposobów.

- Określone ustawienie skanowania można zastosować na wszystkich agentach zarządzanych przez serwer lub tylko na agentach, którzy mają przypisane określone uprawnienia do skanowania. Jeśli na przykład skonfigurowano czas odłożenia skanowania zaplanowanego, z tego ustawienia mogą korzystać tylko agenci z uprawnieniem odkładania skanowania zaplanowanego.
- Określone ustawienie skanowania można zastosować względem wszystkich typów skanowania lub tylko względem określonego typu skanowania. Na przykład na punktach końcowych, na których jest jednocześnie zainstalowany serwer OfficeScan i Agent OfficeScan, można wykluczyć ze skanowania bazę danych serwera OfficeScan. To ustawienie jest jednak stosowane tylko podczas skanowania w czasie rzeczywistym.
- Określone ustawienie skanowania można zastosować tylko podczas skanowania w poszukiwaniu wirusów / złośliwego oprogramowania lub tylko podczas skanowania w poszukiwaniu oprogramowania spyware/grayware albo w obu przypadkach. Tryb oceny można na przykład stosować tylko podczas skanowania w poszukiwaniu oprogramowania spyware/grayware.

Konfigurowanie globalnych ustawień skanowania

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Kliknij kartę **Ustawienie zabezpieczeń** i skonfiguruj globalne ustawienia skanowania w każdej dostępnej sekcji.
   - *Sekcja ustawień skanowania na stronie 7-81*
   - *Sekcja ustawień skanowania zaplanowanego na stronie 7-87*
3. Kliknij kartę **System**.

4. W sekcji **Ustawienia usługi Certified Safe Software Service** skonfiguruj ustawienie **Włącz usługę Certified Safe Software Service dla monitorowania zachowania, zapory i skanowania oprogramowania antywirusowego**.

   Usługa Certified Safe Software przeszukuje centra danych firmy Trend Micro w celu weryfikacji bezpieczeństwa programu wykrytego przez blokowanie działania złośliwego oprogramowania, monitorowanie zdarzeń, zaporę lub skanowanie oprogramowania antywirusowego. Należy włączyć włączyć usługę Certified Safe Software, aby zmniejszyć prawdopodobieństwo fałszywych alarmów.

   Uwaga

   Przed włączeniem usługi Certified Safe Software Service należy się upewnić, że Agenci OfficeScan mają skonfigurowane prawidłowe ustawienia proxy (szczegółowe informacje zawiera sekcja *Ustawienia serwera proxy agenta OfficeScan na stronie 15-52*). Nieprawidłowe ustawienia serwera proxy lub wadliwe połączenie z Internetem mogą być przyczyną opóźnień lub niepowodzenia odbioru odpowiedzi z centrów danych firmy Trend Micro, przez co monitorowane programy będą sprawiać wrażenie zawieszonych.

   Ponadto Agenci OfficeScan korzystający wyłącznie z protokołu IPv6 nie mogą bezpośrednio przeszukiwać centrów danych firmy Trend Micro. Aby umożliwić agentom OfficeScan nawiązanie połączenia z centrami danych firmy Trend Micro, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.

5. Kliknij kartę **Sieć**.

6. W sekcji **Ustawienia przepustowości dziennika wirusów / złośliwego oprogramowania** skonfiguruj ustawienie **Włącz na agencie OfficeScan tworzenie jednego wpisu dziennika w przypadku ponownego wykrycia tego samego wirusa/złośliwego oprogramowania w ciągu godziny**.

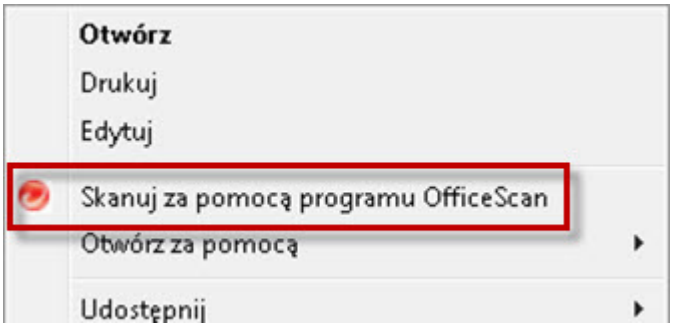
   Program OfficeScan łączy zapisy w dzienniku wirusów w przypadku wykrycia wielokrotnej infekcji tym samym wirusem lub złośliwym oprogramowaniem w krótkim czasie. Program OfficeScan może wielokrotnie wykryć pojedynczego wirusa/złośliwe oprogramowanie, co powoduje szybkie zapełnianie dziennika wirusów/złośliwego oprogramowania i zużywanie przepustowości sieci, gdy Agent OfficeScan wysyła informacje dziennika do serwera. Włączenie tej funkcji pozwala zredukować zarówno liczbę wpisów wirusów/złośliwego oprogramowania

w dzienniku, jak i część przepustowości sieci zajmowaną przez agentów OfficeScan podczas zgłaszania informacji dziennika wirusów do serwera.

7. Kliknij kartę **Kontrola agentów**.

8. W sekcji **Ustawienia ogólne** skonfiguruj ustawienie **Dodaj opcję Skanowanie ręczne do menu podręcznego systemu Windows na punktach końcowych**.

   Gdy to ustawienie jest włączone, wszyscy Agenci OfficeScan zarządzani przez serwer dodają opcję **Skanuj za pomocą programu OfficeScan** do menu podręcznego w Eksploratorze Windows. Gdy użytkownik kliknie prawym przyciskiem myszy plik lub folder na pulpicie systemu Windows lub w programie Eksplorator Windows, a następnie wybierze tę opcję, wybrana lokalizacja zostanie przeskanowana pod względem wirusów i złośliwego oprogramowania oraz pod względem oprogramowania spyware/grayware.



ILUSTRACJA 7-6. Opcja Skanuj za pomocą programu OfficeScan

9. Kliknij przycisk **Zapisz**.

Sekcja ustawień skanowania

Sekcja **Ustawienia skanowania** na karcie **Ustawienia zabezpieczeń** ekranu **Ustawienia agenta globalnego** umożliwia administratorom skonfigurowanie następujących elementów:

- *Wyklucz folder bazy danych serwera OfficeScan ze skanowania w czasie rzeczywistym na stronie 7-82*

Wyklucz folder bazy danych serwera OfficeScan ze skanowania w czasie rzeczywistym

Jeśli na tym samym punkcie końcowym jest zainstalowany Agent OfficeScan i serwer OfficeScan, podczas skanowania w czasie rzeczywistym Agent OfficeScan nie skanuje bazy danych serwera pod względem wirusów i złośliwego oprogramowania oraz pod względem oprogramowania spyware/grayware.

Porada

To ustawienie należy włączyć w celu uniknięcia uszkodzenia bazy danych podczas skanowania.

Wyklucz ze skanowania foldery i pliki serwera Microsoft Exchange

Jeśli na tym samym punkcie końcowym jest zainstalowany Agent OfficeScan i serwer Microsoft Exchange 2000/2003, podczas skanowania ręcznego, skanowania w czasie rzeczywistym, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz program OfficeScan nie skanuje folderów Microsoft Exchange pod kątem wirusów/złośliwego oprogramowania oraz pod względem oprogramowania spyware/grayware.

- Następujące foldery w folderze `\Exchsrvr\Mailroot\vsi 1`: `Queue`, `PickUp` i `BadMail`
- Folder `.\Exchsrvr\mdbdata`, łącznie z następującymi plikami: `priv1.stm`, `priv1.edb`, `pub1.stm` i `pub1.edb`

- `.\Exchsrvr\Storage Group`

W przypadku programu Microsoft Exchange 2007 lub nowszego należy ręcznie dodać foldery do lista wykluczeń skanowania. Szczegółowe informacje na temat wykluczenia skanowania można znaleźć w witrynie internetowej:

http://technet.microsoft.com/en-us/library/bb332342.aspx

Opis poszczególnych etapów konfiguracji lista wykluczeń skanowania znajduje się w *Wykluczenia skanowania na stronie 7-35*.

Włącz odroczone skanowanie w odniesieniu do operacji na plikach

Administratorzy mogą skonfigurować program OfficeScan do odroczenia skanowania plików. Program OfficeScan umożliwia użytkownikowi skopiowanie plików, a następnie skanuje te pliku po zakończeniu procesu kopiowania. Odroczone skanowanie pozwala podnieść wydajność procesów kopiowania i skanowania.

Uwaga

Odroczone skanowanie wymaga silnika skanowania antywirusowego (VSAPI) w wersji 9.713 lub nowszej. Szczegółowe informacje na temat aktualizacji serwera zawiera sekcja *Ręczna aktualizacja serwera OfficeScan na stronie 6-27*.

Włączanie ochrony przed złośliwym oprogramowaniem dla wstępnego rozruchu na punktach końcowych

OfficeScan obsługuje funkcję ochrony przed złośliwym oprogramowaniem dla wstępnego rozruchu jako część standardu bezpiecznego rozruchu, aby zapewnić ochronę punktów końcowych podczas rozruchu. Administratorzy mogą włączyć tę funkcję w celu uruchamiania agentów OfficeScan podczas rozruchu punktów końcowych, zanim zostaną uruchomione sterowniki oprogramowania innych firm. Ta funkcja umożliwia agentom OfficeScan wykrywanie złośliwego oprogramowania podczas procesu rozruchu.

Po przeskanowaniu wszystkich sterowników oprogramowania innych firm agent OfficeScan zgłasza informacje klasyfikacji sterowników do jądra systemu. Administratorzy mogą definiować operacje na podstawie klasyfikacji sterowników

w zasadach grupy systemu Windows i wyświetlać wyniki skanowania w Dzienniku zdarzeń na punktach końcowych.

Uwaga

Funkcja ochrony przed złośliwym oprogramowaniem dla wstępnego rozruchu jest obsługiwana tylko w systemach Windows 8, Windows Server 2012 i nowszych wersjach.

Wyczyść/usuń zainfekowane pliki w plikach skompresowanych

Jeśli agenci zarządzani przez serwer wykryją wirusa/złośliwe oprogramowanie w skompresowanych plikach (podczas skanowania ręcznego, skanowania w czasie rzeczywistym, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz) i dodatkowo są spełnione poniższe warunki, agenci oczyszczą lub usuną zarażone pliki.

- Operacje, które zostaną przeprowadzone przez program OfficeScan, to „Wyczyść" lub „Usuń". Aby sprawdzić, jakie operacje są wykonywane przez program OfficeScan na zarażonych plikach, należy przejść do karty **Agenci** > **Zarządzanie agentami > Ustawienia** > **Ustawienia skanowania** > **{Typ skanowania}** > **Operacja**.
- Należy włączyć to ustawienie. Włączenie tego ustawienia może spowodować wzrost zużycia zasobów punktu końcowego podczas skanowania oraz wydłużyć czas skanowania. Wynika to z faktu, że program OfficeScan dekompresuje skompresowany plik, zarażone pliki są czyszczone lub usuwane, a następnie plik jest ponownie kompresowany.
- Obsługiwany jest format skompresowanego pliku. W programie OfficeScan obsługiwane są tylko niektóre formaty kompresji bazujące na algorytmie ZIP, w tym ZIP i Office Open XML. Format Office Open XML jest domyślnym formatem dla aplikacji pakietu Microsoft Office 2007 takich, jak Excel, PowerPoint i Word.

  Uwaga

  W celu uzyskania pełnej listy obsługiwanych formatów kompresji skontaktuj się z działem pomocy technicznej.

Przykład: skanowanie w czasie rzeczywistym jest skonfigurowane tak, aby zarażone wirusem pliki były usuwane. Po zdekompresowaniu pliku o nazwie `abc.zip` i wykryciu

w nim zarażonego pliku `123.doc` program OfficeScan usuwa plik `123.doc`, a następnie ponownie kompresuje plik `abc.zip`. Dostęp do skompresowanego pliku jest teraz bezpieczny.

W poniższej tabeli przedstawiono opis sytuacji, gdy którykolwiek z warunków nie zostanie spełniony.

TABELA 7-19. Scenariusze i wyniki skompresowanych plików

STAN USTAWIENIA „WYCZYŚĆ/ USUŃ ZARAŻONE PLIKI W PLIKACH SKOMPRESOWANYCH”	OPERACJA, KTÓRĄ PROGRAM OFFICESCAN MA WYKONAĆ	FORMAT SKOMPRESOWANEGO PLIKU	WYNIK
Włączone	Wyczyść lub Usuń	Nieobsługiwane Przykład: plik `def.rar` zawiera zarażony plik `123.doc`.	Program OfficeScan szyfruje plik `def.rar`, ale plik `123.doc` nie zostaje wyczyszczony, usunięty, ani też nie jest wykonywana na nim inna operacja.
Wyłączone	Wyczyść lub Usuń	Obsługiwany/ nieobsługiwany Przykład: plik `abc.zip` zawiera zarażony plik `123.doc`.	Program OfficeScan nie czyści, nie usuwa ani też nie wykonuje innych operacji na plikach `def.rar` i `123.doc`.

Stan ustawienia „Wyczyść/ usuń zarażone pliki w plikach skompresowanych”	Operacja, którą program OfficeScan ma wykonać	Format skompresowanego pliku	Wynik
Włączone/ wyłączone	Ani Wyczyść, ani Usuń (operacje: Zmień nazwę, Poddaj kwarantannie, Odmowa dostępu lub Zezwól)	Obsługiwany/ nieobsługiwany Przykład: plik `abc.zip` zawiera zarażony plik `123.doc`.	Operacja określona w programie OfficeScan (Zmień nazwę, Poddaj kwarantannie, Odmów dostępu lub Pomiń) zostanie wykonana na pliku `abc.zip`, ale nie na pliku `123.doc`. W przypadku wybrania operacji: **Zmień nazwę**: program OfficeScan zmienia nazwę pliku `abc.zip` na `abc.vir`, ale nie zmienia nazwy pliku `123.doc`. **Poddaj kwarantannie**: program OfficeScan poddaje plik `abc.zip` kwarantannie (w tym plik `123.doc` i wszystkie niezarażone pliki). **Zezwól**: program OfficeScan nie wykonuje żadnej operacji na plikach `abc.zip` i `123.doc`, ale wykrycie wirusa zostaje zapisane w dzienniku. **Odmowa dostępu**: program OfficeScan blokuje dostęp podczas otwierania pliku `abc.zip` (nie można otworzyć pliku `123.doc` ani innych, niezarażonych plików).

Włącz tryb oceny

W trybie oceny wszyscy agenci zarządzani przez serwer rejestrują w dzienniku informacje o oprogramowaniu spyware/grayware wykrytym podczas skanowania ręcznego, skanowania w czasie rzeczywistym, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz, ale nie czyszczą tych składników. Czyszczenie kończy procesy lub usuwa rejestry, pliki, pliki cookie oraz skróty.

Firma Trend Micro stworzyła tryb oceny, aby użytkownik mógł najpierw ocenić elementy wykryte przez oprogramowanie Trend Micro jako oprogramowanie spyware/grayware, a następnie podjąć działanie na podstawie dokonanej oceny. Na przykład wykryte oprogramowanie spyware/grayware, którego użytkownik nie uważa za zagrożenie bezpieczeństwa, można dodać do listy dozwolonych spyware/grayware.

W trybie oceny program OfficeScan przeprowadza następujące operacje skanowania:

- **Zezwól**: w przypadku skanowania ręcznego, skanowania zaplanowanego i funkcji Skanuj teraz
- **Odmowa dostępu**: w przypadku skanowania w czasie rzeczywistym

Uwaga

Tryb oceny zastępuje wszystkie zdefiniowane przez użytkownika operacje skanowania. Na przykład, nawet jeśli użytkownik wybierze operację „Wyczyść” jako operację skanowania podczas Skanowania ręcznego, w trybie oceny jako operacja skanowania agenta jest stosowana operacja „Pomiń”.

Skanuj w poszukiwaniu plików typu cookie

Tę opcję należy wybrać, jeśli pliki cookie mają być traktowane jako potencjalne zagrożenia bezpieczeństwa. Gdy ta opcja jest wybrana, wszyscy agenci zarządzani przez serwer skanują pliki typu cookie pod względem oprogramowania spyware/grayware (dotyczy skanowania ręcznego, skanowania w czasie rzeczywistym, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz).

Sekcja ustawień skanowania zaplanowanego

Z poniższych ustawień korzystają tylko agenci skonfigurowani do uruchamiania skanowania zaplanowanego. Skanowanie zaplanowane dotyczy skanowania pod

względem wirusów i złośliwego oprogramowania oraz pod względem oprogramowania spyware/grayware.

Sekcja Ustawienia skanowania zaplanowanego globalnych ustawień skanowania umożliwia administratorom skonfigurowanie następujących elementów:

- *Przypominaj użytkownikom o skanowaniu zaplanowanym __ min przed rozpoczęciem skanowania na stronie 7-88*
- *Odłóż skanowanie zaplanowane na __ godz. i __ min na stronie 7-88*
- *Automatycznie zatrzymaj skanowanie zaplanowane, jeżeli trwa dłużej niż __ godz. i __ min. na stronie 7-89*
- *Pominięcie skanowania zaplanowanego, jeżeli poziom naładowania baterii bezprzewodowego punktu końcowego będzie niższy niż __ % i punkt końcowy nie będzie podłączony do źródła zasilania na stronie 7-89*
- *Wznów niewykonane Skanowanie zaplanowane na stronie 7-89*

Przypominaj użytkownikom o skanowaniu zaplanowanym __ min przed rozpoczęciem skanowania

Program OfficeScan może wyświetlać powiadomienie kilka minut przed rozpoczęciem skanowania, aby przypomnieć użytkownikom o harmonogramie skanowania (data i godzina) oraz o jakimkolwiek przyznanym im uprawnieniom do przeprowadzenia skanowania zaplanowanego.

Powiadomienie programu można włączyć/wyłączyć w obszarze **Agenci > Zarządzanie agentami > Ustawienia > Uprawnienia i inne ustawienia > Inne ustawienia (karta) > Ustawienia skanowania zaplanowanego**. Po wyłączeniu funkcji nie będą wyświetlane żadne powiadomienia.

Odłóż skanowanie zaplanowane na __ godz. i __ min

Tylko użytkownicy z uprawnieniami do uruchomienia funkcji „ Odłóż skanowanie zaplanowane” mogą wykonać następujące działania:

- Odłóż skanowanie zaplanowane zanim się rozpocznie, a następnie określ czas, na jaki skanowanie ma zostać odłożone.

- Jeśli skanowanie zaplanowane jest uruchomione, można je zatrzymać i ponownie uruchomić w późniejszym czasie. Użytkownicy mogą następnie określić czas, który minie przed ponownym uruchomieniem skanowania. Gdy skanowanie zostanie ponownie uruchomione, wszystkie przeskanowane wcześniej pliki zostaną przeskanowane powtórnie.

  Maksymalny czas odłożenia określony przez użytkownika wynosi 12 godzin i 45 minut. Można go skrócić poprzez określenie w odpowiednich polach liczby godzin i/lub minut.

Automatycznie zatrzymaj skanowanie zaplanowane, jeżeli trwa dłużej niż __ godz. i __ min.

Jeśli skanowanie nie zakończy się po ustalonym czasie, program OfficeScan zatrzymuje skanowanie. Następnie program OfficeScan powiadamia użytkowników o wszystkich zagrożeniach bezpieczeństwa wykrytych podczas skanowania.

Pominięcie skanowania zaplanowanego, jeżeli poziom naładowania baterii bezprzewodowego punktu końcowego będzie niższy niż __ % i punkt końcowy nie będzie podłączony do źródła zasilania

Jeśli program OfficeScan wykryje, że bateria bezprzewodowego punktu końcowego się rozładowuje i nie jest on podłączony do źródła zasilania, skanowanie jest pomijane natychmiast po uruchomieniu skanowania zaplanowanego. Skanowanie nie jest pomijane, jeśli poziom naładowania baterii jest niski, ale komputer jest podłączony do źródła zasilania.

Wznów niewykonane Skanowanie zaplanowane

Jeśli skanowanie zaplanowane nie zostało rozpoczęte w związku z tym, że program OfficeScan nie był uruchomiony w dniu i o godzinie skanowania zaplanowanego, albo jeśli użytkownik przerwał skanowanie zaplanowane (np. wyłączył punkt końcowy po rozpoczęciu skanowania), można określić, kiedy program OfficeScan wznowi skanowanie:

Określ, które skanowanie zaplanowane należy uruchomić ponownie:

- **Wznów przerwane skanowanie zaplanowane**: wznawia skanowanie zaplanowane przerwane przez użytkownika przez wyłączenie punktu końcowego
- **Wznów pominięte skanowanie zaplanowane**: wznawia skanowanie zaplanowane, które zostało pominięte, ponieważ punkt końcowy nie był włączony

Określ, kiedy należy wznowić skanowanie:

- **O tej samej godzinie następnego dnia**: jeśli program OfficeScan będzie uruchomiony o tej samej godzinie następnego dnia, skanowanie zostanie wznowione.
- **Po __ minutach od uruchomienia punktu końcowego**: program OfficeScan wznawia skanowanie po określonej liczbie minut od włączenia punktu końcowego przez użytkownika. Liczba minut mieści się w zakresie od 10 do 120.

Uwaga

Użytkownicy mogą odłożyć lub pominąć wznowione Skanowanie zaplanowane, jeśli administrator włączył to uprawnienie. Szczegółowe informacje zawiera sekcja *Uprawnienia do skanowania zaplanowanego i inne ustawienia na stronie 7-65*.

Powiadomienia o zagrożeniu bezpieczeństwa

Program OfficeScan zawiera zestaw domyślnych powiadomień programu informujących administratorów programu OfficeScan i użytkowników agenta OfficeScan o wykrytych zagrożeniach bezpieczeństwa.

Szczegółowe informacje o powiadomieniach wysyłanych do administratorów zawiera temat *Powiadamianie administratorów o zagrożeniach bezpieczeństwa na stronie 7-91*.

Szczegółowe informacje o powiadomieniach wysyłanych do użytkowników agentów zawiera sekcja *Powiadamianie użytkowników agenta OfficeScan o zagrożeniach bezpieczeństwa na stronie 7-97*.

Powiadamianie administratorów o zagrożeniach bezpieczeństwa

Można skonfigurować program OfficeScan, aby wysyłał powiadomienie do administratorów OfficeScan, kiedy wykryje zagrożenie bezpieczeństwa lub tylko wtedy, gdy operacja wymierzona w zagrożenie nie przyniesie efektu i będzie wymagała interwencji administratora.

Program OfficeScan zawiera domyślne powiadomienia informujące administratorów OfficeScan o wykryciu zagrożeń bezpieczeństwa. Można zmodyfikować powiadomienia i skonfigurować dodatkowe ustawienia powiadamiania zgodnie z potrzebami.

TABELA 7-20. Typy powiadomień o zagrożeniach bezpieczeństwa

TYP	REFERENCJE
Wirusy/złośliwe oprogramowanie	*Konfigurowanie powiadomień o zagrożeniach bezpieczeństwa dla administratorów na stronie 7-92*
Program szpiegujący/ grayware	*Konfigurowanie powiadomień o zagrożeniach bezpieczeństwa dla administratorów na stronie 7-92*
Transmisje zasobów cyfrowych	*Konfiguracja powiadamiania dotyczącego Zapobieganie utracie danych dla administratorów na stronie 11-57*
Wywołania zwrotne C&C	*Konfigurowanie powiadomień o wywołaniach zwrotnych C&C dla administratorów na stronie 12-16*

Uwaga

Program OfficeScan może wysyłać powiadomienia za pomocą poczty elektronicznej, pułapki SNMP i dzienników zdarzeń systemu Windows NT. Ustawienia należy skonfigurować, jeśli program OfficeScan wysyła powiadomienia za pomocą tych kanałów. Szczegółowe informacje zawiera sekcja *Ustawienia powiadamiania administratorów na stronie 14-37*.

Konfigurowanie powiadomień o zagrożeniach bezpieczeństwa dla administratorów

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Administrator**.
2. Na karcie **Kryteria**:
   a. Przejdź do sekcji **Wirusy/złośliwe oprogramowanie** lub **Spyware/ Grayware**.
   b. Określ, czy powiadomienia mają być wysyłane po wykryciu przez program OfficeScan wirusa/złośliwego oprogramowania i oprogramowania spyware/ grayware, czy tylko, gdy nie powiedzie się wykonanie operacji związanej z tymi zagrożeniami.
3. Na karcie **E-mail**:
   a. Przejdź do sekcji **Przypadki wykrycia wirusa/złośliwego oprogramowania** lub **Przypadki wykrycia oprogramowania spyware/ grayware**.
   b. Wybierz opcję **Włącz powiadamianie za pomocą wiadomości e-mail**.
   c. Wybierz opcję **Wyślij powiadomienia do użytkowników z uprawnieniami do domeny drzewa agentów**.

      Administrowanie oparte na rolach umożliwia przyznanie użytkownikom uprawnień do domeny drzewa agentów. Jeżeli nastąpi wykrycie na dowolnym agencie OfficeScan należącym do określonej domeny, na adresy e-mail użytkowników z uprawnieniami do domeny zostaną wysłane wiadomości. Przykłady znajdują się w poniższej tabeli:

TABELA 7-21. Domeny i uprawnienia w drzewie agentów

DOMENA DRZEWA AGENTÓW	ROLE Z UPRAWNIENIAMI DO DOMENY	KONTO UŻYTKOWNIKA Z ROLĄ	ADRES E-MAIL DLA KONTA UŻYTKOWNIKA
Domena A	Administrator (wbudowany)	konto główne	mary@xyz.com
	Rola_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domena B	Administrator (wbudowany)	konto główne	mary@xyz.com
	Rola_02	admin_jane	jane@xyz.com

Jeśli Agent OfficeScan należący do Domeny A wykryje wirusa, wiadomość e-mail zostanie wysłana na adresy mary@xyz.com, john@xyz.com i chris@xyz.com.

Jeśli oprogramowanie spyware zostanie wykryte przez agenta OfficeScan należącego do Domeny B, wiadomość e-mail zostanie wysłana na adresy mary@xyz.com i jane@xyz.com.

Uwaga

Jeżeli ta opcja jest włączona, wszyscy użytkownicy z uprawnieniami do domeny muszą mieć odpowiedni adres e-mail. Powiadomienie e-mail nie zostanie wysłane do użytkowników bez adresu e-mail. Użytkowników i adresy e-mail można skonfigurować na ekranie **Administracja** > **Zarządzanie kontami** > **Konta użytkowników**.

d. Wybierz opcję **Wysyłaj powiadomienia na następujące adresy e-mail** i wpisz adresy e-mail.

e. Zaakceptuj lub zmień domyślny temat i wiadomość. Dane w polach **Temat** i **Wiadomość** można przedstawiać za pomocą znaczników.

TABELA 7-22. Zmienne znaczników dla powiadomień o zagrożeniach bezpieczeństwa

ZMIENNA	OPIS
Przypadki wykrycia wirusa/złośliwego oprogramowania	
%v	Nazwa wirusa/złośliwego oprogramowania
%s	Punkt końcowy z wirusem/złośliwym oprogramowaniem
%i	Adres IP punktu końcowego
%c	Adres MAC punktu końcowego
%m	Domena punktu końcowego
%p	Lokalizacja wirusa/złośliwego oprogramowania
%y	Data i godzina wykrycia wirusa/złośliwego oprogramowania
%e	Wersja silnika skanowania antywirusowego
%r	Wersja sygnatur wirusów
%a	Działanie podjęte w związku z zagrożeniem bezpieczeństwa
%n	Nazwa użytkownika zalogowanego na zarażonym punkcie końcowym
Przypadki wykrycia oprogramowania spyware/grayware	
%s	Punkt końcowy z oprogramowaniem spyware/grayware
%i	Adres IP punktu końcowego
%m	Domena punktu końcowego
%y	Data i godzina wykrycia spyware/grayware
%n	Nazwa użytkownika zalogowanego na punkcie końcowym w momencie wykrycia
%T	Spyware/grayware i wynik skanowania

4. Na karcie **Pułapka SNMP**:

a. Przejdź do sekcji **Przypadki wykrycia wirusa/złośliwego oprogramowania** lub **Przypadki wykrycia oprogramowania spyware/grayware**.

b. Wybierz opcję **Włącz powiadamianie przez pułapkę SNMP**.

c. Zaakceptuj lub zmień domyślną wiadomość. Dane w polu **Wiadomość** można przedstawiać za pomocą zmiennych znaczników podanych w poniższej tabeli.

TABELA 7-23. Zmienne znaczników dla powiadomień o zagrożeniach bezpieczeństwa

ZMIENNA	OPIS
Przypadki wykrycia wirusa/złośliwego oprogramowania	
%v	Nazwa wirusa/złośliwego oprogramowania
%s	Punkt końcowy z wirusem/złośliwym oprogramowaniem
%i	Adres IP punktu końcowego
%c	Adres MAC punktu końcowego
%m	Domena punktu końcowego
%p	Lokalizacja wirusa/złośliwego oprogramowania
%y	Data i godzina wykrycia wirusa/złośliwego oprogramowania
%e	Wersja silnika skanowania antywirusowego
%r	Wersja sygnatur wirusów
%a	Działanie podjęte w związku z zagrożeniem bezpieczeństwa
%n	Nazwa użytkownika zalogowanego na zarażonym punkcie końcowym
Przypadki wykrycia oprogramowania spyware/grayware	
%s	Punkt końcowy z oprogramowaniem spyware/grayware
%i	Adres IP punktu końcowego

ZMIENNA	OPIS
%m	Domena punktu końcowego
%y	Data i godzina wykrycia spyware/grayware
%n	Nazwa użytkownika zalogowanego na punkcie końcowym w momencie wykrycia
%T	Spyware/grayware i wynik skanowania
%v	Nazwa spyware/grayware
%a	Działanie podjęte w związku z zagrożeniem bezpieczeństwa

5. Na karcie **Dziennik zdarzeń systemu Windows NT**:

   a. Przejdź do sekcji **Przypadki wykrycia wirusa/złośliwego oprogramowania** lub **Przypadki wykrycia oprogramowania spyware/grayware**.

   b. Wybierz opcję **Włącz powiadamianie przez rejestr zdarzeń NT**.

   c. Zaakceptuj lub zmień domyślną wiadomość. Dane w polu **Wiadomość** można przedstawiać za pomocą zmiennych znaczników podanych w poniższej tabeli.

TABELA 7-24. Zmienne znaczników dla powiadomień o zagrożeniach bezpieczeństwa

ZMIENNA	OPIS
Przypadki wykrycia wirusa/złośliwego oprogramowania	
%v	Nazwa wirusa/złośliwego oprogramowania
%s	Punkt końcowy z wirusem/złośliwym oprogramowaniem
%i	Adres IP punktu końcowego
%c	Adres MAC punktu końcowego
%m	Domena punktu końcowego
%p	Lokalizacja wirusa/złośliwego oprogramowania

ZMIENNA	OPIS
%y	Data i godzina wykrycia wirusa/złośliwego oprogramowania
%e	Wersja silnika skanowania antywirusowego
%r	Wersja sygnatur wirusów
%a	Działanie podjęte w związku z zagrożeniem bezpieczeństwa
%n	Nazwa użytkownika zalogowanego na zarażonym punkcie końcowym
Przypadki wykrycia oprogramowania spyware/grayware	
%s	Punkt końcowy z oprogramowaniem spyware/grayware
%i	Adres IP punktu końcowego
%m	Domena punktu końcowego
%y	Data i godzina wykrycia spyware/grayware
%n	Nazwa użytkownika zalogowanego na punkcie końcowym w momencie wykrycia
%T	Spyware/grayware i wynik skanowania
%v	Nazwa spyware/grayware
%a	Działanie podjęte w związku z zagrożeniem bezpieczeństwa

6. Kliknij przycisk **Zapisz**.

Powiadamianie użytkowników agenta OfficeScan o zagrożeniach bezpieczeństwa

Program OfficeScan może wyświetlać powiadomienia programu na punkcie końcowym agenta OfficeScan:

- Natychmiast, gdy skanowanie w czasie rzeczywistym i skanowanie zaplanowane wykryje wirusa/złośliwe oprogramowanie i oprogramowanie spyware/grayware.

Należy włączyć powiadomienia programu oraz w razie potrzeby zmodyfikować ich treść.

- Jeśli wymagane jest ponowne uruchomienie punktu końcowego agenta w celu zakończenia czyszczenia zarażonych plików. W przypadku skanowania w czasie rzeczywistym komunikat jest wyświetlany po przeskanowaniu określonego zagrożenia bezpieczeństwa. W przypadku skanowania ręcznego, skanowania zaplanowanego i skanowania za pomocą funkcji Skanuj teraz komunikat jest wyświetlany tylko raz, gdy program OfficeScan zakończy skanowanie wszystkich elementów docelowych.

TABELA 7-25. Typy powiadomień o zagrożeniach bezpieczeństwa agenta

TYP	REFERENCJE
Wirusy/złośliwe oprogramowanie	*Konfigurowanie powiadomień o wirusach/złośliwym oprogramowaniu na stronie 7-100*
Program szpiegujący/ grayware	*Konfigurowanie powiadomień o oprogramowaniu spyware/ grayware na stronie 7-100*
Naruszenia zapory	*Modyfikowanie treści powiadomienia programu od zapory na stronie 13-30*
Naruszenia usługi Web Reputation	*Modyfikowanie powiadomień o zagrożeniach internetowych na stronie 12-15*
Naruszenia kontroli urządzeń	*Modyfikowanie powiadomień kontroli urządzeń na stronie 10-19*
Naruszenia reguł monitorowania zachowań	*Zmiana treści powiadomień programu na stronie 9-18*
Transmisje zasobów cyfrowych	*Konfiguracja powiadamiania dotyczącego Zapobieganie utracie danych dla agentów na stronie 11-60*
Wywołania zwrotne C&C	*Modyfikowanie powiadomień o zagrożeniach internetowych na stronie 12-15*

Powiadamianie użytkowników o wykrytych wirusach/złośliwym oprogramowaniu oraz wystąpieniach oprogramowania spyware/grayware

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Ustawienia skanowania** > **Ustawienia skanowania w czasie rzeczywistym** lub **Ustawienia** > **Ustawienia skanowania** > **Ustawienia skanowania zaplanowanego**.
4. Kliknij kartę **Operacja**.
5. Wybierz następujące opcje:
   - **Wyświetl powiadomienie programu na punkcie końcowym agenta po wykryciu wirusa/złośliwego oprogramowania**
   - **Wyświetl powiadomienie programu na punkcie końcowym agenta po wykryciu potencjalnego wirusa/złośliwego oprogramowania**
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Konfigurowanie powiadomień o wirusach/złośliwym oprogramowaniu

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Agent**.
2. Na liście rozwijanej **Typ** wybierz opcję **Wirus/złośliwe oprogramowanie**.
3. Skonfiguruj ustawienia wykrywania.
   a. Wybierz wyświetlanie jednego powiadomienia dla wszystkich zdarzeń związanych z wirusami/złośliwym oprogramowaniem lub oddzielnych powiadomień dotyczących następujących poziomów ważności:
      - **Wysoki**: Agent OfficeScan nie poradził sobie z bardzo groźnym złośliwym oprogramowaniem.
      - **Średni**: Agent OfficeScan nie poradził sobie ze złośliwym oprogramowaniem.
      - **Niski**: Agent OfficeScan wyeliminował wszystkie zagrożenia.

   b. Zaakceptuj lub zmień domyślne wiadomości.
4. Kliknij przycisk **Zapisz**.

Konfigurowanie powiadomień o oprogramowaniu spyware/grayware

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Agent**.
2. Na liście rozwijanej **Typ** wybierz opcję **Spyware/Grayware**.
3. Zaakceptuj lub zmień domyślną wiadomość.
4. Kliknij przycisk **Zapisz**.

Powiadamianie agentów o ponownym uruchomieniu w celu zakończenia czyszczenia zarażonych plików

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Kliknij kartę **Inne ustawienia** i przejdź do sekcji **Powiadomienie o ponownym uruchomieniu**.
5. Wybierz opcję **Wyświetl powiadomienie, jeżeli konieczne jest ponowne uruchomienie punktu końcowego, aby możliwe było zakończenie czyszczenia zainfekowanych plików**.
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Dzienniki zagrożeń bezpieczeństwa

Program OfficeScan tworzy dzienniki tego typu po wykryciu wirusa / złośliwego oprogramowania lub oprogramowania spyware/grayware oraz gdy przywraca oprogramowanie spyware/grayware.

Aby dzienniki nie zajmowały zbyt dużo miejsca na dysku twardym, można je ręcznie usunąć lub skonfigurować harmonogram ich usuwania. Dodatkowe informacje dotyczące dzienników zarządzania zawiera sekcja *Zarządzanie dziennikiem na stronie 14-41*.

Wyświetlanie dzienników wirusów/złośliwego oprogramowania

Agent OfficeScan tworzy dzienniki tego typu po wykryciu wirusów lub złośliwego oprogramowania i wysyła je na serwer.

Procedura

1. Przejdź do jednej z następujących opcji:
   - **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa**
   - **Agenci** > **Zarządzanie agentami**
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Dzienniki** > **Dzienniki wirusów/złośliwego oprogramowania** lub **Wyświetl dzienniki** > **Dzienniki wirusów/złośliwego oprogramowania**.
4. Określ kryteria dziennika i kliknij przycisk **Wyświetl dzienniki**.
5. Wyświetl dzienniki. Dziennik zawiera następujące informacje:
   - Data i godzina wykrycia wirusa/złośliwego oprogramowania
   - Punkt końcowy
   - Zagrożenie bezpieczeństwa
   - Źródło zarażenia
   - Zarażony plik lub obiekt
   - Ścieżka pliku

- Kanał zarażenia
- Typ skanowania, podczas którego wykryto wirusa lub złośliwe oprogramowanie
- Wyniki skanowania

Uwaga

Więcej informacji o wynikach skanowania zawiera sekcja *Wyniki skanowania w poszukiwaniu wirusów/złośliwego oprogramowania na stronie 7-103*.

- Adres IP
- Adres MAC
- Szczegółowe dane dziennika (kliknij **Wyświetl**, aby zobaczyć szczegóły)

6. Aby zapisać dzienniki w formacie CSV (plik z tekstem oddzielanym przecinkami), kliknij opcję **Eksportuj do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

   Plik CSV zawiera następujące informacje:

   - Wszystkie informacje w dziennikach
   - Nazwa użytkownika zalogowanego na punkcie końcowym w momencie wykrycia

Wyniki skanowania w poszukiwaniu wirusów/złośliwego oprogramowania

Następujące wyniki skanowania są wyświetlane w dziennikach wirusów/złośliwego oprogramowania:

TABELA 7-26. Wyniki skanowania

WYNIK	OPIS
Usunięto	• Pierwsza operacja to “Usuń”; zarażony plik został usunięty.

Wynik	Opis
	• Pierwsza operacja to “Wyczyść”; operacja została zakończona niepowodzeniem. Druga operacja to “Usuń”; zarażony plik został usunięty.
Kwarantanna	• Pierwsza operacja to “Poddaj kwarantannie”; zarażony plik został poddany kwarantannie. • Pierwsza operacja to “Wyczyść”; operacja została zakończona niepowodzeniem. Druga operacja to “Poddaj kwarantannie”; zarażony plik został poddany kwarantannie.
Wyczyszczono	Zarażony plik został wyczyszczony.
Zmieniono nazwę	• Pierwsza operacja to “Zmień nazwę”; nazwa zarażonego pliku została zmieniona. • Pierwsza operacja to “Wyczyść”; operacja została zakończona niepowodzeniem. Druga operacja to “Zmień nazwę”; nazwa zarażonego pliku została zmieniona.
Odmowa dostępu	• Pierwsza operacja to “Odmów dostępu”; dostęp do zarażonego pliku został zabroniony, gdy użytkownik chciał otworzyć plik. • Pierwsza operacja to “Wyczyść”; operacja została zakończona niepowodzeniem. Druga operacja to “Odmów dostępu”; dostęp do pliku został zabroniony, gdy użytkownik chciał otworzyć plik. • Podczas skanowania w czasie rzeczywistym wykryto potencjalnego wirusa/złośliwe oprogramowanie. • Funkcja skanowania w czasie rzeczywistym może zablokować dostęp do plików zarażonych wirusem sektora rozruchowego, nawet jeśli operacja skanowania to “Wyczyść” (pierwsza operacja) i “Poddaj kwarantannie” (druga operacja). Wynika to z faktu, że próba wyczyszczenia wirusa sektora rozruchowego może spowodować uszkodzenie głównego rekordu rozruchowego (MBR, Master Boot Record) zarażonego punktu końcowego. Uruchom skanowanie ręczne, aby umożliwić programowi OfficeScan wyczyszczenie pliku lub poddanie go kwarantannie.
Pominięto	• Pierwsza operacja to “Zezwól”, więc program OfficeScan nie wykonał żadnej operacji na zarażonym pliku.

Wynik	Opis
	• Pierwsza operacja to “Wyczyść”; operacja została zakończona niepowodzeniem. Druga operacja to “Pomiń”, więc program OfficeScan nie wykonał żadnej operacji na zarażonym pliku.
Pominięto potencjalne ryzyko zabezpieczeń	Wyniki skanowania są wyświetlane tylko wtedy, gdy program OfficeScan wykryje „prawdopodobny wirus/złośliwe oprogramowanie” podczas skanowania ręcznego, skanowania zaplanowanego i używania funkcji Skanuj teraz. Informacje o potencjalnych wirusach/złośliwym oprogramowaniu oraz o sposobie przesyłania podejrzanych plików do firmy Trend Micro w celu analizy znajdują się w Encyklopedii wirusów firmy Trend Micro pod adresem: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=POSSIBLE_VIRUS&VSect=Sn
Nie można wyczyścić pliku lub poddać go kwarantannie	Pierwsza operacja to “Wyczyść”. Druga operacja to “Poddaj kwarantannie”; obie operacje zostały zakończone niepowodzeniem. Rozwiązanie: Patrz sekcja *Nie można poddać kwarantannie/ zmienić nazwy pliku na stronie 7-105*.
Nie można wyczyścić lub usunąć pliku	Pierwsza operacja to “Wyczyść”. Druga operacja to “Usuń”; obie operacje zostały zakończone niepowodzeniem. Rozwiązanie: Patrz sekcja *Nie można usunąć pliku na stronie 7-106*.
Nie można wyczyścić pliku lub zmienić jego nazwy	Pierwsza operacja to “Wyczyść”. Druga operacja to “Zmień nazwę”; obie operacje zostały zakończone niepowodzeniem. Rozwiązanie: Patrz sekcja *Nie można poddać kwarantannie/ zmienić nazwy pliku na stronie 7-105*.
Nie można poddać kwarantannie/ zmienić nazwy pliku	Wyjaśnienie 1 Zarażony plik może być zablokowany przez inną aplikację, jest obecnie wykonywany lub znajduje się na dysku CD. Program OfficeScan podda plik kwarantannie/zmieni jego nazwę po zwolnieniu pliku przez aplikację lub po jego wykonaniu. Rozwiązanie

Wynik	Opis
	Jeśli zarażone pliki znajdują się na dysku CD, należy zaprzestać używania tego dysku CD, ponieważ znajdujący się na nim wirus może zarazić inne punkty końcowe w sieci.
	Wyjaśnienie 2 Zarażony plik znajduje się w folderze tymczasowych plików internetowych na punkcie końcowym agenta. Ponieważ podczas przeglądania sieci Web punkt końcowy pobiera pliki, przeglądarka internetowa może blokować zarażony plik. Po zwolnieniu pliku przez przeglądarkę internetową zostanie on podany kwarantannie lub jego nazwa zostanie zmieniona w programie OfficeScan. Rozwiązanie: Brak
Nie można usunąć pliku	Wyjaśnienie 1 Zarażony plik może być zawarty w pliku skompresowanym, a ustawienie **Wyczyść/usuń zarażone pliki w plikach skompresowanych** dostępne na ekranie **Agenci** > **Ustawienia agenta globalnego** na karcie **Ustawienia zabezpieczeń** jest wyłączone. Rozwiązanie Włącz opcję **Wyczyść/usuń zarażone pliki w plikach skompresowanych**. Po włączeniu tej funkcji program OfficeScan dekompresuje skompresowane pliki, czyści/usuwa zapisane w nich zarażone pliki i kompresuje je ponownie. **Uwaga** Włączenie tego ustawienia może spowodować wzrost zużycia zasobów punktu końcowego podczas skanowania oraz wydłużyć czas skanowania.
	Wyjaśnienie 2 Zarażony plik może być zablokowany przez inną aplikację, jest obecnie wykonywany lub znajduje się na dysku CD. Program OfficeScan usunie plik po jego zwolnieniu przez aplikację lub po jego wykonaniu. Rozwiązanie

WYNIK	OPIS
	Jeśli zarażone pliki znajdują się na dysku CD, należy zaprzestać używania tego dysku CD, ponieważ znajdujący się na nim wirus może zarazić inne punkty końcowe w sieci.
	Wyjaśnienie 3 Zarażony plik znajduje się w folderze tymczasowych plików internetowych na punkcie końcowym Agent OfficeScan. Ponieważ podczas przeglądania sieci Web punkt końcowy pobiera pliki, przeglądarka internetowa może blokować zarażony plik. Po zwolnieniu pliku przez przeglądarkę internetową program OfficeScan usunie ten plik. Rozwiązanie: Brak
Nie można przesłać pliku poddanego kwarantannie do wyznaczonego folderu kwarantanny	Mimo że program OfficeScan poddał z powodzeniem kwarantannie plik w folderze `\Suspect` na punkcie końcowym agenta Agent OfficeScan, przesłanie pliku do wyznaczonego katalogu kwarantanny jest niemożliwe. Rozwiązanie Określ, który rodzaj skanowania (Skanowanie ręczne, Skanowanie w czasie rzeczywistym, Skanowanie planowane lub Skanuj teraz) wykrył wirus/złośliwe oprogramowanie, a następnie sprawdź katalog kwarantanny określony na karcie **Agenci** > **Zarządzanie agentami > Ustawienia** > **{Typ skanowania}** > **Operacja**. Jeśli katalog kwarantanny znajduje się na komputerze serwera OfficeScan lub na innym komputerze serwera OfficeScan: 1. Sprawdź, czy agent może połączyć się z serwerem. 2. Jeżeli jako format katalogu kwarantanny wykorzystywany jest adres URL: a. Upewnij się, że nazwa punktu końcowego podana po prefiksie `http://` jest prawidłowa. b. Sprawdź rozmiar zainfekowanego pliku. Jeżeli przekracza on maksymalny rozmiar pliku określony w obszarze **Administracja** > **Ustawienia** > **Menedżer kwarantanny**, dostosuj ustawienie, aby plik się zmieścił. Można również wykonać inne operacje, na przykład usunąć plik.

Wynik	Opis
	c. Sprawdź rozmiar katalogu kwarantanny i określ, czy nie została przekroczona pojemność katalogu określona w obszarze **Administracja** > **Ustawienia** > **Menedżer kwarantanny**. Zmień pojemność folderu lub ręcznie usuń pliki z katalogu kwarantanny. 3. Jeżeli jest używana ścieżka UNC, należy upewnić się, że katalog kwarantanny został przydzielony do grupy “Wszyscy” oraz że przypisano tej grupie uprawnienie do odczytu i do zapisu. Sprawdź także, czy istnieje katalog kwarantanny i czy ścieżka UNC jest prawidłowa. Jeśli katalog kwarantanny znajduje się na innym punkcie końcowym w sieci (w tym scenariuszu można korzystać tylko ze ścieżki UNC): 1. Sprawdź, czy Agent OfficeScan może połączyć się z punktem końcowym. 2. Upewnij się, że katalog kwarantanny jest przydzielony do grupy“Wszyscy” i że przypisano tej grupie uprawnienie do odczytu i do zapisu. 3. Sprawdź, czy katalog kwarantanny istnieje. 4. Sprawdź, czy ścieżka UNC jest prawidłowa. Jeśli katalog kwarantanny znajduje się w innym katalogu na punkcie końcowym Agent OfficeScan (w tym scenariuszu można używać tylko ścieżek bezwzględnych), sprawdź, czy ten katalog istnieje.
Nie można wyczyścić pliku	Wyjaśnienie 1 Zarażony plik może być zawarty w pliku skompresowanym, a ustawienie “Wyczyść/usuń” zarażone pliki w plikach skompresowanych dostępne na ekranie **Agenci** > **Ustawienia agenta globalnego** na karcie **Ustawienia zabezpieczeń** jest wyłączone. Rozwiązanie Włącz opcję **Wyczyść/usuń zarażone pliki w plikach skompresowanych**. Po włączeniu tej funkcji program OfficeScan dekompresuje skompresowane pliki, czyści/usuwa zapisane w nich zarażone pliki i kompresuje je ponownie.

WYNIK	OPIS
	Uwaga Włączenie tego ustawienia może spowodować wzrost zużycia zasobów punktu końcowego podczas skanowania oraz wydłużyć czas skanowania.
	Wyjaśnienie 2 Zarażony plik znajduje się w folderze `Tymczasowe pliki internetowe` na punkcie końcowym Agent OfficeScan. Ponieważ podczas przeglądania sieci Web punkt końcowy pobiera pliki, przeglądarka internetowa może blokować zarażony plik. Kiedy przeglądarka internetowa zwolni plik, program OfficeScan wyczyści ten plik. Rozwiązanie: Brak
	Wyjaśnienie 3 Wyczyszczenie pliku jest prawdopodobnie niemożliwe. Szczegółowe informacje zawiera sekcja *Pliki, których nie można wyczyścić na stronie E-17*.
Wymagane działanie	Program OfficeScan nie może wykonać skonfigurowanej operacji na zarażonym pliku bez interwencji użytkownika. Przesuń wskaźnik myszy na kolumnę **Wymagane działanie**, aby wyświetlić następujące szczegóły. • "Wymagane działanie — skontaktuj się z pomocą techniczną, aby uzyskać informacje dotyczące sposobu usuwania tego zagrożenia za pomocą narzędzia „Czysty rozruch" w dodatku Anti-Threat Tool Kit w programie OfficeScan ToolBox." • "Wymagane działanie — skontaktuj się z pomocą techniczną, aby uzyskać informacje dotyczące sposobu usuwania tego zagrożenia za pomocą narzędzia „Dysk ratunkowy" w dodatku Anti-Threat Tool Kit w programie OfficeScan ToolBox." • "Wymagane działanie — skontaktuj się z pomocą techniczną, aby uzyskać informacje dotyczące sposobu usuwania tego zagrożenia za pomocą narzędzia „Rootkit Buster" w dodatku Anti-Threat Tool Kit w programie OfficeScan ToolBox."

WYNIK	OPIS
	• "Wymagane działanie — program OfficeScan wykrył zagrożenie na zarażonym agencie. Uruchom ponownie punkt końcowy, aby zakończyć czyszczenie zagrożenia" • "Wymagane działanie — do usunięcia wykrytego zagrożenia oprogramowaniem typu rootkit z punktu końcowego wymagane jest pełne skanowanie systemu."

Wyświetlanie dzienników centralnego przywracania kwarantanny

Po wyczyszczeniu złośliwego oprogramowania agenci Agenci OfficeScan tworzą kopie zapasowe jego danych. Jeśli usunięte dane są uważane za nieszkodliwe, można powiadomić agenta online o chęci ich przywrócenia. W dziennikach są zapisywane informacje o danych kopii zapasowej złośliwego oprogramowania, zarażonym punkcie końcowym oraz o wynikach operacji przywracania.

Procedura

1. Przejdź do opcji **Dzienniki** > **Agenci** > **Centralne przywracanie kwarantanny**.
2. Sprawdź w kolumnach **Powodzenie**, **Niepowodzenie** i **Oczekujące**, czy program OfficeScan pomyślnie przywrócił dane poddane kwarantannie.
3. Kliknij łącza z numerem w poszczególnych kolumnach, aby uzyskać szczegółowe informacje na temat każdego zarażonego punktu końcowego.

   Uwaga

   W przypadku przywróceń o stanie **Niepowodzenie** można ponowić próbę przywrócenia pliku na ekranie **Szczegóły centralnego przywracania kwarantanny**, klikając polecenie **Przywróć wszystkie**.

4. Aby zapisać dzienniki w formacie CSV (plik z tekstem oddzielanym przecinkami), kliknij opcję **Eksportuj do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Wyświetlanie dzienników oprogramowania spyware/grayware

Agent OfficeScan tworzy dzienniki tego typu po wykryciu oprogramowania spyware lub grayware i wysyła je na serwer.

Procedura

1. Przejdź do jednej z następujących opcji:
   - **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa**
   - **Agenci** > **Zarządzanie agentami**
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Dzienniki** > **Dzienniki spyware/grayware** lub **Wyświetl dzienniki** > **Dzienniki spyware/grayware**.
4. Określ kryteria dziennika i kliknij przycisk **Wyświetl dzienniki**.
5. Wyświetl dzienniki. Dziennik zawiera następujące informacje:
   - Data i godzina wykrycia spyware/grayware
   - Zarażony punkt końcowy
   - Nazwa spyware/grayware
   - Kanał zarażenia
   - Typ skanowania, podczas którego wykryto oprogramowanie spyware/grayware
   - Szczegółowe informacje o wynikach skanowania w poszukiwaniu oprogramowania spyware/grayware (niezależnie od tego, czy wykonanie operacji skanowania się powiodło czy nie).

     Szczegółowe informacje można znaleźć w części *Wynik skanowania w poszukiwaniu oprogramowania spyware/grayware na stronie 7-112*.

- Adres IP
- Adres MAC
- Szczegółowe dane dziennika (kliknij **Wyświetl**, aby zobaczyć szczegóły)

6. Oprogramowanie spyware/grayware, które uważasz za nieszkodliwe, można dodać do listy dozwolonych programów spyware/grayware.

7. Aby zapisać dzienniki w formacie CSV (plik z tekstem oddzielanym przecinkami), kliknij opcję **Eksportuj do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

   Plik CSV zawiera następujące informacje:

   - Wszystkie informacje w dziennikach
   - Nazwa użytkownika zalogowanego na punkcie końcowym w momencie wykrycia

---

Wynik skanowania w poszukiwaniu oprogramowania spyware/grayware

Następujące wyniki skanowania są wyświetlane w dziennikach spyware/grayware:

TABELA 7-27. Wyniki pierwszego poziomu skanowania w poszukiwaniu oprogramowania spyware/grayware

WYNIK	OPIS
Zakończone powodzeniem, nie jest wymagane żadne działanie	Jest to wynik pierwszego poziomu, jeśli operacja skanowania powiodła się. Możliwe wyniki skanowania drugiego poziomu: • *Wyczyszczono* • *Odmowa dostępu*

Wynik	Opis
Wymagana dalsza operacja	Jest to wynik pierwszego poziomu, jeśli operacja skanowania nie powiodła się. Wyniki drugiego poziomu zawierają co najmniej jeden z następujących komunikatów: • *Pominięto* • *Czyszczenie spyware/grayware wiąże się z zagrożeniem* • *Skanowanie spyware/grayware zostało zatrzymane ręcznie. Przeprowadź kompletne skanowanie* • *Wyczyszczono spyware/grayware, wymagane jest ponowne uruchomienie komputera. Uruchom ponownie komputer* • *Nie można wyczyścić oprogramowania spyware/grayware* • *Niezidentyfikowany wynik skanowania spyware/grayware. Należy skontaktować się z pomocą techniczną firmy Trend Micro*

Tabela 7-28. Wyniki drugiego poziomu skanowania w poszukiwaniu oprogramowania spyware/grayware

Wynik	Opis	Rozwiązanie
Wyczyszczono	Program OfficeScan zakończył działanie procesów lub usunął klucze rejestrów, pliki, pliki cookie oraz skróty.	nd.
Odmowa dostępu	Program OfficeScan zablokował dostęp (kopiowanie, otwieranie) do wykrytych składników spyware/grayware.	nd.
Pominięto	Program OfficeScan nie wykonał żadnej operacji, ale informacje na temat wykrycia oprogramowania spyware/grayware zostały zapisane do późniejszej oceny.	dodaj oprogramowanie spyware/grayware, które uważasz za nieszkodliwe, do listy dozwolonego oprogramowania spyware/grayware.

Wynik	Opis	Rozwiązanie
Czyszczenie spyware/grayware wiąże się z zagrożeniem	: Ten komunikat jest wyświetlany, jeśli silnik skanowania w poszukiwaniu oprogramowania spyware próbuje wyczyść dowolny folder i spełnione zostaną następujące kryteria: • Wielkość elementów do wyczyszczenia przekracza 250 MB. • System operacyjny korzysta z plików z tego folderu. Folder może być także niezbędny do normalnego działania systemu. • Folder jest katalogiem głównym (na przykład `C:` lub `F:`)	Aby uzyskać pomoc, skontaktuj się z przedstawicielem działu pomocy technicznej.
Skanowanie spyware/grayware zostało zatrzymane ręcznie. Przeprowadź kompletne skanowanie	Skanowanie zostało zatrzymane przez użytkownika przed zakończeniem procesu.	Uruchom skanowanie ręczne i poczekaj, aż proces zostanie ukończony.
Wyczyszczono spyware/grayware, wymagane jest ponowne uruchomienie komputera. Uruchom ponownie komputer	Składniki spyware/grayware zostały wyczyszczone pomyślnie przez program OfficeScan, lecz w celu zakończenia zadania wymagane jest ponowne uruchomienie punktu końcowego.	Niezwłocznie uruchom ponownie punkt końcowy.
Nie można wyczyścić oprogramowania spyware/grayware	Oprogramowanie spyware/grayware wykryto na dysku CD-ROM lub na dysku sieciowym. Program OfficeScan nie usuwa oprogramowania spyware/grayware wykrytego w tych lokalizacjach.	Usuń ręcznie zarażony plik.

Wynik	Opis	Rozwiązanie
Niezidentyfikowany wynik skanowania spyware/grayware. Należy skontaktować się z pomocą techniczną firmy Trend Micro	Nowa wersja silnika skanowania w poszukiwaniu oprogramowania spyware zapewnia nowy wynik skanowania, do obsługi którego program OfficeScan nie został skonfigurowany.	W celu określenia nowego wyniku skanowania skontaktuj się z działem pomocy technicznej.

Wyświetlanie dzienników przywracania po usunięciu oprogramowania spyware/grayware

Po usunięciu oprogramowania spyware/grayware Agenci OfficeScan tworzą jego kopie zapasowe. Jeśli usunięte dane są uważane za nieszkodliwe, można powiadomić agenta online o chęci ich przywrócenia. W dziennikach są zapisywane informacje o danych kopii zapasowej oprogramowania spyware/grayware, zarażonym punkcie końcowym oraz o wynikach operacji przywracania.

Procedura

1. Przejdź do opcji **Dzienniki** > **Agenci** > **Przywracanie spyware/grayware**.
2. Sprawdź w kolumnie **Wynik**, czy program OfficeScan pomyślnie przywrócił oprogramowanie spyware/grayware.
3. Aby zapisać dzienniki w formacie CSV (plik z tekstem oddzielanym przecinkami), kliknij opcję **Eksportuj do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Wyświetlanie dzienników podejrzanych plików

Agent OfficeScan tworzy dzienniki tego typu po wykryciu plików na liście podejrzanych plików i wysyła je na serwer.

Procedura

1. Przejdź do jednej z następujących opcji:
   - **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa**
   - **Agenci** > **Zarządzanie agentami**
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, albo wybierz określone domeny lub agentów.
3. Kliknij kolejno pozycje **Dzienniki** > **Dzienniki podejrzanych plików** lub **Wyświetl dzienniki** > **Dzienniki podejrzanych plików**.
4. Określ kryteria dziennika i kliknij przycisk **Wyświetl dzienniki**.
5. Wyświetl dzienniki. Dziennik zawiera następujące informacje:
   - Data i godzina wykrycia podejrzanego pliku
   - Punkt końcowy
   - Domena
   - Wartość hash SHA-1 pliku dla źródła zarażenia
   - Ścieżka pliku
   - Typ skanowania, podczas którego wykryto podejrzany plik
   - Wyniki skanowania

     Uwaga

     Więcej informacji o wynikach skanowania zawiera sekcja *Wyniki skanowania w poszukiwaniu wirusów/złośliwego oprogramowania na stronie 7-103*.
   - Adres IP

Wyświetlanie dzienników operacji skanowania:

Po uruchomieniu skanowania ręcznego, skanowania zaplanowanego lub funkcji Skanuj teraz Agent OfficeScan tworzy dziennik skanowania zawierający informacje

o skanowaniu. Aby przejrzeć dziennik skanowania, należy przejść do konsoli serwera agenta OfficeScan lub agenta OfficeScan.

Aby wyświetlić dzienniki operacji skanowania na serwerze OfficeScan, należy przejść do jednej z następujących lokalizacji:

- **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa** i kliknij polecenie **Wyświetl dzienniki** > **Dzienniki operacji skanowania**
- **Agenci** > **Zarządzanie agentami** i kliknij polecenie **Dzienniki** > **Dzienniki operacji skanowania**

Dzienniki operacji skanowania zawierają następujące informacje:

- Data i godzina rozpoczęcia skanowania przez program OfficeScan
- Data i godzina zakończenia skanowania przez program OfficeScan
- Stan skanowania
    - **Ukończono**: Skanowanie zakończyło się w zwykły sposób.
    - **Przerwano**: Użytkownik zatrzymał skanowanie zanim zostało ukończone.
    - **Nieoczekiwanie zatrzymano**: skanowanie zostało przerwane przez użytkownika, system lub nieoczekiwane zdarzenie. Na przykład działanie usługi skanowania w czasie rzeczywistym programu OfficeScan mogło zostać nieoczekiwanie przerwane lub użytkownik wymusił ponowne uruchomienie agenta.
- Typ skanowania
- Liczba skanowanych obiektów
- Liczba wykrytych wirusów/złośliwego oprogramowania
- Liczba przypadków wykrycia spyware/grayware
- Wersja sygnatura Agenta Smart Scan
- Wersja sygnatur wirusów
- Wersja sygnatury oprogramowania spyware/grayware

Epidemie zagrożeń bezpieczeństwa

Epidemia zagrożeń bezpieczeństwa występuje, gdy liczba przypadków wykrycia wirusów/złośliwego oprogramowania, oprogramowania spyware/grayware i sesji folderów udostępnionych w określonym przedziale czasu przekracza ustaloną wartość graniczną. Epidemię można zlikwidować i przechować we wnętrzu sieci na kilka sposobów:

- umożliwienie programowi OfficeScan monitorowania sieci w poszukiwaniu podejrzanej aktywności,
- zablokowanie krytycznych portów i folderów punktu końcowego agenta,
- wysłanie komunikatów ostrzegających o epidemii do agentów,
- wyczyszczenie zarażonych punktów końcowych.

Epidemia zagrożeń bezpieczeństwa — kryteria i powiadamianie

Program OfficeScan można skonfigurować w celu wysyłania do administratorów OfficeScan powiadomienia po wystąpieniu następujących zdarzeń:

TABELA 7-29. Typy powiadomień o epidemiach zagrożeń bezpieczeństwa

TYP	REFERENCJE
• Wirusy/złośliwe oprogramowanie • Program szpiegujący/ grayware • Sesja folderu udostępnionego	*Konfigurowanie kryteriów epidemii zagrożeń bezpieczeństwa oraz opcji powiadamiania na stronie 7-119*
Naruszenia zapory	*Konfiguracja kryteriów epidemii naruszeń zapory oraz opcji powiadamiania na stronie 13-32*

TYP	REFERENCJE
Wywołania zwrotne C&C	*Konfigurowanie kryteriów i powiadomień o epidemii wywołań zwrotnych C&C na stronie 12-21*

- Epidemia wirusów/złośliwego oprogramowania
- Epidemia spyware/grayware
- Epidemie naruszeń zapory
- Epidemia sesji folderów udostępnionych

Epidemia jest definiowana przez liczbę wykryć oraz przedział czasu. Epidemia powstaje, kiedy liczba wykryć zostaje przekroczona w określonym czasie wykrywania.

Program OfficeScan zawiera domyślne powiadomienia informujące administratorów OfficeScan o epidemii. Można zmodyfikować powiadomienia i skonfigurować dodatkowe ustawienia powiadamiania zgodnie z potrzebami.

Uwaga

Program OfficeScan może wysyłać powiadomienia o epidemii zagrożeń bezpieczeństwa za pomocą poczty elektronicznej, pułapki SNMP i dzienników zdarzeń systemu Windows NT. W przypadku epidemii sesji folderów udostępnionych program OfficeScan wysyła powiadomienia za pomocą poczty elektronicznej. Ustawienia należy skonfigurować, jeśli program OfficeScan wysyła powiadomienia za pomocą tych kanałów. Szczegółowe informacje zawiera sekcja *Ustawienia powiadamiania administratorów na stronie 14-37*.

Konfigurowanie kryteriów epidemii zagrożeń bezpieczeństwa oraz opcji powiadamiania

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Epidemia**.
2. Na karcie **Kryteria**:
   a. Przejdź do sekcji **Wirusy/złośliwe oprogramowanie** lub **Spyware/Grayware**.

b. Określ liczbę unikatowych źródeł wykryć.

c. Określ liczbę wykryć i okres wykrywania każdego zagrożenia bezpieczeństwa.

Porada

Firma Trend Micro zaleca zaakceptowanie domyślnych wartości na tym ekranie.

OfficeScan wysyła powiadomienie po zgłoszeniu łącznie 101 zagrożeń bezpieczeństwa przez 10 różnych typów przypadków wykrycia wirusa/złośliwego programu w okresie 5 godzin. Jeśli jeden agent ma 101 przypadków wykrycia wirusa/złośliwego programu dowolnego typu w okresie 5 godzin, program OfficeScan wysyła także powiadomienie o epidemii.

3. Na karcie **Kryteria**:

   a. Przejdź do sekcji **Sesje folderów udostępnionych**.

   b. Wybierz opcję **Monitoruj sesje folderów udostępnionych w sieci**.

   c. W sekcji **Sesje folderów udostępnionych** kliknij łącze z liczbą, aby wyświetlić punkty końcowe z udostępnionymi folderami i punkty końcowe, które uzyskały dostęp do folderów udostępnionych.

   d. Określ liczbę sesji folderów udostępnionych i okres wykrywania.

   Program OfficeScan wysyła komunikat z powiadomieniem po przekroczeniu określonej liczby sesji folderów udostępnionych.

4. Na karcie **E-mail**:

   a. Przejdź do sekcji **Epidemie wirusów/złośliwego oprogramowania**, **Epidemie spyware/grayware** i **Epidemie sesji folderów udostępnionych**.

   b. Wybierz opcję **Włącz powiadamianie za pomocą wiadomości e-mail**.

   c. Określ odbiorców wiadomości e-mail.

   d. Zaakceptuj lub zmień domyślny temat i wiadomość. Dane w polach **Temat** i **Wiadomość** można przedstawiać za pomocą znaczników.

TABELA 7-30. Zmienne znaczników dla powiadomień o epidemiach zagrożeń bezpieczeństwa

ZMIENNA	OPIS
Epidemie wirusów/złośliwego oprogramowania	
%CV	Ogólna liczba wykrytych wirusów/złośliwego oprogramowania
%CC	Łączna liczba punktów końcowych z wirusem/złośliwym oprogramowaniem
Epidemie oprogramowania spyware/grayware	
%CV	Ogólna liczba wykrytych programów spyware/grayware
%CC	Łączna liczba punktów końcowych z oprogramowaniem spyware/grayware
Epidemie sesji folderów udostępnionych	
%S	Liczba sesji folderów udostępnionych
%T	Okres gromadzenia sesji folderów udostępnionych
%M	Okres w minutach

e. Wybierz dodatkowe informacje o wirusach/złośliwym oprogramowaniu i oprogramowaniu spyware/grayware, które mają zostać dołączone do wiadomości e-mail. Można dołączyć informacje takie jak nazwa agenta/domeny, nazwa zagrożenia bezpieczeństwa, data i godzina wykrycia, ścieżka i zarażony plik oraz wyniki skanowania.

f. Zaakceptuj lub zmień domyślne wiadomości z powiadomieniem programu.

5. Na karcie **Pułapka SNMP**:

a. Przejdź do sekcji **Epidemie wirusów/złośliwego oprogramowania** lub **Epidemie spyware/grayware**.

b. Wybierz opcję **Włącz powiadamianie przez pułapkę SNMP**.

c. Zaakceptuj lub zmień domyślną wiadomość. Dane w polu **Wiadomość** można przedstawiać za pomocą znaczników. Szczegółowe informacje można

znaleźć w części *Tabela 7-30: Zmienne znaczników dla powiadomień o epidemiach zagrożeń bezpieczeństwa na stronie 7-121*.

6. Na karcie **Dziennik zdarzeń systemu Windows NT**:

   a. Przejdź do sekcji **Epidemie wirusów/złośliwego oprogramowania** lub **Epidemie spyware/grayware**.

   b. Wybierz opcję **Włącz powiadamianie przez rejestr zdarzeń NT**.

   c. Zaakceptuj lub zmień domyślną wiadomość. Dane w polu **Wiadomość** można przedstawiać za pomocą znaczników. Szczegółowe informacje można znaleźć w części *Tabela 7-30: Zmienne znaczników dla powiadomień o epidemiach zagrożeń bezpieczeństwa na stronie 7-121*.

7. Kliknij przycisk **Zapisz**.

Konfigurowanie zapobiegania epidemiom zagrożeń bezpieczeństwa

W przypadku wystąpienia epidemii należy zastosować środki ochrony przed epidemią wirusów, aby ją zlikwidować i zapobiec wydostaniu się poza sieć. Ustawienia ochrony należy konfigurować ostrożnie, ponieważ nieprawidłowa konfiguracja może spowodować nieprzewidziane problemy z siecią.

Procedura

1. Przejdź do opcji **Agenci** > **Ochrona przed epidemią**.

2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.

3. Kliknij opcję **Rozpocznij ochronę przed epidemią**.

4. Kliknij dowolną regułę ochrony przed epidemią, a następnie skonfiguruj ustawienia reguły:

   - *Ograniczanie/blokowanie dostępu do folderów udostępnionych na stronie 7-124*

- *Blokowanie narażonych portów na stronie 7-125*
- *Blokowanie prawa do zapisu w plikach i folderach na stronie 7-127*
- *Odmowa dostępu do wykonywalnych plików skompresowanych na stronie 7-129*
- *Tworzenie obsługi wzajemnego wykluczania dla procesów/plików złośliwego oprogramowania na stronie 7-128*

5. Wybierz reguły, które chcesz egzekwować.

6. Określ liczbę godzin, przez jaką ma być aktywna funkcja ochrony przed epidemią. Domyślne ustawienie to 48 godzin. Można ręcznie przywrócić ustawienia sieci przed końcem okresu ochrony przed epidemią.

OSTRZEŻENIE!

Funkcji ochrony przed epidemią nie można włączyć bezterminowo. Aby na stałe zablokować dostęp lub odmówić dostępu do określonych plików, folderów lub portów, należy bezpośrednio zmodyfikować ustawienia punktu końcowego oraz ustawienia sieciowe bez korzystania z programu OfficeScan.

7. Zaakceptuj lub zmień domyślne powiadomienie agenta.

Uwaga

Aby skonfigurować program OfficeScan tak, aby powiadamiał o epidemii, należy przejść do opcji **Administracja** > **Powiadomienia** > **Epidemia**.

8. Kliknij opcję **Rozpocznij ochronę przed epidemią**.

   Wybrane środki ochrony przed epidemią zostaną wyświetlone w nowym oknie.

9. W drzewie agentów ochrony przed epidemią zaznacz kolumnę **Ochrona przed epidemią**.

   Przy punktach końcowych stosujących środki ochrony przed epidemią pojawi się symbol zaznaczenia.

Program OfficeScan zapisuje następujące zdarzenia w dziennikach zdarzeń systemowych:

- zdarzenia związane z serwerem (inicjowanie ochrony przed epidemią i powiadamianie agentów o konieczności włączenia ochrony przed epidemią),
- zdarzenie związane z agentem OfficeScan (włączanie ochrony przed epidemią).

Reguły ochrony przed epidemią

Gdy wystąpi epidemia, należy zastosować następujące reguły:

- *Ograniczanie/blokowanie dostępu do folderów udostępnionych na stronie 7-124*
- *Blokowanie narażonych portów na stronie 7-125*
- *Blokowanie prawa do zapisu w plikach i folderach na stronie 7-127*
- *Odmowa dostępu do wykonywalnych plików skompresowanych na stronie 7-129*
- *Tworzenie obsługi wzajemnego wykluczania dla procesów/plików złośliwego oprogramowania na stronie 7-128*

Ograniczanie/blokowanie dostępu do folderów udostępnionych

W trakcie epidemii można ograniczać lub blokować dostęp do folderów udostępnionych w sieci, aby zapobiec rozprzestrzenianiu się zagrożeń przez foldery udostępnione.

Gdy jest stosowana ta reguła, użytkownicy nadal mogą udostępniać kolejne foldery, jednak w ich przypadku reguła ta nie ma zastosowania. W związku z tym należy zabronić użytkownikom udostępniania folderów podczas trwania epidemii lub ponownie wdrożyć regułę w celu zablokowania nowo udostępnionych folderów.

Procedura

1. Przejdź do opcji **Agenci** > **Ochrona przed epidemią**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij opcję **Rozpocznij ochronę przed epidemią**.

4. Kliknij opcję **Ograniczaj/blokuj dostęp do folderów udostępnionych**.

5. Wybierz odpowiednie opcje:

   - **Zezwól na dostęp tylko do odczytu**: Powoduje ograniczenie dostępu do folderów udostępnionych.
   - **Odmów dostępu**

   Uwaga

   Ustawienie dostępu tylko do odczytu nie jest stosowane do folderów udostępnionych, które wcześniej zostały skonfigurowane z całkowicie zablokowanym dostępem.

6. Kliknij przycisk **Zapisz**.

   Zostanie ponownie wyświetlony ekran **Ustawienia ochrony przed epidemią**.

7. Kliknij opcję **Rozpocznij ochronę przed epidemią**.

   Wybrane środki ochrony przed epidemią zostaną wyświetlone w nowym oknie.

Blokowanie narażonych portów

Podczas epidemii można blokować najbardziej zagrożone porty, które wirusy/złośliwe oprogramowanie mogą wykorzystywać do uzyskiwania dostępu do punktów końcowych programu Agent OfficeScan.

OSTRZEŻENIE!

Ustawienia ochrony przed epidemią należy konfigurować z zachowaniem ostrożności. Dzięki zablokowaniu używanych portów zależne od nich usługi sieciowe staną się niedostępne. Na przykład po zablokowaniu portu zaufanego program OfficeScan nie będzie mógł przez czas trwania epidemii komunikować się z agentami.

Procedura

1. Przejdź do opcji **Agenci** > **Ochrona przed epidemią**.

2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij opcję **Rozpocznij ochronę przed epidemią**.
4. Kliknij opcję **Blokowanie portów**.
5. Wybierz ustawienie opcji **Blokuj zaufany port**.
6. Wybierz porty do blokowania w kolumnie **Zablokowane porty**.
   a. Jeśli w tabeli nie ma żadnych portów, kliknij przycisk **Dodaj**. Na ekranie, który zostanie wyświetlony, wybierz porty do blokowania i kliknij przycisk **Zapisz**.
      - **Wszystkie porty (włączając ICMP)**: Powoduje zablokowanie wszystkich portów z wyjątkiem zaufanego. Aby zablokować również port zaufany, na poprzednim ekranie należy zaznaczyć pole wyboru Blokuj zaufany port.
      - **Określone porty**
        - **Popularne porty**: Wybierz co najmniej jeden numer portu, aby program OfficeScan mógł zapisać ustawienia blokowana portów.
        - **Popularne porty używane przez programy typu „koń trojański”**: Są blokowane porty często używane przez programy typu „koń trojański”. Szczegółowe informacje można znaleźć w części *Porty trojanów na stronie E-14*.
        - **Dowolny numer portu z zakresu od 1 do 65535 lub zakres portów**: opcjonalnie określ kierunek ruchu, który ma zostać zablokowany, i dodaj komentarze, na przykład powód blokowania określonych portów.
        - **Protokół ping (Odrzuć ICMP)**: Opcja ta pozwala zablokować pakiety ICMP, na przykład żądania typu ping.
   b. Aby edytować ustawienia blokowanego portu, kliknij jego numer.
   c. Na ekranie, który zostanie wyświetlony, zmień ustawienia i kliknij przycisk **Zapisz**.

d. Aby usunąć port z listy, zaznacz pole wyboru obok numeru portu i kliknij przycisk **Usuń**.

7. Kliknij przycisk **Zapisz**.

   Zostanie ponownie wyświetlony ekran **Ustawienia ochrony przed epidemią**.

8. Kliknij opcję **Rozpocznij ochronę przed epidemią**.

   Wybrane środki ochrony przed epidemią zostaną wyświetlone w nowym oknie.

Blokowanie prawa do zapisu w plikach i folderach

Wirusy/złośliwe oprogramowanie mogą modyfikować lub usuwać pliki oraz foldery z punktów końcowych będących hostami. Podczas epidemii program OfficeScan należy skonfigurować tak, aby zapobiec modyfikacji lub usuwaniu plików i folderów z punktów końcowych agentów.

OSTRZEŻENIE!

Program OfficeScan nie obsługuje odmowy prawa zapisu na zmapowanych dyskach sieciowych.

Procedura

1. Przejdź do opcji **Agenci** > **Ochrona przed epidemią**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij opcję **Rozpocznij ochronę przed epidemią**.
4. Kliknij opcję **Odmowa prawa zapisu do plików i folderów**.
5. Wpisz ścieżkę katalogu. Po wpisaniu ścieżki dostępu do katalogu, który ma być zabezpieczony, kliknij przycisk **Dodaj**.

Uwaga

Wprowadź bezwzględną ścieżkę dostępu do katalogu, a nie ścieżkę wirtualną.

6. Określ pliki, które mają być chronione w chronionych katalogach. Zaznacz wszystkie pliki lub pliki o określonych rozszerzeniach. Aby określić rozszerzenie, którego nie ma na liście, wpisz je w polu tekstowym, a następnie kliknij przycisk **Dodaj**.

7. Aby chronić określone pliki, w obszarze **Chronione pliki** wpisz pełną nazwę pliku i kliknij przycisk **Dodaj**.

8. Kliknij przycisk **Zapisz**.

   Zostanie ponownie wyświetlony ekran **Ustawienia ochrony przed epidemią**.

9. Kliknij opcję **Rozpocznij ochronę przed epidemią**.

   Wybrane środki ochrony przed epidemią zostaną wyświetlone w nowym oknie.

Tworzenie obsługi wzajemnego wykluczania dla procesów/plików złośliwego oprogramowania

Funkcję ochrony przed epidemią można skonfigurować w celu ochrony przed zagrożeniami bezpieczeństwa, które wykorzystują procesy mutex. Odbywa się to przez zastąpienie zasobów wymaganych przez zagrożenie do zarażania i rozprzestrzeniania się w systemie. Ochrona przed epidemią wirusów tworzy wzajemne wykluczenia plików i procesów związanych ze znanym złośliwym oprogramowaniem, co zapobiega dostępowi złośliwego oprogramowania do tych zasobów.

Porada

Firma Trend Micro zaleca obsługę tych wykluczeń do momentu, w którym będzie możliwe zaimplementowanie rozwiązania tego zagrożenia złośliwym oprogramowaniem. Skontaktuj się z pomocą techniczną, aby uzyskać prawidłowe nazwy obiektów mutex w celu zapewnienia ochrony podczas epidemii wirusów.

Uwaga

Obsługa wzajemnego wykluczania wymaga usługi zapobiegania nieautoryzowanym zmianom i obsługuje wyłącznie platformy 32-bitowe.

Procedura

1. Przejdź do opcji **Agenci** > **Ochrona przed epidemią**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij opcję **Rozpocznij ochronę przed epidemią**.
4. Kliknij opcję **Utwórz obsługę wzajemnego wykluczania (mutex) dla procesów/plików złośliwego oprogramowania**.
5. Wpisz w podanym polu nazwę obiektu mutex, dla którego wymagana jest ochrona.

   Nazwy obiektów mutex na liście można dodawać i usuwać za pomocą przycisków **+** i **-**.

   Uwaga

   Ochrona przed epidemią zapewnia obsługę wzajemnego wykluczania dla maksymalnie sześciu wątków mutex.

6. Kliknij przycisk **Zapisz**.

   Zostanie ponownie wyświetlony ekran **Ustawienia ochrony przed epidemią**.

7. Kliknij opcję **Rozpocznij ochronę przed epidemią**.

   Wybrane środki ochrony przed epidemią zostaną wyświetlone w nowym oknie.

Odmowa dostępu do wykonywalnych plików skompresowanych

Odmowa dostępu do wykonywalnych plików skompresowanych podczas epidemii może zapobiec w rozprzestrzenianiu się w sieci potencjalnych zagrożeń bezpieczeństwa, które mogą być zawarte w takich plikach. Można zezwolić na dostęp do zaufanych plików utworzonych przez obsługiwane programy do tworzenia wykonywalnych plików skompresowanych.

Procedura

1. Przejdź do opcji **Agenci** > **Ochrona przed epidemią**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij opcję **Rozpocznij ochronę przed epidemią**.
4. Kliknij opcję **Odmowa dostępu do wykonywalnych plików skompresowanych**.
5. Dokonaj wyboru na liście obsługiwanych programów do tworzenia wykonywalnych plików skompresowanych i kliknij przycisk **Dodaj**, aby zezwolić na dostęp do wykonywalnych plików skompresowanych utworzonych przez te programy.

   Uwaga

   Można zezwolić wyłącznie na użycie skompresowanych plików, które zostały utworzone przez programy znajdujące się na liście programów do tworzenia wykonywalnych plików skompresowanych. Ochrona przed epidemią odmawia dostępu do wszystkich innych formatów wykonywalnych plików skompresowanych.

6. Kliknij przycisk **Zapisz**.

   Zostanie ponownie wyświetlony ekran **Ustawienia ochrony przed epidemią**.

7. Kliknij opcję **Rozpocznij ochronę przed epidemią**.

   Wybrane środki ochrony przed epidemią zostaną wyświetlone w nowym oknie.

Wyłączenie ochrony przed epidemią

Jeśli istnieje pewność, że epidemia została powstrzymana i program OfficeScan wyczyścił lub poddał kwarantannie wszystkie zarażone pliki, można przywrócić normalne ustawienia sieciowe, wyłączając ochronę przed epidemią wirusów.

Procedura

1. Przejdź do opcji **Agenci** > **Ochrona przed epidemią**.

2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, albo wybierz określone domeny lub agentów.
3. Kliknij polecenie **Przywróć ustawienia**.
4. Aby poinformować użytkowników o powstrzymaniu epidemii, wybierz polecenie **Powiadamiaj użytkowników po przywróceniu oryginalnych ustawień**.
5. Zaakceptuj lub zmień domyślne powiadomienie agenta.
6. Kliknij polecenie **Przywróć ustawienia**.

Uwaga

Jeżeli ustawienia sieciowe nie zostaną przywrócone ręcznie, program OfficeScan przywróci je automatycznie po upływie czasu określonego w polu **Automatycznie przywróć normalne ustawienia sieciowe po __ godzinach** na ekranie **Ustawienia ochrony przed epidemią**. Domyślne ustawienie to 48 godzin.

Program OfficeScan zapisuje następujące zdarzenia w dziennikach zdarzeń systemowych:

- zdarzenia związane z serwerem (inicjowanie ochrony przed epidemią i powiadamianie agentów o konieczności włączenia ochrony przed epidemią),
- zdarzenie związane z agentem OfficeScan (włączanie ochrony przed epidemią).

7. Po wyłączeniu ochrony przed epidemią należy przeskanować punkty końcowe w sieci w poszukiwaniu zagrożeń bezpieczeństwa, aby się upewnić, że epidemia została powstrzymana.

Rozdział 8

Ochrona przed nieznanymi zagrożeniami

W tym rozdziale przedstawiono sposób ochrony punktów końcowych przed nieznanymi zagrożeniami, które podejmują próbę infiltracji sieci.

Rozdział składa się z następujących tematów:

Predykcyjne uczenie maszynowe

Przewidujące uczenie maszynowe Trend Micro korzysta z zaawansowanej technologii uczenia maszynowego w celu tworzenia powiązań z informacjami o zagrożeniu oraz wykonuje szczegółową analizę w celu wykrywania nieznanych zagrożeń bezpieczeństwa przez stosowanie cyfrowych znaczników DNA, mapowania interfejsu API oraz innych cech plików. Predykcyjne uczenie maszynowe wykonuje także analizę zachowania nieznanych lub sporadycznie występujących procesów w celu określenia, czy nowe lub nieznane zagrożenie podejmuje próbę infekcji sieci.

Predykcyjne uczenie maszynowe to zaawansowane narzędzie, które pomaga chronić środowisko przed niezidentyfikowanymi zagrożeniami i nowymi atakami.

Typ wykrytego zagrożenia	Opis
Plik	Po wykryciu nieznanego lub sporadycznie występującego pliku program OfficeScan skanuje plik przy użyciu silnika skanowania w poszukiwaniu zagrożeń zaawansowanych w celu wyodrębnienia cech pliku, a następnie wysyła raport do silnika przewidującego uczenia maszynowego w sieci Trend Micro Smart Protection Network. Korzystając z funkcji modelowania złośliwego oprogramowania, predykcyjne nauczanie maszynowe porównuje próbkę z modelem złośliwego oprogramowania, przypisuje ocenę prawdopodobieństwa i określa prawdopodobny typ złośliwego oprogramowania zawartego w pliku. W zależności od konfiguracji przewidującego nauczania maszynowego, program OfficeScan może wykonać próbę poddania określonego pliku “kwarantannie”, aby zapobiec rozprzestrzenianiu się zagrożenia w sieci.

Typ wykrytego zagrożenia	Opis
Proces	Po wykryciu nieznanego lub sporadycznie występującego pliku program OfficeScan monitoruje proces przy użyciu silnika analizy kontekstowej i wysyła raport dotyczący zachowania do silnika przewidującego uczenia maszynowego. Korzystając z funkcji modelowania zachowania złośliwego oprogramowania, predykcyjne nauczanie maszynowe porównuje zachowanie procesu z modelem, przypisuje ocenę prawdopodobieństwa i określa prawdopodobny typ złośliwego oprogramowania wykonywanego przez proces. W zależności od konfiguracji przewidującego nauczania maszynowego, program OfficeScan może “przerwać” odpowiedni proces i podjąć próbę wyczyszczenia pliku, który uruchomił ten proces.

Konfigurowanie ustawień przewidującego uczenia maszynowego

Uwaga

Predykcyjne uczenie maszynowe wymaga włączenia następujących usług:

- Zapobieganie nieautoryzowanym zmianom
- Usługa zaawansowanej ochrony

Aby uzyskać więcej informacji, patrz *Włączanie lub wyłączanie usług agenta za pośrednictwem konsoli Web na stronie 15-8*.

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij opcje **Ustawienia** > **Ustawienia przewidującego uczenia maszynowego**.

Zostanie wyświetlony ekran **Ustawienia przewidującego uczenia maszynowego**.

4. Wybierz opcję **Włącz predykcyjne uczenie maszynowe**.

5. W sekcji **Ustawienia wykrywania** wybierz typ wykrywanych zagrożeń i powiązane działanie podejmowane przez funkcję przewidującego uczenia maszynowego.

TYP WYKRYTEGO ZAGROŻENIA	OPERACJE
Plik	• **Kwarantanna**: Wybierz tę opcję, aby automatycznie poddać kwarantannie pliki o cechach związanych ze złośliwym oprogramowaniem na podstawie analizy przewidującego uczenia maszynowego • **Tylko dziennik**: Wybierz tę opcję, aby skanować nieznane pliki i zapisywać analizę przewidującego uczenia maszynowego w dzienniku w celu dalszego zbadania zagrożenia w firmie
Proces	• **Przerwij**: Wybierz tę opcję, aby automatycznie przerwać procesy o zachowaniach związanych ze złośliwym oprogramowaniem na podstawie analizy przewidującego uczenia maszynowego **Ważne** Predykcyjne uczenie maszynowe podejmuje próbę wyczyszczenia plików, które uruchomiły złośliwe procesy. Jeśli czyszczenie się nie powiedzie, program OfficeScan poddaje odpowiednie pliki kwarantannie. • **Tylko dziennik**: Wybierz tę opcję, aby skanować nieznane procesy i zapisywać analizę przewidującego uczenia maszynowego w dzienniku w celu dalszego zbadania zagrożenia w firmie

6. W sekcji **Wyjątki** skonfiguruj globalną listę wyjątków przewidującego uczenia maszynowego, aby uniemożliwić wszystkim agentom wykrywanie pliku jako złośliwego.

a. Kliknij opcję **Dodaj skrót pliku**.

   Zostanie wyświetlony ekran **Dodaj plik do listy wyjątków**.

b. Określ wartość skrótu SHA-1 pliku w celu wykluczenia ze skanowania.

c. Opcjonalnie dodaj notatkę z przyczyną utworzenia wyjątku lub opisz nazwy plików związanych z wartością skrótu.

d. Kliknij przycisk **Dodaj**.

   Program OfficeScan doda skrót pliku do listy wyjątków.

7. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.

   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Usługa podejrzanego połączenia

Usługa podejrzanego połączenia zarządza zdefiniowaną przez użytkownika listą adresów IP oraz globalną listą adresów IP C&C, a także monitoruje zachowanie połączeń nawiązywanych przez punkty końcowe z potencjalnymi serwerami C&C.

- Zdefiniowane przez użytkownika listy dozwolonych i zablokowanych adresów IP zapewniają dalszą kontrolę nad tym, czy punkty końcowe mogą uzyskać dostęp do określonych adresów IP. Należy skonfigurować te listy, aby zapewnić dostęp do adresu zablokowanego przez globalną listę adresów IP C&C lub zablokować dostęp do adresu, który może stanowić zagrożenie bezpieczeństwa.

  Szczegółowe informacje zawiera sekcja *Konfigurowanie globalnych, zdefiniowanych przez użytkownika list adresów IP na stronie 8-6*.

- Globalna lista adresów IP C&C działa w połączeniu z silnikiem kontroli zawartości sieciowej (NCIE) w celu wykrywania połączeń sieciowych z serwerami C&C, które zostały potwierdzone przez firmę Trend Micro. Silnik NCIE wykrywa kontakt z serwerem C&C przez dowolny kanał sieciowy. Usługa podejrzanego połączenia rejestruje informacje o wszystkich połączeniach z serwerami z globalnej listy adresów IP C&C na potrzeby oceny.

  Szczegółowe informacje na temat włączania globalnej listy adresów IP C&C zawiera temat *Konfigurowanie ustawień podejrzanego połączenia na stronie 8-7*.

- Po wykryciu złośliwego oprogramowania na punktach końcowych poprzez dopasowanie sygnatury zasady istotności do pakietów sieciowych usługa podejrzanego połączenia może dalej badać zachowanie połączenia w celu określenia, czy wystąpiło wywołanie zwrotne C&C. Kiedy zostanie wykryte wywołanie zwrotne C&C, usługa podejrzanego połączenia może podjąć próbę zablokowania i wyczyszczenia źródła połączenia przy użyciu technologii GeneriClean.

  Szczegółowe informacje na temat konfigurowania usługi podejrzanego połączenia zawiera sekcja *Konfigurowanie ustawień podejrzanego połączenia na stronie 8-7*.

  Szczegółowe informacje o technologii GeneriClean zawiera sekcja *GeneriClean na stronie E-5*.

Włącz usługę podejrzanego połączenia na ekranie **Ustawienia dodatkowej usługi**, aby chronić agentów przed wywołaniami zwrotnymi serwera C&C. Szczegółowe informacje zawiera sekcja *Włączanie lub wyłączanie usług agenta za pośrednictwem konsoli Web na stronie 15-8*.

Konfigurowanie globalnych, zdefiniowanych przez użytkownika list adresów IP

Administratorzy mogą skonfigurować program OfficeScan w celu zezwalania, blokowania lub rejestrowania wszystkich połączeń między agentami a zdefiniowanymi przez użytkownika adresami IP C&C.

Uwaga

Zdefiniowane przez użytkownika listy adresów IP obsługują tylko adresy IPv4.

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Kliknij kartę **Ustawienia zabezpieczeń**.
3. Przejdź do sekcji **Ustawienia podejrzanego połączenia**.
4. Kliknij opcję **Edytuj zdefiniowaną przez użytkownika listę adresów IP**.
5. Na karcie **Lista dozwolonych** lub **Lista zablokowanych** dodaj adresy IP, które chcesz monitorować.

   Porada

   Program OfficeScan można skonfigurować w celu rejestrowania tylko połączeń nawiązywanych z adresami znajdującymi się na zdefiniowanej przez użytkownika liście zablokowanych adresów IP. Aby rejestrować tylko połączenia nawiązywane z adresami znajdującymi się na zdefiniowanej przez użytkownika liście zablokowanych adresów IP, patrz sekcja *Konfigurowanie ustawień podejrzanego połączenia na stronie 8-7*.

   a. Kliknij przycisk **Dodaj**.

   b. Na wyświetlonym ekranie wpisz adres IP, zakres adresów IP lub adres IPv4 i maskę podsieci w celu monitorowania przez program OfficeScan.

   c. Kliknij przycisk **Zapisz**.

6. Aby usunąć adresy IP z listy, zaznacz pole wyboru obok adresu i kliknij przycisk **Usuń**.
7. Po skonfigurowaniu list kliknij przycisk **Zamknij**, aby wrócić do ekranu **Ustawienia agenta globalnego**.
8. Kliknij przycisk **Zapisz**, aby zastosować zaktualizowaną listę na agentach.

Konfigurowanie ustawień podejrzanego połączenia

Program OfficeScan może rejestrować i blokować wszystkie połączenia nawiązywane między agentami a adresami na globalnej liście adresów IP C&C. Ekran **Ustawienia**

podejrzanego połączenia także umożliwia rejestrowanie, jak również zapewnia dostęp do adresów IP skonfigurowanych na zdefiniowanej przez użytkownika liście zablokowanych adresów IP.

Program OfficeScan może także monitorować połączenia powodowane przez sieć botów lub inne zagrożenie złośliwym oprogramowaniem. Po wykryciu zagrożenia złośliwym oprogramowaniem program OfficeScan może podjąć próbę wyczyszczenia infekcji.

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij kolejno pozycje **Ustawienia** > **Ustawienia podejrzanego połączenia**.

   Zostanie wyświetlony ekran **Ustawienia podejrzanego połączenia**.
4. Włącz ustawienie **Wykrywaj połączenia sieciowe nawiązywane z adresami na globalnej liście adresów IP C&C**, aby monitorować połączenia z serwerami C&C, które zostały potwierdzone przez firmę Trend Micro, a następnie wybierz opcję **Tylko dziennik** lub **Zablokuj** dla połączeń.

   - Aby umożliwić agentom łączenie się z adresami na zdefiniowanej przez użytkownika liście zablokowanych adresów IP, włącz ustawienie **Rejestruj i zezwalaj na dostęp do zdefiniowanej przez użytkownika listy zablokowanych adresów IP**.

Uwaga

Aby program OfficeScan mógł zezwalać na dostęp do adresów na zdefiniowanej przez użytkownika liście zablokowanych adresów IP, należy włączyć rejestrowanie połączeń sieciowych.

Szczegółowe informacje o globalnej liście adresów IP C&C zawiera temat *Usługa podejrzanego połączenia na stronie 8-5*.

5. Włącz ustawienie **Wykrywaj połączenia przy użyciu pakietu identyfikacyjnego złośliwej sieci**, a następnie wybierz opcję **Tylko dziennik** lub **Zablokuj** dla połączeń.

   Funkcja rejestrowania połączenia przy użyciu pakietu identyfikacyjnego złośliwej sieci dopasowuje sygnatury w nagłówkach pakietów. Program OfficeScan rejestruje wszystkie połączenia nawiązywane przez pakiety z nagłówkami pasującymi do znanych zagrożeń złośliwym oprogramowaniem, używając do tego celu sygnatury zasady istotności.

   - Aby umożliwić programowi OfficeScan podjęcie próby wyczyszczenia połączeń nawiązywanych z serwerami C&C, włącz ustawienie **Wyczyść podejrzane połączenia, gdy zostanie wykryte wywołanie zwrotne C&C**. Program OfficeScan używa technologii GeneriClean do czyszczenia zagrożenia złośliwym oprogramowaniem i przerwania połączenia z serwerem C&C.

   Uwaga

   Aby program OfficeScan podejmował próby czyszczenia połączeń nawiązywanych z serwerami C&C, które zostały wykryte przez dopasowywanie struktury pakietów, należy włączyć opcję **Rejestruj połączenia przy użyciu pakietu identyfikacyjnego złośliwej sieci**.

6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Przesyłanie próbek

Możesz skonfigurować Agenci OfficeScan w celu przesyłania obiektów plikowych, które mogą zawierać wcześniej niezidentyfikowane zagrożenia, do usługi Virtual Analyzer w celu przeprowadzenia dalszej analizy. Po dokonaniu oceny obiektów usługa Virtual Analyzer dodaje wszystkie obiekty z nieznanymi zagrożeniami do list podejrzanych obiektów usługi Virtual Analyzer, a następnie rozsyła te listy do innych Agenci OfficeScan w sieci.

Aby uzyskać więcej informacji, patrz *Ustawienia listy podejrzanych obiektów na stronie 14-33*.

W celu przesyłania próbek wymagane są następujące warunki:

- Należy zarejestrować serwer OfficeScan na serwerze Trend Micro Control Manager (wersja 6.0 SP3 z poprawką 2 lub nowszą)
- Serwer Trend Micro Control Manager musi mieć aktywne połączenie z serwerem Trend Micro Deep Discovery Analyzer (wersja 5.1 lub nowsza)

Do podejrzanych plików zaliczamy:

- Programy nieznane firmie Trend Micro (pobrane w obsługiwanych przeglądarkach internetowych lub pocztą e-mail)
- Procesy wykryte algorytmami heurystycznymi (pobrane w obsługiwanych przeglądarkach internetowych lub pocztą e-mail)
- Sporadycznie występujące programy autostartu na dyskach wymiennych

Ważne

Agenci OfficeScan mogą przesyłać pliki próbek o maksymalnym rozmiarze 50 MB do usługi Virtual Analyzer w celu analizy.

Konfigurowanie przesyłania próbek

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.

2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij opcje **Ustawienia** > **Ustawienia przesyłania próbek**.

   Zostanie wyświetlony ekran **Ustawienia przesyłania próbek**.
4. Wybierz opcję **Włącz przesyłanie podejrzanych plików do usługi Virtual Analyzer**.
5. Kliknij przycisk **Zapisz**.

Dzienniki nieznanych zagrożeń

Agenci OfficeScan rejestrują aktywność nieznanych zagrożeń i wysyłają dzienniki do serwera. Agent OfficeScan, który jest stale uruchomiony, agreguje dzienniki i wysyła je na serwer w określonych odstępach czasu, wynoszących domyślnie 60 minut.

Aby dzienniki nie zajmowały zbyt dużo miejsca na dysku twardym, można je ręcznie usunąć lub skonfigurować harmonogram ich usuwania. Dodatkowe informacje dotyczące dzienników zarządzania zawiera sekcja *Zarządzanie dziennikiem na stronie 14-41*.

Wyświetlanie dzienników przewidującego uczenia maszynowego

Procedura

1. Przejdź do opcji **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa** lub **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij opcje **Wyświetl dzienniki** > **Dzienniki przewidującego uczenia maszynowego** lub **Dzienniki** > **Dzienniki przewidującego uczenia maszynowego**.

4. Określ kryteria dziennika i kliknij przycisk **Wyświetl dzienniki**.

5. Wyświetl dzienniki. Dziennik zawiera następujące informacje:

ELEMENT	OPIS
Data/godzina	Godzina wykrycia
Punkt końcowy	Punkt końcowy, na którym nastąpiło wykrycie
Adres IP	Adres IP źródłowego punktu końcowego i jego numer portu
Zagrożenie bezpieczeństwa	Nazwa zagrożenia bezpieczeństwa określona przez silnik przewidującego uczenia maszynowego
Wynik	Wynik wykonanej operacji
Nazwa pliku	Nazwa obiektu plikowego lub programu, który wykonał proces
Typ	Typ obiektu, który wyzwolił wykrycie (“Plik” lub “Proces”)
Ścieżka pliku	Ścieżka obiektu plikowego lub programu, który wykonał proces
Kanał zarażenia	Kanał, z którego pochodzi zagrożenie
Szczegóły	Łącze powodujące wyświetlenie szczegółowej analizy określonego wykrycia Aby uzyskać więcej informacji, patrz *Szczegóły dziennika przewidującego uczenia maszynowego na stronie 8-12*.

6. Aby zapisać dzienniki jako plik rozdzielany przecinkami (CSV), kliknij opcję **Eksportuj wszystkie do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Szczegóły dziennika przewidującego uczenia maszynowego

Szczegółowy raport dla każdego wykrycia w dzienniku przewidującego uczenia maszynowego można wyświetlić, klikając łącze **Wyświetl** w kolumnie **Szczegóły**.

Ekran **Szczegóły dziennika** składa się z dwóch sekcji:

- Górny baner: szczegóły związane z określonym wykryciem w dzienniku
- Elementy sterujące na dolnej karcie: szczegóły związane z zagrożeniem przewidującego uczenia maszynowego, takie jak oceny prawdopodobieństwa zagrożenia, informacje o pliku i inne punkty końcowe w sieci, na których wystąpiło to samo wykrycie

Poniższa tabela przedstawia informacje dostępne na górnym banerze.

TABELA 8-1. Szczegóły dziennika — górny baner

SEKCJA	OPIS
Godzina wykrycia / działanie	Wskazuje, kiedy wystąpiło określone wykrycie w dzienniku oraz działanie podjęte przez agenta dla zagrożenia
Nazwa pliku	Wskazuje nazwę pliku, który spowodował rozpoczęcie wykrywania na określonym punkcie końcowym **Porada** Kliknij opcję **Dodaj do listy wyjątków**, aby szybko dodać wartość skrótu odpowiedniego pliku do globalnej listy wyjątków przewidującego uczenia maszynowego. Całą listę wyjątków można wyświetlić na ekranie **Ustawienia przewidującego uczenia maszynowego**. Aby uzyskać więcej informacji, patrz *Konfigurowanie ustawień przewidującego uczenia maszynowego na stronie 8-3*. **Ważne** Nazwa wykrytego pliku dla tego wykrycia może się różnić od nazwy pliku wykrytego na innych agentach. Predykcyjne uczenie maszynowe tworzy powiązania wykryć na podstawie wartości skrótu plików, a nie określonych nazw plików. Aby sprawdzić nazwę pliku na innych punktach końcowych, wyświetl kartę **Zmodyfikowane punkty końcowe**.

Sekcja	Opis
Informacje o punkcie końcowym	Wyświetla zalogowanego użytkownika w momencie wykrycia oraz nazwę i adres IP punktu końcowego
Informacje o kanale	Wyświetla kanał, z którego pochodzi zagrożenie, oraz lokalizację folderu na punkcie końcowym, do którego przeniesiono zagrożenie

Poniższa tabela przedstawia informacje dostępne na dolnych kartach.

Tabela 8-2. Szczegóły dziennika — informacje na kartach

Karta	Opis
Wskaźniki zagrożenia	Przedstawia wyniki analizy przewidującego uczenia maszynowego • **Prawdopodobieństwo zagrożenia**: Wskazuje stopień dopasowania pliku/procesu do modelu złośliwego oprogramowania • **Prawdopodobny typ zagrożenia**: Wskazuje najbardziej prawdopodobny typ zagrożenia zawartego w pliku po wykonaniu przewidującego uczenia maszynowego w porównaniu z analizą innych znanych zagrożeń • **Identyfikatory zagrożeń**: Przedstawia listę funkcji interfejsu API używanych przez plik/proces, które mogą wskazywać wykryty typ zagrożenia **Ważne** Identyfikacja funkcji interfejsu API to tylko jeden czynnik podczas określania typu zagrożenia. Predykcyjne uczenie maszynowe wykorzystuje wiele innych cech plików i metod analizy do obliczania prawdopodobieństwa zagrożenia i jego potencjalnego typu. • **Podobne znane zagrożenia**: Przedstawia listę znanych typów zagrożeń, które mają podobne cechy pliku/procesu jak wykryty plik

KARTA	OPIS
Szczegóły pliku	Przedstawia ogólne szczegóły związane z właściwościami pliku i informacje o certyfikacie dla dziennika tego wykrycia
Zmodyfikowane punkty końcowe	Przedstawia listę innych agentów z sieci z tym samym zagrożeniem wykrytym przez predykcyjne uczenie maszynowe, a także szczegółowe informacje o wykryciach na innych agentach

Przeglądanie dzienników podejrzanego połączenia

Procedura

1. Przejdź do opcji **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa** lub **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij kolejno pozycje **Wyświetl dzienniki** > **Dzienniki podejrzanego połączenia** lub **Dzienniki** > **Dzienniki podejrzanego połączenia**.
4. Określ kryteria dziennika i kliknij przycisk **Wyświetl dzienniki**.
5. Wyświetl dzienniki. Dziennik zawiera następujące informacje:

ELEMENT	OPIS
Data i godzina	Godzina wykrycia
Punkt końcowy	Punkt końcowy, na którym nastąpiło wykrycie
Domena	Domena punktu końcowego, na którym nastąpiło wykrycie
Proces	Proces, który zainicjował transmisję (ścieżka \nazwa_aplikacji)
Lokalny adres IP i port	Adres IP źródłowego punktu końcowego i jego numer portu

Element	Opis
Zdalny adres IP i port	Adres IP docelowego punktu końcowego i jego numer portu
Wynik	Wynik wykonanej operacji
Wykryto przez	Źródło listy C&C, która zidentyfikowała serwer C&C
Kierunek ruchu	Kierunek transmisji

6. Aby zapisać dzienniki jako plik rozdzielany przecinkami (CSV), kliknij opcję **Eksportuj wszystkie do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Wyświetlanie dzienników przesyłania próbek

Program OfficeScan przechowuje dane przesłanych próbek w dziennikach zdarzeń systemowych. Aby uzyskać bardziej wszechstronne podsumowanie danych przesłanych próbek, firma Trend Micro zaleca wyświetlanie dzienników przy użyciu konsoli Control Manager. Program Control Manager zapewnia szczegółową analizę procesu obsługi podejrzanego pliku obiektu, co umożliwia lepszy wgląd w informacje, jak podejrzane obiekty mogą wpłynąć na sieć.

Procedura

1. Przejdź do opcji **Dzienniki** > **Zdarzenia systemowe**.
2. W obszarze **Zdarzenie** sprawdź następujące typy dzienników:
   - "Przesłano próbkę do usługi Virtual Analyzer [plik[<nazwa_pliku], SHA1[<wartość_SHA1_pliku>]"
   - "Ukończono analizę próbki w usłudze Virtual Analyzer [<data_godzina_ukończenia_analizy>, plik[<nazwa_pliku], SHA1[<wartość_SHA1_pliku>], wirus[<typ_wykrycia], reguła[<typ_reguły_virtual_analyzer]]"

Rozdział 9

Korzystanie z funkcji Monitorowanie zachowań

W tym rozdziale przedstawiono sposób ochrony komputerów przed zagrożeniami bezpieczeństwa przy użyciu funkcji Monitorowanie zachowań.

Rozdział składa się z następujących tematów:

Monitorowanie zachowań

Monitorowanie zachowań stale monitoruje punkty końcowe w poszukiwaniu nieoczekiwanych modyfikacji systemu operacyjnego i zainstalowanego oprogramowania. Chroni punkty końcowe poprzez **blokowanie działania złośliwego oprogramowania** i **monitorowanie zdarzeń**. Te dwie funkcje uzupełnia skonfigurowana przez użytkownika **lista wyjątków** i **usługa Certified Safe Software**.

Ważne

- Usługa monitorowania zachowań nie jest zgodna z 64-bitowymi systemami Windows XP i Windows 2003.
- Usługa monitorowania zachowań nie jest zgodna z 64-bitowymi systemami Windows Vista z dodatkiem SP1 lub nowszym.
- Monitorowanie zachowań jest domyślnie wyłączone we wszystkich wersjach systemów Windows Server. Przed włączeniem monitorowania zachowań na tych platformach serwerowych należy zapoznać się z wytycznymi i sprawdzonymi metodami przedstawionymi w sekcji *Usługi agenta OfficeScan na stronie 15-7*.

Blokowanie działania złośliwego oprogramowania

Funkcja blokowania działania złośliwego oprogramowania zapewnia niezbędną warstwę dodatkowej ochrony przed zagrożeniami powodowanymi przez programy, które wykonują złośliwe działania. Funkcja ta obserwuje zdarzenia systemowe w przedziale czasu. Podczas gdy programy wykonują różne kombinacje lub sekwencje działań, funkcja blokowania działania złośliwego oprogramowania wykrywa znane złośliwe działania i blokuje powiązane programy. Korzystanie z tej funkcji pozwala uzyskać wyższy stopień ochrony przed nowymi, nieznanymi zagrożeniami.

W przypadku blokowania działania złośliwego oprogramowania dostępne są następujące opcje skanowania w zależności od poziomu zagrożenia:

- **Znane zagrożenia**: Blokowanie zachowań związanych ze znanymi zagrożeniami
- **Znane i potencjalne zagrożenia**: Blokowanie zachowań związanych ze znanymi zagrożeniami i podejmowanie działań wobec zachowań potencjalnie szkodliwych

Jeśli program zostanie zablokowany, a powiadomienia są włączone, program OfficeScan wyświetli powiadomienie na punkcie końcowym agenta OfficeScan. Szczegółowe informacje na temat powiadomień zawiera sekcja *Powiadomienia monitorowania zachowań dla użytkowników agenta OfficeScan na stronie 9-17*.

Ochrona przed oprogramowaniem typu ransomware

Ochrona przed oprogramowaniem typu ransomware zapobiega nieautoryzowanemu modyfikowaniu lub szyfrowaniu plików na agentach OfficeScan przez zagrożenia "ransomware". Ransomware to typ złośliwego oprogramowania, które ogranicza dostęp do plików i domaga się dokonania płatności w celu przywrócenia tych plików.

Program OfficeScan zapewnia następujące metody ochrony środowiska przed zagrożeniami ransomware.

Uwaga

Aby ograniczyć możliwość uznania przez program OfficeScan bezpiecznego procesu za złośliwy, należy upewnić się, że agent ma dostęp do Internetu w celu przeprowadzenia dodatkowych procesów weryfikacji z użyciem serwerów firmy Trend Micro.

Opcja	Opis
Chroń dokumenty przed nieautoryzowanym szyfrowaniem lub modyfikacją.	Monitorowanie zachowania można skonfigurować w celu wykrywania określonej sekwencji zdarzeń, która może wskazywać atak typu ransomware. Gdy funkcja Monitorowanie zachowania stwierdzi spełnienie wszystkich poniższych kryteriów, program OfficeScan kończy działanie złośliwych programów i poddaje je kwarantannie: 1. Program, który nie został rozpoznany jako bezpieczny, podejmuje próby zmodyfikowania, usunięcia lub zmiany nazwy trzech plików w określonym przedziale czasu. 2. Proces podejmuje próbę zmodyfikowania typu rozszerzenia chronionego pliku. Dodatkowo włącz opcję **Automatycznie twórz kopie zapasowe plików zmienionych przez podejrzane programy**, aby tworzyć kopie plików szyfrowanych na punktach końcowych. Gdy proces szyfrowania zakończy się, a program OfficeScan wykryje zagrożenie ransomware, program OfficeScan wyświetla użytkownikom końcowym monit o przywrócenie zmodyfikowanych plików bez utraty żadnych danych.  **Uwaga** Automatyczne tworzenie kopii zapasowych wymaga co najmniej 100 MB miejsca na dysku punktu końcowego agenta. Tworzona jest kopia zapasowa tylko tych plików, których rozmiar jest mniejszy niż 10 MB. Lokalizacja folderu kopii zapasowej na punktach końcowych agentów to: <folder instalacji agenta>`\CCSF \module\DRE\data`.  **OSTRZEŻENIE!** Jeśli opcja **Automatycznie twórz kopie zapasowe plików zmienionych przez podejrzane programy** nie została włączona, program OfficeScan nie może odzyskać pierwszych plików zmodyfikowanych przez zagrożenie ransomware.

Opcja	Opis
Blokuj procesy często powiązane z oprogramowaniem typu ransomware.	Procesy typu ransomware zwykle rozmieszczają pliki wykonywalne w konkretnych miejscach na punktach końcowych przed podjęciem próby przejęcia plików. Blokowanie procesów, które zostały uruchomione w tych lokalizacjach, może zapobiec przejmowaniu plików przez programy typu ransomware.
Włącz inspekcję programów, aby wykrywać i blokować zaatakowane pliki wykonywalne	Inspekcja programów monitoruje procesy i przechwytuje interfejs API w celu określenia, czy program zachowuje się w nieoczekiwany sposób. Chociaż procedura ta zwiększa ogólny wskaźnik wykrywania zaatakowanych plików wykonywalnych, może ona obniżać wydajność systemu. **Porada** Inspekcja programów zapewnia wyższy poziom bezpieczeństwa w przypadku wyboru opcji **Znane i potencjalne zagrożenia** w menu rozwijanym **Blokowane zagrożenia**. **Ważne** Funkcja nie jest obsługiwana w systemie Windows Server 2003 bez dodatku SP2 (lub nowszego) ani w 64-bitowych systemach Windows XP.

Ochrona przed programami wykorzystującymi luki

Ochrona przed programami wykorzystującymi luki działa wspólnie z inspekcją programów w celu monitorowania zachowania programów i wykrywania nieprawidłowego zachowania, które może wskazywać, że osoba atakująca wykorzystała lukę w programie. Po wykryciu takiego zdarzenia usługa monitorowania zachowań kończy działanie procesów programu.

Ważne

Ochrona przed programami wykorzystującymi luki wymaga wybrania opcji **Włącz inspekcję programów, aby wykrywać i blokować zaatakowane pliki wykonywalne**.

Ochrona przed nowo napotkanymi programami

Monitorowanie zachowania działa w połączeniu z usługami Web Reputation Services i skanowaniem w czasie rzeczywistym w celu weryfikacji ogromnej ilości plików pobieranych przez kanały HTTP, aplikacje poczty elektronicznej i skrypty makr pakietu Microsoft Office. Po wykryciu „nowo napotkanego" pliku administratorzy mogą wybrać monitowanie użytkowników przed wykonaniem pliku. Firma Trend Micro klasyfikuje program jako nowo napotkany na podstawie liczby wykrytych plików lub wieku historycznego pliku zgodnie z definicją sieci Smart Protection Network.

Monitorowanie zachowań skanuje następujące typy plików dla każdego kanału:

- HTTP/HTTPS: Skanuje pliki `.exe`.
- Aplikacje poczty elektronicznej: Skanuje pliki `.exe` i skompresowane pliki `.exe` w niezaszyfrowanych plikach `.zip` i `.rar`.

Uwaga

- Aby możliwe było wyświetlenie tego monitu, administratorzy muszą wcześniej włączyć usługi Web Reputation Services na agencie w celu skanowania ruchu HTTP lub HTTPS przez program OfficeScan.
- Podczas procesu wykonywania program OfficeScan dopasowuje nazwy plików pobranych przez aplikacje poczty elektronicznej. Jeśli nazwa pliku została zmieniona, monit nie jest wyświetlany użytkownikowi.

Monitorowanie zdarzeń

Monitorowanie zdarzeń zapewnia ogólniejsze podejście do ochrony przed nieautoryzowanym oprogramowaniem i atakami złośliwego oprogramowania. Funkcja ta monitoruje obszary systemowe pod kątem określonych zdarzeń, umożliwiając administratorom kontrolowanie programów wyzwalających takie zdarzenia. Funkcji monitorowania zdarzeń należy używać w przypadku określonych wymagań dotyczących ochrony systemu, które wykraczają poza możliwości zapewniane przez funkcję blokowania działania złośliwego oprogramowania.

W poniższej tabeli przedstawiono listę monitorowanych zdarzeń systemowych.

Tabela 9-1. Monitorowane zdarzenia systemowe

Zdarzenia	Opis
Zduplikowany system plików	Wiele złośliwych programów tworzy kopie siebie lub innych złośliwych programów przy użyciu nazw plików systemowych Windows. Zwykle ma to na celu nadpisanie lub zastąpienie plików systemowych, zapobieżenie wykryciu lub zniechęcenie użytkowników do usuwania złośliwych plików.
Modyfikacja pliku hosts	Plik hosts porównuje nazwy domen z adresami IP. Wiele złośliwych programów modyfikuje plik hostów, tak aby przeglądarka sieci Web była przekierowywana do zarażonych, nieistniejących lub fałszywych witryn sieci Web.
Podejrzane zachowanie	Podejrzane zachowanie to określone działanie lub seria działań, które nie są zwykle wykonywane przez legalne programy. Należy zachować ostrożność w przypadku programów, które cechuje podejrzane zachowanie.
Nowy dodatek do przeglądarki Internet Explorer	Programy spyware/grayware często instalują niechciane wtyczki przeglądarki Internet Explorer, włącznie z paskami narzędzi i obiektami pomocniczymi przeglądarki.
Modyfikacja ustawień przeglądarki Internet Explorer	Wiele wirusów/złośliwych programów zmienia ustawienia programu Internet Explorer, takie jak strona domowa, zaufane witryny sieci Web, ustawienia serwera proxy i rozszerzenia menu.
Modyfikacja reguł zabezpieczeń	Modyfikacje reguł zabezpieczeń systemu Windows mogą umożliwić uruchamianie niechcianych aplikacji oraz zmianę przez nie ustawień systemu.
Wstrzykiwanie biblioteki programu	Wiele złośliwych programów konfiguruje system Windows w taki sposób, aby wszystkie aplikacje automatycznie ładowały bibliotekę programu (DLL). Umożliwia to wykonanie złośliwych procedur w bibliotece DLL przy każdym uruchomieniu aplikacji.

Zdarzenia	Opis
Modyfikacja powłoki	Wiele złośliwych programów modyfikuje ustawienia powłoki systemu Windows, aby utworzyć powiązania z określonymi typami plików. W ten sposób złośliwe programy mogą być uruchamiane automatycznie, jeśli użytkownik otworzy powiązane pliki w Eksploratorze Windows. Zmiany w ustawieniach powłoki systemu Windows umożliwiają złośliwym programom także śledzenie używanych programów i uruchamianie się wraz z autentycznymi aplikacjami.
Nowa usługa	Usługi systemu Windows to procesy mające specjalne funkcje, które zwykle działają w tle, z pełnym dostępem administracyjnym. Złośliwe programy czasami instalują się jako usługi w celu pozostania w ukryciu.
Modyfikacja systemu plików	Niektóre pliki systemowe Windows określają zachowanie systemu, włącznie z programami startowymi i ustawieniami wygaszacza ekranu. Wiele złośliwych programów modyfikuje pliki systemowe w celu automatycznego uruchamiania podczas startu komputera i kontrolowania działania systemu.
Modyfikacja reguł zapory	Reguły zapory systemu Windows określają aplikacje mające dostęp do sieci, porty otwarte do komunikacji oraz adresy IP, które mogą komunikować się z komputerem. Wiele złośliwych programów modyfikuje reguły, aby zapewnić sobie dostęp do sieci i Internetu.
Modyfikacja procesów systemowych	Wiele złośliwych programów wykonuje różne działania na wbudowanych procesach systemu Windows. Te działania mogą obejmować przerywanie lub modyfikowanie aktywnych procesów.
Nowy program startowy	Złośliwe aplikacje zwykle dodają lub modyfikują wpisy automatycznego uruchamiania w rejestrze systemu Windows, aby uruchamiać się automatycznie przy każdym uruchomieniu komputera.

Kiedy funkcja monitorowania zdarzeń wykryje monitorowane zdarzenie systemowe, wykonuje operację skonfigurowaną dla tego zdarzenia.

W poniższej tabeli znajduje się lista operacji, jakie administrator może wykonać w związku z monitorowanymi zdarzeniami systemowymi.

TABELA 9-2. Operacje dla monitorowanych zdarzeń systemowych

AKCJA	OPIS
Oceń	Program OfficeScan zawsze zezwala na działanie procesów związanych ze zdarzeniem, ale rejestruje informacje o tym działaniu w dzienniku w celu przeprowadzenia późniejszej oceny. Jest to operacja domyślna dla wszystkich monitorowanych zdarzeń systemowych. **Uwaga** Ta opcja nie jest obsługiwana w przypadku iniekcji bibliotek programów w systemach 64-bitowych.
Zezwól	Program OfficeScan zawsze zezwala na działanie procesów związanych ze zdarzeniem.
Pytaj w razie konieczności	Program OfficeScan pyta użytkowników, czy działanie programów powiązanych ze zdarzeniem ma zostać umożliwione lub zablokowane, a także czy programy mają zostać dodane do listy wyjątków Jeśli użytkownik nie odpowie w określonym czasie, program OfficeScan automatycznie zezwoli na uruchomienie programu. Ustawienie domyślne to 30 sekund. Aby zmienić ten okres, należy zapoznać się z tematem *Konfigurowanie globalnych ustawień monitorowania zachowań na stronie 9-14*. **Uwaga** Ta opcja nie jest obsługiwana w przypadku iniekcji bibliotek programów w systemach 64-bitowych.

Akcja	Opis
Odrzuć	Program OfficeScan zawsze blokuje działanie programów związanych ze zdarzeniem i rejestruje informacje o tym działaniu w dziennikach. Jeśli program zostanie zablokowany, a powiadomienia są włączone, program OfficeScan wyświetli powiadomienie na komputerze z programem OfficeScan. Szczegółowe informacje na temat powiadomień zawiera sekcja *Powiadomienia monitorowania zachowań dla użytkowników agenta OfficeScan na stronie 9-17*.

Lista wyjątków monitorowania zachowań

Lista wyjątków monitorowania zachowań zawiera programy, które nie są monitorowane przez funkcję monitorowania zachowań.

- **Dozwolone programy**: Programy na tej liście mogą być uruchamiane. Dozwolony program zostanie jednak sprawdzony przez inne funkcje programu OfficeScan (takie jak skanowanie oparte na plikach), zanim zostanie dozwolone jego uruchomienie.
- **Zablokowane programy**: Programów znajdujących się na tej liście nigdy nie można uruchamiać. Aby skonfigurować tę listę, należy włączyć monitorowanie zdarzeń.

Listę wyjątków można skonfigurować w konsoli Web. Użytkownikom można także przyznać uprawnienia do konfigurowania własnej listy wyjątków w konsoli agenta OfficeScan. Szczegółowe informacje zawiera sekcja *Uprawnienia monitorowania zachowań na stronie 9-16*.

Konfigurowanie blokowania działania złośliwego oprogramowania, monitorowania zdarzeń i listy Wyjątek

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Ustawienia monitorowania zachowań**.
4. Kliknij kartę **Reguły**.
5. Aby włączyć blokowanie działania złośliwego oprogramowania:
   a. Wybierz opcję **Włącz blokowanie działania złośliwego oprogramowania** i określ typy zagrożeń do blokowania:
      - **Znane zagrożenia**: Blokuje zachowania powiązane ze znanymi zagrożeniami złośliwego oprogramowania.
      - **Znane i potencjalne zagrożenia:** Blokuje zachowanie powiązane ze znanymi zagrożeniami i wykonuje operację dla zachowania, które jest potencjalnie złośliwe.

   b. Wybierz, których mechanizmów funkcji ochrony przed oprogramowaniem typu ransomware potrzebujesz do ochrony przed zagrożeniami typu ransomware.
      - **Chroń dokumenty przed nieautoryzowanym szyfrowaniem lub modyfikacją**: Uniemożliwia programom typu ransomware szyfrowanie lub modyfikowanie zawartości dokumentów.
        - **Automatycznie twórz kopie zapasowe i przywracaj pliki zmienione przez podejrzane programy**: Tworzy kopie zapasowe plików szyfrowanych na punktach końcowych, aby zapobiec utracie danych w przypadku, gdy program OfficeScan wykryje zagrożenie typu ransomware.

Uwaga

Automatyczne tworzenie kopii zapasowych wymaga co najmniej 100 MB miejsca na dysku punktu końcowego agenta. Tworzona jest kopia zapasowa tylko tych plików, których rozmiar jest mniejszy niż 10 MB.

- **Blokuj procesy często powiązane z oprogramowaniem typu ransomware**: Blokuje procesy powiązane ze znanym oprogramowaniem typu ransomware, zanim dojdzie do zaszyfrowania lub zmodyfikowania dokumentów.
- **Włącz inspekcję programów, aby wykrywać i blokować zaatakowane pliki wykonywalne**: Inspekcja programów monitoruje procesy i przechwytuje interfejs API w celu określenia, czy program zachowuje się w nieoczekiwany sposób. Chociaż procedura ta zwiększa ogólny wskaźnik wykrywania zaatakowanych plików wykonywalnych, może ona obniżać wydajność systemu.

Porada

Inspekcja programów zapewnia wyższy poziom bezpieczeństwa w przypadku wyboru opcji **Znane i potencjalne zagrożenia** w menu rozwijanym **Blokowane zagrożenia**.

Szczegółowe informacje zawiera sekcja *Ochrona przed oprogramowaniem typu ransomware na stronie 9-3*.

c. W sekcji **Ochrona przed programami wykorzystującymi luki** włącz opcję **Przerywaj działanie programów z oznakami nieprawidłowego zachowania w wyniku ataku programów wykorzystujących luki**, aby zapewnić ochronę przed programami wykorzystującymi luki.

Uwaga

Ochrona przed programami wykorzystującymi luki wymaga wybrania opcji **Włącz inspekcję programów, aby wykrywać i blokować zaatakowane pliki wykonywalne**.

Szczegółowe informacje zawiera sekcja *Ochrona przed programami wykorzystującymi luki na stronie 9-5*.

6. W sekcji **Nowo napotkane programy** włącz opcję **Monitoruj nowe programy pobrane przez protokół HTTP lub aplikacje poczty elektronicznej** i wybierz, czy należy **monitować użytkownika** przed wykonaniem pobranego programu lub czy program OfficeScan ma tylko rejestrować wykrycie w dzienniku.

7. Skonfiguruj ustawienia monitorowania zachowań.

   a. Wybierz opcję **Włącz monitorowanie zdarzeń**.

   b. Wybierz zdarzenia systemowe do monitorowania oraz operację dla każdego wybranego zdarzenia.

      Informacje na temat monitorowanych zdarzeń systemowych i operacji zawiera temat *Monitorowanie zdarzeń na stronie 9-6*.

8. Kliknij kartę **Wyjątki**, aby skonfigurować listy wyjątków.

   a. W pozycji **Wpisz pełną ścieżkę do programu** wpisz pełną ścieżkę programu do zatwierdzenia lub zablokowania. Poszczególne wpisy należy oddzielać średnikami (;).

   b. Kliknij opcję **Dodaj do listy dozwolonych** lub **Dodaj do listy zablokowanych**.

   c. Aby usunąć zablokowany lub zatwierdzony program z listy, kliknij ikonę kosza () obok programu.

Uwaga

Program OfficeScan obsługuje maksymalnie 1024 pozycji dla zatwierdzonych programów i 1024 pozycji dla zablokowanych programów.

9. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.

- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Konfigurowanie globalnych ustawień monitorowania zachowań

Program OfficeScan stosuje ustawienia agenta globalnego do wszystkich agentów lub tylko do agentów o określonych uprawnieniach.

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Kliknij kartę **Ustawienia zabezpieczeń**.
3. Przejdź do sekcji **Ustawienia monitorowania zachowań**.
4. Skonfiguruj ustawienie **Automatycznie podejmij działanie, jeśli użytkownik nie odpowie w ciągu __ s** zgodnie z potrzebami.

   To ustawienie działa tylko w przypadku, gdy włączono monitorowano zdarzeń oraz wybrano operację „Pytaj w razie konieczności” dla monitorowanego zdarzenia systemowego. Ta operacja powoduje zapytanie użytkownika, czy działanie programów powiązanych ze zdarzeniem ma zostać umożliwione lub zablokowane. Jeśli użytkownik nie odpowie w określonym czasie, program OfficeScan automatycznie zezwoli na uruchomienie programu.

   Szczegółowe informacje zawiera sekcja *Monitorowanie zdarzeń na stronie 9-6*.
5. Kliknij kartę **System**.
6. Przejdź do sekcji **Ustawienia usługi Certified Safe Software Service** i włącz usługę Certified Safe Software Service zgodnie z potrzebami.

   Usługa Certified Safe Software przeszukuje centra danych firmy Trend Micro w celu weryfikacji bezpieczeństwa programu wykrytego przez blokowanie działania złośliwego oprogramowania, monitorowanie zdarzeń, zaporę lub skanowanie

oprogramowania antywirusowego. Należy włączyć włączyć usługę Certified Safe Software, aby zmniejszyć prawdopodobieństwo fałszywych alarmów.

Uwaga

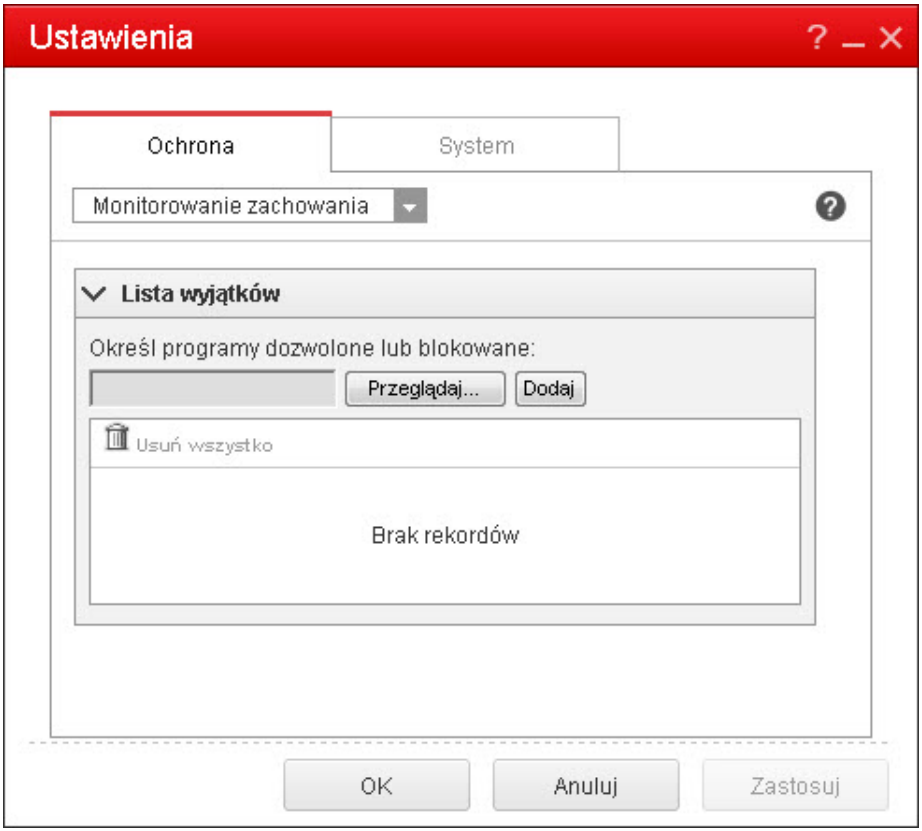
Przed włączeniem usługi Certified Safe Software Service należy się upewnić, że Agenci OfficeScan mają skonfigurowane prawidłowe ustawienia proxy (szczegółowe informacje zawiera sekcja *Ustawienia serwera proxy agenta OfficeScan na stronie 15-52*). Nieprawidłowe ustawienia serwera proxy lub wadliwe połączenie z Internetem mogą być przyczyną opóźnień lub niepowodzenia odbioru odpowiedzi z centrów danych firmy Trend Micro, przez co monitorowane programy będą sprawiać wrażenie zawieszonych.

Ponadto Agenci OfficeScan korzystający wyłącznie z protokołu IPv6 nie mogą bezpośrednio przeszukiwać centrów danych firmy Trend Micro. Aby umożliwić agentom OfficeScan nawiązanie połączenia z centrami danych firmy Trend Micro, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.

7. Kliknij przycisk **Zapisz**.

Uprawnienia monitorowania zachowań

Jeśli agenci mają przydzielone uprawnienia do monitorowania zachowań, na ekranie **Ustawienia** w konsoli agenta OfficeScan jest wyświetlana opcja Monitorowanie zachowań. Użytkownicy mogą zarządzać własną listą wyjątków.



ILUSTRACJA 9-1. Opcja Monitorowanie zachowań w konsoli agenta OfficeScan

Przyznawanie uprawnień monitorowania zachowań

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Na karcie **Uprawnienia** przejdź do sekcji **Uprawnienia monitorowania zachowań**.
5. Wybierz opcję **Wyświetl ustawienia Monitorowanie zachowań w konsoli agenta OfficeScan**.
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Powiadomienia monitorowania zachowań dla użytkowników agenta OfficeScan

Program OfficeScan może wyświetlić powiadomienie programu na komputerze agenta OfficeScan natychmiast po zablokowaniu programu przez usługę monitorowania zachowań. Należy włączyć opcję wysyłania powiadomień programu i w razie potrzeby zmodyfikować treść powiadomienia programu.

Włączanie wysyłania powiadomień programu

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Kliknij kartę **Inne ustawienia** i przejdź do sekcji **Ustawienia monitorowania zachowań**.
5. Wybierz opcję **Wyświetl powiadomienie, gdy program zostanie zablokowany**.
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszlych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Zmiana treści powiadomień programu

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Agent**.
2. Na liście rozwijanej **Typ** wybierz opcję **Naruszenia reguł monitorowania zachowań**.
3. Zmodyfikuj domyślne komunikaty w odpowiednim polu.

- Naruszenia reguł monitorowania zachowania: podaj komunikat, który otrzymują użytkownicy końcowi, gdy funkcja blokowania działania złośliwego oprogramowania wykryje naruszenie reguły.
- Nowo napotkane programy: podaj komunikat, który otrzymują użytkownicy końcowi, gdy funkcja blokowania działania wykryje nierozpoznany program pobrany przez kanały HTTP/HTTPS i aplikacje poczty elektronicznej.

4. Kliknij przycisk **Zapisz**.

Dzienniki monitorowania zachowań

Agenci OfficeScan rejestrują informacje o próbach uzyskania dostępu przez nieautoryzowane programy i przesyłają dzienniki na serwer. Agent OfficeScan, który jest stale uruchomiony, agreguje dzienniki i wysyła je na serwer w określonych odstępach czasu, wynoszących domyślnie 60 minut.

Aby dzienniki nie zajmowały zbyt dużo miejsca na dysku twardym, można je ręcznie usunąć lub skonfigurować harmonogram ich usuwania. Dodatkowe informacje dotyczące dzienników zarządzania zawiera sekcja *Zarządzanie dziennikiem na stronie 14-41*.

Wyświetlanie dzienników monitorowania zachowań

Procedura

1. Przejdź do opcji **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa** lub **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij kolejno opcje **Dzienniki** > **Dzienniki monitorowania zachowań** lub **Wyświetl dzienniki** > **Dzienniki monitorowania zachowań**.
4. Określ kryteria dziennika i kliknij przycisk **Wyświetl dzienniki**.

5. Wyświetl dzienniki. Dziennik zawiera następujące informacje:
   - data i godzina wykrycia nieautoryzowanego procesu;
   - punkt końcowy, na którym wykryto nieautoryzowany proces;
   - domena punktu końcowego;
   - Naruszenie, stanowiące zasadę monitorowania zdarzeń naruszoną przez proces
   - Operacja wykonana po wykryciu naruszenia
   - Zdarzenie stanowiące typ obiektu, do którego program uzyskał dostęp
   - poziom zagrożenia związany z nieautoryzowanym programem;
   - nazwa nieautoryzowanego programu;
   - Operacja, stanowiąca czynność wykonaną przez nieautoryzowany program
   - element docelowy, czyli proces, do którego uzyskano dostęp;
   - kanał zarażenia, z którego pochodzi zagrożenie.
6. Aby zapisać dzienniki w formacie `CSV` (plik z tekstem oddzielanym przecinkami), kliknij opcję **Eksportuj do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Konfigurowanie harmonogramu wysyłania dziennika monitorowania zachowań

Procedura

1. Uzyskaj dostęp do lokalizacji <*Folder instalacji serwera*>`\PCCSRV`.
2. Otwórz plik `ofcscan.ini` w edytorze tekstu, na przykład w Notatniku.
3. Wyszukaj ciąg „`SendBMLogPeriod`” i sprawdź wartość znajdującą się obok niego.

   Domyślna wartość to 3600 sekund. Tekst wygląda wtedy następująco: „`SendBMLogPeriod=3600`”.

4. Określ wartość w sekundach.

   Aby na przykład zmienić przedział czasu na 2 godziny, należy wpisać wartość 7200.

5. Zapisz plik.

6. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.

7. Kliknij polecenie **Zapisz**, pozostawiając wszystkie ustawienia bez zmian.

8. Uruchom ponownie agenta.

Rozdział 10

Korzystanie z funkcji kontroli urządzeń

W tym rozdziale przedstawiono sposób ochrony komputerów przed zagrożeniami bezpieczeństwa przy użyciu funkcji kontroli urządzeń.

Rozdział składa się z następujących tematów:

Kontrola urządzeń

Kontrola urządzeń zapewnia dostęp do zewnętrznych urządzeń pamięci masowej oraz do zasobów sieciowych połączonych z komputerami. Funkcja kontroli urządzeń ułatwia zapobieganie utracie i wyciekowi danych oraz, w połączeniu z funkcją skanowania plików, wzmacnia ochronę przed zagrożeniami bezpieczeństwa.

Reguły kontroli urządzeń można skonfigurować dla agentów wewnętrznych i zewnętrznych. Administratorzy programu OfficeScan z reguły wprowadzają ściślejsze reguły dla agentów zewnętrznych.

Reguły to szczegółowe ustawienia w drzewie agentów OfficeScan. Określone reguły można zastosować do grup agentów lub poszczególnych agentów. Można także zastosować jedną regułę do wszystkich agentów.

Po wdrożeniu reguł agenci używają kryteriów lokalizacji, które zostały ustawione na ekranie **Lokalizacja punktu końcowego** (patrz *Lokalizacja punktu końcowego na stronie 15-2*), aby określić swoją lokalizację i reguły do zastosowania. Każda zmiana lokalizacji agentów oznacza przełączenie reguł.

Ważne

- Kontrola urządzeń jest domyślnie wyłączona we wszystkich wersjach systemów Windows Server 2003, Windows Server 2008, Windows Server 2012 i Windows Server 2016. Przed włączeniem kontroli urządzeń na tych platformach serwerowych należy zapoznać się z wytycznymi i sprawdzonymi sposobami przedstawionymi w rozdziale *Usługi agenta OfficeScan na stronie 15-7*.
- Listę obsługiwanych modeli urządzeń zawiera dokument *Listy modułu Ochrona danych* pod adresem:

  http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Typy urządzeń, które mogą być monitorowane przez program OfficeScan, są zależne od tego, czy aktywowano licencję Ochrona danych. Ochrona danych to moduł licencjonowany oddzielnie, który musi zostać aktywowany, zanim będzie możliwe jego użycie. Szczegółowe informacje o licencji Ochrona danych zawiera temat *Licencja Ochrona danych na stronie 3-4*.

TABELA 10-1. Urządzenia monitorowane przez usługę zapobiegania nieautoryzowanym zmianom

TYP URZĄDZENIA	OPIS URZĄDZENIA
Urządzenia pamięci masowej	CD/DVD **Ważne** Funkcja Kontrola urządzeń może ograniczyć dostęp tylko do tych urządzeń nagrywających CD/DVD, które korzystają z formatu Aktywny system plików. Niektóre aplikacje innych firm, korzystające z formatu głównego, mogą wykonywać operacje odczytu/zapisu nawet wówczas, gdy funkcja Kontrola urządzeń jest włączona. Aby ograniczyć dostęp do urządzeń nagrywających CD/DVD korzystających z formatu dowolnego typu, należy użyć funkcji Zapobieganie utracie danych. Szczegółowe informacje zawiera sekcja *Blokowanie dostępu do rejestratorów danych (CD/DVD) na stronie 11-36*.
	Dyskietki
	Dyski sieciowe
	Urządzenia pamięci masowej USB

TABELA 10-2. Urządzenia monitorowane przez usługę Zapobieganie utracie danych

TYP URZĄDZENIA	OPIS URZĄDZENIA
Urządzenia mobilne	Urządzenia mobilne
Urządzenia pamięci masowej	CD/DVD
	Dyskietki
	Dyski sieciowe
	Urządzenia pamięci masowej USB

Typ urządzenia	Opis urządzenia
Urządzenia inne niż pamięci masowe	Adaptery Bluetooth
	Porty COM i LPT
	Interfejs IEEE 1394
	Urządzenia do przetwarzania obrazu
	Urządzenia na podczerwień
	Modemy
	Karty PCMCIA
	Klawisz Print Screen
	Karty sieci bezprzewodowej

Uprawnienia urządzeń pamięci masowej

Uprawnienia kontroli urządzeń pamięci masowej są używane w następujących przypadkach:

- Podczas przyznawania dostępu do urządzeń pamięci masowej USB, napędów CD/DVD, napędów dyskietek i dysków sieciowych. Dla tych urządzeń można przyznać pełny dostęp lub ograniczyć poziom dostępu.
- Skonfiguruj listę zatwierdzonych urządzeń pamięci masowej USB. Kontrola urządzeń umożliwia blokowanie dostępu do wszystkich urządzeń pamięci masowej USB z wyjątkiem tych, które dodano do listy urządzeń zatwierdzonych. Dla tych urządzeń można przyznać pełny dostęp lub ograniczyć poziom dostępu.

W poniższej tabeli znajduje się lista uprawnień dla urządzeń pamięci masowej.

TABELA 10-3. Uprawnienia kontroli urządzeń dla urządzeń pamięci masowej

UPRAWNIENIA	PLIKI NA URZĄDZENIU	PLIKI PRZYCHODZĄCE
Pełny dostęp	Dozwolone operacje: kopiowanie, przenoszenie, otwieranie, zapisywanie, usuwanie, wykonywanie	Dozwolone operacje: zapisywanie, przenoszenie, kopiowanie Oznacza to, że plik można zapisywać, przenosić oraz kopiować na urządzenie.
Modyfikuj	Dozwolone operacje: kopiowanie, przenoszenie, otwieranie, zapisywanie, usuwanie Niedozwolone operacje: wykonywanie	Dozwolone operacje: zapisywanie, przenoszenie, kopiowanie
Odczyt i wykonywanie	Dozwolone operacje: kopiowanie, otwieranie, wykonywanie Niedozwolone operacje: zapisywanie, przenoszenie, usuwanie	Niedozwolone operacje: zapisywanie, przenoszenie, kopiowanie
Odczyt	Dozwolone operacje: kopiowanie, otwieranie Niedozwolone operacje: zapisywanie, przenoszenie, usuwanie, wykonywanie	Niedozwolone operacje: zapisywanie, przenoszenie, kopiowanie
Wyświetl wyłącznie zawartość urządzenia	Niedozwolone operacje: wszystkie Urządzenie oraz zapisane na nim pliki są widoczne dla użytkownika (np. z programu Windows Explorer).	Niedozwolone operacje: zapisywanie, przenoszenie, kopiowanie

UPRAWNIENIA	PLIKI NA URZĄDZENIU	PLIKI PRZYCHODZĄCE
Blokuj (dostępne po zainstalowaniu Ochrona danych)	Niedozwolone operacje: wszystkie Urządzenie oraz zapisane na nim pliki nie są widoczne dla użytkownika (np. z programu Windows Explorer).	Niedozwolone operacje: zapisywanie, przenoszenie, kopiowanie

Funkcja skanowania plików w programie OfficeScan uzupełnia uprawnienia urządzenia i może je zastępować. Jeśli na przykład uprawnienie zezwala na otwieranie pliku, ale program OfficeScan wykryje, że plik jest zarażony przez złośliwe oprogramowanie, zostanie wykonana określona operacja skanowania w celu usunięcia złośliwego kodu. Jeśli operacja skanowania to Wyczyść, plik jest otwierany po jego wyczyszczeniu. Jednak jeśli operacja skanowania to Usuń, plik jest usuwany.

Porada

Kontrola urządzeń dla Ochrona danych jest zgodna wyłącznie z platformami 64-bitowymi. Aby włączyć monitorowanie zapobiegania nieautoryzowanym zmianom w systemach, które nie są zgodne z programem OfficeScan, należy ustawić uprawnienie urządzenia na **Blokuj** w celu ograniczenia dostępu do tego urządzenia.

Uprawnienia zaawansowane dla urządzeń pamięci masowej

Uprawnienia zaawansowane są stosowane w przypadku zapewniania ograniczonych uprawnień do większości urządzeń pamięci masowej. Mogą to być:

- **Modyfikuj**
- **Odczyt i wykonywanie**
- **Odczyt**
- **Wyświetl wyłącznie zawartość urządzenia**

Można zachować uprawnienia ograniczone, ale przyznać uprawnienia zaawansowane do niektórych programów na urządzeniach pamięci masowej i na lokalnym punkcie końcowym.

Aby zdefiniować programy, należy skonfigurować poniższe listy programów.

TABELA 10-4. Listy programów

LISTA PROGRAMÓW	OPIS	NIEPRAWIDŁOWE DANE
Programy z uprawnieniem odczytu z urządzeń i zapisu na urządzeniach	Ta lista zawiera programy lokalne i programy na urządzeniach pamięci masowej, które dysponują uprawnieniami do odczytu i zapisu na tych urządzeniach. Przykładem takiego programu jest program Microsoft Word (`winword.exe`), który zwykle znajduje się w folderze `C:\Program Files\Microsoft Office\Office`. Jeśli uprawnienie dla urządzeń pamięci masowej USB to „Wyświetl wyłącznie zawartość urządzenia”, ale program „`c:\Program Files\Microsoft Office\Office\winword.exe`” znajduje się na liście: • Użytkownik będzie dysponował dostępem do odczytu i zapisu na dowolnym pliku zapisanym na urządzeniu pamięci masowej USB, który jest dostępny z poziomu programu Microsoft Word. • Użytkownik może zapisać, przenieść lub skopiować plik programu Microsoft Word do urządzenia pamięci masowej USB.	ścieżka programu i nazwa Szczegółowe informacje zawiera sekcja *Określanie ścieżki programu i nazwy na stronie 10-9*.

Lista programów	Opis	Nieprawidłowe dane
Programy na urządzeniach, które można wykonywać	Ta lista zawiera programy na urządzeniach pamięci masowej, które mogą być wykonywane przez użytkowników lub system. Aby na przykład zezwolić użytkownikom na instalowanie oprogramowania z dysku CD, do listy należy dodać ścieżkę instalacyjną programu i nazwę, np. „`E:\Installer\Setup.exe`”.	Ścieżka do programu i nazwa pliku lub dostawca podpisu cyfrowego Szczegółowe informacje zawiera sekcja *Określanie ścieżki programu i nazwy na stronie 10-9* lub *Określanie dostawcy podpisu cyfrowego na stronie 10-9*.

Występują sytuacje, gdy program należy dodać do obydwu list. Przykładowo: funkcja zabezpieczenia danych w urządzeniach pamięci masowej USB, która po włączeniu, wyświetla monity o wprowadzenie prawidłowej nazwy użytkownika i hasła, co pozwala na odblokowanie urządzenia. Funkcja blokady danych korzysta z programu „`Password.exe`”, który musi mieć zgodę na uruchomienie, aby umożliwić użytkownikom odblokowanie urządzenia. Program „`Password.exe`” musi również mieć możliwość odczytu i zapisu danych w urządzeniu, aby użytkownicy mogli zmienić nazwę użytkownika i hasło.

Każda lista programów w interfejsie użytkownika może zawierać do 100 programów.

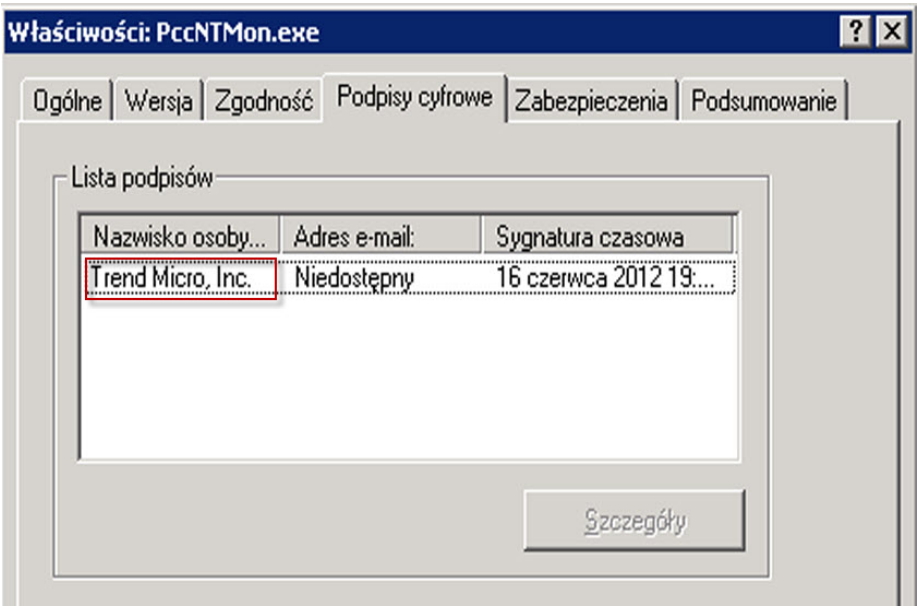
Aby dodać więcej programów do listy, należy dodać je do pliku `ofcscan.ini`, w którym można zapisać do 1000 programów. Instrukcje dotyczące dodawania programów do pliku `ofcscan.ini` przedstawiono w sekcji *Dodawanie programów do listy Kontrola urządzeń przy użyciu pliku ofcscan.ini na stronie 10-17*.

OSTRZEŻENIE!

Programy dodane do pliku `ofcscan.ini` zostaną wprowadzone do domeny głównej i zastąpią programy w poszczególnych domenach i na agentach.

Określanie dostawcy podpisu cyfrowego

Jeśli użytkownik ufa programom wydanym przez dostawcę, należy określić dostawcę podpisu cyfrowego. Należy na przykład wpisać Microsoft Corporation lub Trend Micro Inc. Dostawcę podpisu cyfrowego można poznać przez sprawdzenie właściwości programu (na przykład klikając prawym przyciskiem myszy program i wybierając pozycję **Właściwości**).



ILUSTRACJA 10-1. Dostawca podpisu cyfrowego programu agenta OfficeScan (`PccNTMon.exe`)

Określanie ścieżki programu i nazwy

Ścieżka programu i nazwa powinny się składać z maksymalnie 259 znaków i zawierać tylko znaki alfanumeryczne (A-Z, a-z, 0-9). Nie ma możliwości określenia tylko nazwy programu.

W miejscach liter dysków i nazw programów można używać symboli wieloznacznych. Znak zapytania (?) może być użyty do przedstawienia danych jednoznakowych, takich

jak litery dysku. Znak gwiazdki (*) może być użyty do przedstawienia danych wieloznakowych, takich jak nazwy programów.

Uwaga

Symboli wieloznacznych nie można używać do reprezentowania nazw folderów. Należy wprowadzić dokładną nazwę folderu.

Prawidłowe użycie symboli wieloznacznych:

TABELA 10-5. Prawidłowe użycie symboli wieloznacznych

PRZYKŁAD	ODPOWIADAJĄCE DANE
?:\Password.exe	Plik „Password.exe” zapisany w katalogu głównym dowolnego dysku
C:\Program Files\Microsoft *.exe	Dowolny plik w folderze C:\Program Files mający rozszerzenie
C:\Program Files*.*	Dowolny plik w folderze C:\Program Files mający rozszerzenie
C:\Program Files\a**?**c.exe	Dowolny plik .exe w folderze C:\Program Files składający się z 3 znaków, którego pierwsza litera to „a”, a ostatnia to „c”
C:*	Dowolny plik zapisany w katalogu głównym dysku C:, z rozszerzeniem lub bez

Nieprawidłowe użycie symboli wieloznacznych:

TABELA 10-6. Nieprawidłowe użycie symboli wieloznacznych

PRZYKŁAD	PRZYCZYNA
??:\Buffalo\Password.exe	?? oznacza dwa znaki, a nazwa dysku składa się tylko z jednej litery.
***:\Buffalo\Password.exe	* oznacza dane wieloznakowe, a nazwa dysku składa się tylko z jednej litery.

Przykład	Przyczyna
C:*\Password.exe	Symboli wieloznacznych nie można używać do reprezentowania nazw folderów. Należy wprowadzić dokładną nazwę folderu.
C:\?\Password.exe	

Uprawnienia urządzeń innych niż pamięci masowe

Dostęp do urządzeń innych niż pamięci masowe można zablokować lub zezwolić na niego. Nie istnieją żadne zaawansowane ani dokładne uprawnienia dla tych urządzeń.

Zarządzanie dostępem do urządzeń zewnętrznych (Ochrona danych aktywowana)

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Ustawienia kontroli urządzeń**.
4. Kliknij kartę **Agenci zewnętrzni**, aby skonfigurować ustawienia dla agentów zewnętrznych, lub kartę **Agenci wewnętrzni**, aby skonfigurować ustawienia dla agentów wewnętrznych.
5. Wybierz opcję **Włącz kontrolę urządzeń**.
6. Zastosuj ustawienia w następujący sposób:
   - Jeśli wyświetlana jest karta **Agenci zewnętrzni**, można zastosować ustawienia do agentów wewnętrznych, wybierając opcję **Zastosuj ustawienia do agentów wewnętrznych**.

- Jeśli wyświetlana jest karta **Agenci wewnętrzni**, można zastosować ustawienia do agentów zewnętrznych, wybierając opcję **Zastosuj ustawienia do agentów zewnętrznych**.

Zostanie wyświetlona prośba o potwierdzenie. Odczekaj chwilę, aby nastąpiła propagacja polecenia instalacji do wszystkich agentów.

7. Zdecyduj, czy chcesz zablokować funkcję AutoRun (`autorun.inf`) w urządzeniach pamięci masowej USB.

8. Skonfiguruj ustawienia urządzeń pamięci masowej.

   a. Wybierz uprawnienia każdego urządzenia pamięci masowej.

      Szczegółowe informacje o uprawnieniach zawiera sekcja *Uprawnienia urządzeń pamięci masowej na stronie 10-4*.

   b. Jeżeli uprawnienie dla urządzeń pamięci masowej USB to **Blokuj**, należy skonfigurować listę zatwierdzonych urządzeń. Dzięki uprawnieniom użytkownicy mogą uzyskać dostęp do tych urządzeń i sterować poziomem dostępu.

      Patrz sekcja *Konfigurowanie listy dozwolonych urządzeń USB na stronie 10-14*.

9. W przypadku wszystkich urządzeń innych niż urządzenia pamięci masowej wybierz opcję **Zezwól** lub **Zablokuj**.

10. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

    - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.

    - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Konfigurowanie uprawnień zaawansowanych

Zaawansowane uprawnienia i powiadomienia dla określonego urządzenia pamięci masowej można skonfigurować w interfejsie użytkownika, jednak uprawnienia i powiadomienia są w rzeczywistości stosowane do wszystkich urządzeń pamięci masowej. Oznacza to, że po kliknięciu pozycji **Zaawansowane uprawnienia i powiadomienia** dla napędów CD/DVD, w rzeczywistości określane są uprawnienia i powiadomienia dla wszystkich urządzeń pamięci masowej.

Uwaga

Szczegółowe informacje o zaawansowanych uprawnieniach i prawidłowym definiowaniu programów za pomocą uprawnień zaawansowanych zawarto w temacie *Uprawnienia zaawansowane dla urządzeń pamięci masowej na stronie 10-6*.

Procedura

1. Kliknij pozycję **Zaawansowane uprawnienia i powiadomienia**.

   Zostanie wyświetlony nowy ekran.

2. Poniżej pozycji **Programy z uprawnieniem odczytu z urządzeń pamięci masowej i zapisu na tych urządzeniach** wpisz ścieżkę do programu i nazwę pliku, a następnie kliknij przycisk **Dodaj**.

   Dostawca podpisu cyfrowego nie został zaakceptowany

3. Poniżej pozycji **Programy na urządzeniach pamięci masowej, które można wykonywać** wpisz ścieżkę do programu i nazwę dostawcy podpisu cyfrowego, a następnie kliknij przycisk **Dodaj**.

4. Wybierz opcję **Wyświetlaj powiadomienie na punkcie końcowym, gdy program OfficeScan wykryje nieupoważniony dostęp do urządzenia**.

   - Nieupoważniony dostęp do urządzenia oznacza zabronione operacje na urządzeniu. Przykładowo jeśli uprawnieniem dla urządzenia jest „Odczyt”, użytkownicy nie będą mogli zapisywać, przenosić, usuwać ani wykonać plików na tym urządzeniu.

   - Powiadomienie programu można zmodyfikować. Szczegółowe informacje zawiera sekcja *Modyfikowanie powiadomień kontroli urządzeń na stronie 10-19*.

5. Kliknij przycisk **Wstecz**.

Konfigurowanie listy dozwolonych urządzeń USB

Lista dozwolonych urządzeń USB pozwala na używanie gwiazdki (*) jako symbolu wieloznacznego. W celu włączenia wszystkich urządzeń, które spełniają pozostałe pola, zastąp wszystkie pola z gwiazdką (*). Na przykład ciąg [producent]-[model]-* dopuszcza wszystkie urządzenia określonego producenta i typu modelu niezależnie od numeru seryjnego

Procedura

1. Kliknij pozycję **Dozwolone urządzenia**.
2. Wpisz producenta urządzenia.
3. Wpisz model urządzenia i numer seryjny.

   Porada

   Użyj narzędzia Lista urządzeń w celu wyszukania urządzeń podłączonych do punktów końcowych. Narzędzie dostarcza informacje o producencie, modelu i numerze seryjnym każdego urządzenia.

4. Wybierz uprawnienie dla urządzenia.

   Szczegółowe informacje o uprawnieniach zawiera sekcja *Uprawnienia urządzeń pamięci masowej na stronie 10-4*.

5. Aby dodać więcej urządzeń, kliknij ikonę plus (+).
6. Kliknij przycisk **< Wstecz**.

Narzędzie Lista urządzeń

Narzędzie Lista urządzeń można uruchomić lokalnie na każdym punkcie końcowym w celu wyszukania urządzeń zewnętrznych podłączonych do punktu końcowego.

Narzędzie skanuje punkt końcowy w poszukiwaniu urządzeń zewnętrznych, a następnie wyświetla informacje o urządzeniach w oknie przeglądarki. Informacji tych można użyć podczas konfigurowania ustawień urządzeń dla funkcji Zapobieganie utracie danych i kontroli urządzeń.

Uruchamianie narzędzia Lista urządzeń

Procedura

1. Na serwerze OfficeScan przejdź do folderu <*Folder instalacji serwera na stronie xviii*> `\PCCSRV\Admin\Utility\ListDeviceInfo`.
2. Skopiuj plik `listDeviceInfo.exe` na docelowy punkt końcowy.
3. Na punkcie końcowym uruchom plik `listDeviceInfo.exe`.
4. Przejrzyj informacje o urządzeniach w wyświetlonym oknie przeglądarki. Funkcje Zapobieganie utracie danych oraz kontroli urządzeń używają następujących informacji:
   - Producent (wymagane)
   - Model (opcjonalnie)
   - Numer seryjny (opcjonalnie)

Zarządzanie dostępem do urządzeń zewnętrznych (Ochrona danych nieaktywna)

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.

3. Kliknij polecenie **Ustawienia** > **Ustawienia kontroli urządzeń**.

4. Kliknij kartę **Agenci zewnętrzni**, aby skonfigurować ustawienia dla agentów zewnętrznych, lub kartę **Agenci wewnętrzni**, aby skonfigurować ustawienia dla agentów wewnętrznych.

5. Wybierz opcję **Włącz kontrolę urządzeń**.

6. Zastosuj ustawienia w następujący sposób:

   - Jeśli wyświetlana jest karta **Agenci zewnętrzni**, można zastosować ustawienia do agentów wewnętrznych, wybierając opcję **Zastosuj ustawienia do agentów wewnętrznych**.

   - Jeśli wyświetlana jest karta **Agenci wewnętrzni**, można zastosować ustawienia do agentów zewnętrznych, wybierając opcję **Zastosuj ustawienia do agentów zewnętrznych**.

   Zostanie wyświetlona prośba o potwierdzenie. Odczekaj chwilę, aby nastąpiła propagacja polecenia instalacji do wszystkich agentów.

7. Zdecyduj, czy chcesz zablokować funkcję AutoRun (`autorun.inf`) w urządzeniach pamięci masowej USB.

8. Wybierz uprawnienia każdego urządzenia pamięci masowej.

9. Skonfiguruj zaawansowane uprawnienia i powiadomienia, jeśli uprawnieniem dla urządzenia pamięci masowej jest jedno z poniższych: **Modyfikuj**, **Odczyt i wykonywanie**, **Odczyt** lub **Wyświetl wyłącznie zawartość urządzenia**.

   Patrz sekcja *Konfigurowanie uprawnień zaawansowanych na stronie 10-13*.

10. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

    - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.

- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Dodawanie programów do listy Kontrola urządzeń przy użyciu pliku ofcscan.ini

Uwaga

Szczegółowe informacje o listach programów i prawidłowym definiowaniu programów, które można dodać do list, zawarto w temacie *Uprawnienia zaawansowane dla urządzeń pamięci masowej na stronie 10-6*.

Procedura

1. Na komputerze serwera OfficeScan przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV`.
2. Za pomocą edytora tekstu otwórz plik `ofcscan.ini`.
3. Aby dodać programy z uprawnieniem do odczytu z urządzeń pamięci masowej i zapisu na tych urządzeniach:
   a. Znajdź następujące wiersze:

      ```
      [DAC_APPROVED_LIST]

      Count=x
      ```

   b. Zastąp znak „x” liczbą programów na liście programów.
   c. Poniżej ciągu „Count=x” dodaj programy, wpisując:

      ```
      Item<numer>=<ścieżka do programu i nazwa lub dostawca
      podpisu cyfrowego>
      ```

      Na przykład:

      ```
      [DAC_APPROVED_LIST]
      ```

```
Count=3

Item0=C:\Program Files\program.exe

Item1=?:\password.exe

Item2=Microsoft Corporation
```

4. Aby dodać programy na urządzeniach pamięci masowej, które można wykonywać:

   a. Znajdź następujące wiersze:

   ```
   [DAC_EXECUTABLE_LIST]

   Count=x
   ```

   b. Zastąp znak „x" liczbą programów na liście programów.

   c. Poniżej ciągu „Count=x" dodaj programy, wpisując:

   ```
   Item<numer>=<ścieżka do programu i nazwa lub dostawca
   podpisu cyfrowego>
   ```

   Na przykład:

   ```
   [DAC_EXECUTABLE_LIST]

   Count=3

   Item0=?:\Installer\Setup.exe

   Item1=E:\*.exe

   Item2=Trend Micro, Inc.
   ```

5. Zapisz i zamknij plik `ofcscan.ini`.

6. Otwórz konsolę Web programu OfficeScan i przejdź do ekranu **Agenci** > **Ustawienia agenta globalnego**.

7. Kliknij polecenie **Zapisz**, aby zastosować listy programów na wszystkich agenci.

Modyfikowanie powiadomień kontroli urządzeń

Gdy następuje naruszenie kontroli dostępu do urządzeń, na punktach końcowych są wyświetlane powiadomienia programu. W razie potrzeby domyślna treść powiadomienia programu może zostać zmodyfikowana przez administratora.

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Agent**.
2. Na liście rozwijanej **Typ** wybierz opcję **Naruszenie kontroli urządzeń**.
3. Zmodyfikuj domyślny komunikat w odpowiednim polu.
4. Kliknij przycisk **Zapisz**.

Dzienniki kontroli urządzeń

Agenci OfficeScan rejestrują informacje o próbach uzyskania nieautoryzowanego dostępu do urządzeń i przesyłają dzienniki na serwer. Stale uruchomiony agent agreguje dzienniki i przesyła je na serwer w 1-godzinnych odstępach czasu. Agent, który został ponownie uruchomiony, sprawdza ostatnią godzinę przesłania dziennika na serwer. Jeśli minęła więcej niż 1 godzina, agent natychmiast wysyła dziennik.

Aby dzienniki nie zajmowały zbyt dużo miejsca na dysku twardym, można je ręcznie usunąć lub skonfigurować harmonogram ich usuwania. Dodatkowe informacje dotyczące dzienników zarządzania zawiera sekcja *Zarządzanie dziennikiem na stronie 14-41*.

Wyświetlanie dzienników kontroli urządzeń

Uwaga

Tylko próby dostępu do **urządzeń pamięci masowej** powodują wygenerowanie danych dziennika. Agenci OfficeScan blokują lub zezwalają na dostęp do **urządzeń innych niż pamięci masowe** zgodnie z konfiguracją, ale nie rejestrują operacji.

Procedura

1. Przejdź do opcji **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa** lub **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij kolejno opcje **Dzienniki** > **Dzienniki kontroli urządzeń** lub **Wyświetl dzienniki** > **Dzienniki kontroli urządzeń**.
4. Określ kryteria dziennika i kliknij przycisk **Wyświetl dzienniki**.
5. Wyświetl dzienniki. Dziennik zawiera następujące informacje:
   - data i godzina wykrycia nieautoryzowanego dostępu;
   - informacja o punkcie końcowym, do którego jest podłączone zewnętrzne urządzenie lub do którego jest podłączony zasób sieciowy;
   - informacja o domenie punktu końcowego, do którego jest podłączone zewnętrzne urządzenie lub do którego jest podłączony zasób sieciowy;
   - typ urządzenia lub zasobu sieciowego, do którego uzyskano dostęp;
   - element docelowy, czyli obiekt na urządzeniu lub w zasobie sieciowym, do którego uzyskano dostęp;
   - element źródłowy, czyli obiekt, z którego zainicjowano próbę uzyskania dostępu;
   - uprawnienia przypisane do elementu docelowego.
6. Aby zapisać dzienniki w formacie `CSV` (plik z tekstem oddzielanym przecinkami), kliknij opcję **Eksportuj do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Rozdział 11

Używanie funkcji Zapobieganie utracie danych

W tym rozdziale przedstawiono sposób użycia funkcji Zapobieganie utracie danych.

Rozdział składa się z następujących tematów:

Zapobieganie utracie danych (DLP) — informacje

Tradycyjne rozwiązania zabezpieczeń skupiają się na zapobieganiu zewnętrznym zagrożeniom bezpieczeństwa, aby nie miały one dostępu do sieci. W obecnym środowisku bezpieczeństwa jest to jednak tylko jedna strona medalu. Coraz częściej zdarzają się naruszenia bezpieczeństwa danych, powodując ujawnienie poufnych i ważnych danych — nazywanych zasobami cyfrowymi — dla nieautoryzowanych osób z zewnątrz. Naruszenie bezpieczeństwa danych może wystąpić w wyniku pomyłki lub beztroski pracowników wewnętrznych, outsourcingu danych, kradzieży lub zgubienia urządzeń komputerowych bądź złośliwych ataków.

Naruszenia bezpieczeństwa danych mogą:

- Spowodować podkopanie wizerunku marki
- Zmniejszyć zaufanie klientów do organizacji
- Spowodować niepotrzebne koszty związane z naprawą sytuacjami i grzywnami za naruszenie przepisów dotyczących zgodności
- Doprowadzić do utraty możliwości biznesowych i przychodów w wyniku kradzieży własności intelektualnej

Biorąc pod uwagę rosnącą popularność i groźne skutki naruszeń bezpieczeństwa danych, organizacje postrzegają obecnie ochronę zasobów cyfrowych jako ważny składnik infrastruktury zabezpieczeń.

Zabezpieczenia Zapobieganie utracie danych chronią zasoby cyfrowe organizacji przed przypadkowymi lub celowymi wyciekami. Funkcja Zapobieganie utracie danych umożliwia:

- Identyfikację informacji poufnych wymagających ochrony przy użyciu identyfikatorów danych.
- Tworzenie reguł ograniczających lub uniemożliwiających przesyłanie zasobów cyfrowych przez typowe kanały transmisji, takie jak poczta e-mail i urządzenia zewnętrzne.
- Zapewnianie zgodności z określonymi standardami ochrony prywatności.

Przed rozpoczęciem monitorowania informacji poufnych pod kątem potencjalnych strat należy poznać odpowiedzi na następujące pytania:

- Jakie dane wymagają ochrony przed nieautoryzowanym dostępem?
- Gdzie znajdują się dane wrażliwe?
- W jaki sposób są przekazywane dane wrażliwe?
- Którzy użytkownicy są uprawnieni do dostępu do danych wrażliwych i przekazywania ich?
- Jakie działania należy podjąć w przypadku naruszenia bezpieczeństwa?

Ten istotny audyt zwykle obejmuje wiele działów i pracowników zaznajomionych z firmowymi informacjami poufnymi.

Jeśli już zdefiniowano informacje poufne i zasady bezpieczeństwa, można przystąpić do określania identyfikatorów danych i zasad firmy.

Reguły Zapobieganie utracie danych

Program OfficeScan ocenia plik lub dane przy użyciu zestawu reguł zdefiniowanych w regułach DLP. Reguły określają pliki lub dane, które wymagają ochrony przed nieautoryzowanym przesyłaniem i działania podejmowane przez program OfficeScan po wykryciu ich przesyłania.

Uwaga

Program OfficeScan nie monitoruje transmisji danych między serwerem a agentami OfficeScan.

Program OfficeScan umożliwia administratorom skonfigurowanie reguł dla wewnętrznych i zewnętrznych agentów OfficeScan. Administratorzy z reguły konfigurują ściślejsze reguły dla agentów zewnętrznych.

Administratorzy mogą egzekwować określone reguły w celu zastosowania do grup agentów lub poszczególnych agentów.

Po wdrożeniu reguł agenci używają kryteriów lokalizacji, które zostały ustawione na ekranie **Lokalizacja punktu końcowego** (patrz *Lokalizacja punktu końcowego na stronie 15-2*), aby ustalić właściwe ustawienia lokalizacji i reguły do zastosowania. Agenci zmieniają reguły przy każdej zmianie lokalizacji.

Konfiguracja reguł

Reguły DLP są definiowane poprzez skonfigurowanie następujących ustawień i wdrożenie tych ustawień na wybranych agentach:

TABELA 11-1. Ustawienia definiujące regułę DLP

USTAWIENIA	OPIS
Zasady	Reguła DLP może zawierać wiele szablonów, kanałów i operacji. Każda reguła stanowi podzbiór nadrzędnej reguły DLP. **Uwaga** Funkcja Zapobieganie utracie danych przetwarza reguły i szablony według priorytetu. Jeśli reguła jest ustawiona na operację “Pomiń”, funkcja Zapobieganie utracie danych przetwarza następną regułę na liście. Jeśli reguła jest ustawiona na operację “Blokuj” lub “Usprawiedliwienie użytkownika”, funkcja Zapobieganie utracie danych blokuje lub akceptuje działanie użytkownika i nie przetwarza dalej danej reguły/szablonu.

Ustawienia	Opis
Szablony	Szablon DLP łączy identyfikatory danych oraz operatory logiczne (I, Lub, Oprócz) w celu utworzenia instrukcji warunku. Regule DLP podlegają tylko pliki lub dane, które spełniają określoną instrukcję warunku. Funkcja Zapobieganie utracie danych zawiera zestaw wstępnie zdefiniowanych szablonów i umożliwia administratorom tworzenie szablonów niestandardowych. Reguła DLP może zawierać jeden lub więcej szablonów. Podczas sprawdzania szablonów funkcja Zapobieganie utracie danych używa reguły „pierwsze dopasowanie”. Oznacza to, że jeśli plik lub dane pasują do identyfikatorów danych w szablonie, funkcja Zapobieganie utracie danych nie będzie już sprawdzać innych szablonów.
Kanały	Kanały są obiektami przesyłającymi informacje poufne. Funkcja Zapobieganie utracie danych obsługuje popularne kanały transmisji, takie jak poczta e-mail, wymienne urządzenia pamięci masowej i komunikatory.
Operacje	Funkcja Zapobieganie utracie danych wykonuje jedną lub więcej operacji po wykryciu próby przesłania informacji poufnych za pomocą dowolnego z wybranych kanałów.
Wyjątki	Wyjątki zastępują skonfigurowane reguły DLP. Skonfigurowanie wyjątków umożliwia zarządzanie monitorowanymi i niemonitorowanymi miejscami docelowymi oraz skanowaniem skompresowanych plików.
Identyfikatory danych	Funkcja Zapobieganie utracie danych do identyfikacji informacji poufnych używa identyfikatorów danych. Identyfikatory danych obejmują wyrażenia, atrybuty plików oraz słowa kluczowe, które służą jako części składowe szablonów DLP.

Typy identyfikatorów danych

Zasoby cyfrowe to pliki i dane, które organizacja musi chronić przed nieautoryzowanym przesyłaniem. Administratorzy mogą zdefiniować zasoby cyfrowe za pomocą następujących identyfikatorów danych:

- **Wyrażenia**: dane o określonej strukturze.

  Szczegółowe informacje zawiera sekcja *Wyrażenia na stronie 11-6*.

- **Atrybuty plików**: właściwości plików, takie jak typ i rozmiar.

  Szczegółowe informacje zawiera sekcja *Atrybuty pliku na stronie 11-11*.

- **Listy słów kluczowych**: lista specjalnych słów i wyrażeń.

  Szczegółowe informacje zawiera sekcja *Słowa kluczowe na stronie 11-15*.

Uwaga

Administratorzy nie mogą usunąć identyfikatora danych, który jest używany przez szablon DLP. Należy usunąć szablon przed usunięciem identyfikatora danych.

Wyrażenia

Wyrażenie to dane o określonej strukturze. Na przykład numery kart kredytowych zawierają 16 cyfr i są wyświetlane w formacie „nnnn-nnnn-nnnn-nnnn", dzięki czemu możliwe jest ich wykrywanie przy użyciu wyrażeń.

Administratorzy mogą używać wstępnie zdefiniowanych i niestandardowych wyrażeń.

Szczegółowe informacje zawiera sekcja *Wstępnie zdefiniowane wyrażenia na stronie 11-6* i *Wyrażenia niestandardowe na stronie 11-7*.

Wstępnie zdefiniowane wyrażenia

Funkcja Zapobieganie utracie danych zawiera zestaw wstępnie zdefiniowanych wyrażeń. Zdefiniowanych wcześniej wyrażeń nie można modyfikować ani usuwać.

Funkcja Zapobieganie utracie danych sprawdza te wyrażenia za pomocą dopasowywania wzorców i równań matematycznych. Gdy za pomocą wyrażenia funkcja Zapobieganie utracie danych wyszuka potencjalnie dane wrażliwe, dane te mogą również być poddane dodatkowej weryfikacji.

Pełną lista zdefiniowanych wcześniej wyrażeń zawiera dokument *Listy modułu Ochrona danych* pod adresem http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Wyświetlanie ustawień wstępnie zdefiniowanych wyrażeń

Uwaga

Zdefiniowanych wcześniej wyrażeń nie można modyfikować ani usuwać.

Procedura

1. Przejdź do opcji **Agenci** > **Zapobieganie utracie danych** > **Identyfikatory danych**.
2. Kliknij kartę **wyrażenie**.
3. Kliknij nazwę wyrażenia.
4. Zapoznaj się z ustawieniami na wyświetlonym ekranie.

Wyrażenia niestandardowe

Wyrażenia niestandardowe należy utworzyć, jeśli żadne wstępnie zdefiniowane wyrażenia nie spełniają wymagań firmy.

Wyrażenia to bardzo skuteczne narzędzie służące do dopasowywania łańcuchów znaków. Należy dobrze zapoznać się ze składnią wyrażeń. Błędnie napisane wyrażenia mogą znacznie obniżyć wydajność.

Podczas tworzenia wyrażeń:

- Należy zapoznać się ze wstępnie zdefiniowanymi wyrażeniami, aby uzyskać wskazówki dotyczące definiowania prawidłowych wyrażeń. Jeśli na przykład przy tworzeniu wyrażenia zawierającego datę można skorzystać z wyrażeń z przedrostkiem „Data”.

- Należy pamiętać, że funkcja Zapobieganie utracie danych używa formatu wyrażeń zdefiniowanego przez zasady Perl Compatible Regular Expressions (PCRE). Więcej informacji na temat standardu PCRE można znaleźć w witrynie internetowej:

  http://www.pcre.org/

- Należy rozpocząć od prostych wyrażeń. Wyrażenia należy zmodyfikować, jeśli powodują fałszywe alarmy, lub dostosować w celu poprawienia wyników.

Przy tworzeniu wyrażeń administratorzy mogą wybierać spośród kilku kryteriów. Wyrażenie musi spełniać wybrane kryteria, zanim funkcja Zapobieganie utracie danych zastosuje je w regułach DLP. Szczegółowe informacje o różnych opcjach kryteriów zawiera temat *Kryteria wyrażeń niestandardowych na stronie 11-8*.

Kryteria wyrażeń niestandardowych

TABELA 11-2. Kryteria opcji wyrażeń niestandardowych

KRYTERIA	REGUŁA	PRZYKŁAD
Brak	Brak	Wszystkie - Nazwiska z amerykańskiego biura cenzusowego • Wyrażenie: [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
Określone znaki	Wyrażenie musi zawierać określone znaki. Ponadto liczba znaków w wyrażeniu musi spełniać limity minimalnej i maksymalnej liczby znaków.	USA - Numer banku ABA • Wyrażenie: [^\d]([0123678]\d{8})[^\d] • Znaki: 0123456789 • Minimalna liczba znaków: 9 • Maksymalna liczba znaków: 9

Kryteria	Reguła	Przykład
Przyrostek	Przyrostek odnosi się do ostatniego segmentu wyrażenia. Przyrostek musi zawierać określone znaki oraz pewną liczbę znaków. Ponadto liczba znaków w wyrażeniu musi spełniać limity minimalnej i maksymalnej liczby znaków.	Wszystkie - Adres zamieszkania • Wyrażenie: \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (ulica|ul|aleja|al|trasa|tr|plac|pl|bulwar|blw|)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • Znaki w przyrostku: 0123456789- • Liczba znaków: 5 • Minimalna liczba znaków w wyrażeniu: 25 • Maksymalna liczba znaków w wyrażeniu: 80
Separator jednoznakowy	Wyrażenie musi zawierać dwa segmenty rozdzielone znakiem. Znak musi mieć długość 1 bajta. Ponadto liczba znaków z lewej strony separatora musi spełniać limity minimalnej i maksymalnej liczby znaków. Liczba znaków z prawej strony separatora nie może przekraczać limitu maksymalnej liczby znaków.	Wszystkie - Adres e-mail: • Wyrażenie: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • Separator: @ • Minimalna liczba znaków z lewej strony: 3 • Maksymalna liczba znaków z lewej strony: 15 • Maksymalna liczba znaków z prawej strony: 30

Tworzenie wyrażeń niestandardowych

Procedura

1. Przejdź do opcji **Agenci** > **Zapobieganie utracie danych** > **Identyfikatory danych**.
2. Kliknij kartę **wyrażenie**.

3. Kliknij przycisk **Dodaj**.

   Zostanie wyświetlony nowy ekran.

4. Wpisz nazwę wyrażenia. Długość nazwy nie może przekraczać 100 bajtów. Nazwa nie może zawierać następujących znaków:

   - > < * ^ | & ? \ /

5. Wpisz opis, którego długość nie przekracza 256 bajtów.

6. Wpisz wyświetlane dane.

   Jeśli na przykład tworzysz wyrażenie dla numerów identyfikatorów, wpisz przykładowy numer identyfikatora. Dane te służą wyłącznie do celów informacyjnych i nie będą wyświetlane w innym miejscu produktu.

7. Wybierz jedno z następujących kryteriów i skonfiguruj dodatkowe ustawienia dla wybranych kryteriów (patrz *Kryteria wyrażeń niestandardowych na stronie 11-8*):

   - Brak
   - Określone znaki
   - Przyrostek
   - Separator jednoznakowy

8. Przetestuj wyrażenie na rzeczywistych danych.

   Jeśli na przykład wyrażenie dotyczy identyfikatora krajowego, wpisz prawidłowy numer identyfikatora w polu tekstowym **Dane testowe**, kliknij przycisk **Sprawdź**, a następnie sprawdź wynik.

9. Kliknij przycisk **Zapisz**, jeśli wyniki są prawidłowe.

Uwaga

Ustawienia należy zapisać tylko w przypadku, gdy test się powiódł. Wyrażenie, które nie może wykryć żadnych danych, marnuje zasoby systemowe i może wpłynąć na wydajność.

10. Zostanie wyświetlony komunikat przypominający o konieczności wdrożenia ustawień na agentach. Kliknij **Zamknij**.

11. Na ekranie **Identyfikatory danych DLP** kliknij polecenie **Zastosuj do wszystkich agentów**.

Importowanie wyrażeń niestandardowych

Użyj tej opcji, jeśli istnieje prawidłowo sformatowany plik `.dat` zawierający wyrażenia. Plik można wygenerować, eksportując wyrażenia z serwera, do którego aktualnie uzyskujesz dostęp, lub z innego serwera.

Uwaga

Pliki wyrażeń `.dat` wygenerowane przez tę wersję funkcji Zapobieganie utracie danych nie są obsługiwane przez poprzednie wersje.

Procedura

1. Przejdź do opcji **Agenci** > **Zapobieganie utracie danych** > **Identyfikatory danych**.
2. Kliknij kartę **wyrażenie**.
3. Kliknij przycisk **Importuj**, a następnie znajdź plik `.dat` zawierający wyrażenia.
4. Kliknij przycisk **Otwórz**.

   Zostanie wyświetlony komunikat z informacją o powodzeniu importowania. Jeśli wyrażenie do zaimportowania już istnieje, zostanie pominięte.
5. Kliknij przycisk **Zastosuj do wszystkich agentów**.

Atrybuty pliku

Atrybuty pliku to określone właściwości pliku. Podczas definiowania zasobów cyfrowych można używać identyfikatorów danych, a mianowicie typu pliku i rozmiaru pliku. Na przykład producent oprogramowania chce ograniczyć udostępnianie instalatora oprogramowania firmy do działu badań i rozwoju, którego członkowie są odpowiedzialni za tworzenie i testowanie oprogramowania. W takim przypadku

administrator OfficeScan może utworzyć regułę, która blokuje transmisję plików wykonywalnych o rozmiarze od 10 do 40 MB do wszystkich działów z wyjątkiem działu badań i rozwoju.

Atrybuty pliku stanowią słabe identyfikatory poufnych plików. Kontynuując przykład z tego tematu, instalatory oprogramowania innych firm, które są współużytkowane przez inne działy firmy, zostaną prawdopodobnie zablokowane. Z tego powodu firma Trend Micro zaleca połączenie atrybutów plików z innymi identyfikatorami danych DLP, aby lepiej wykrywać poufne pliki.

Pełną lista obsługiwanych typów plików zawiera dokument *Listy modułu Ochrona danych* pod adresem http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Lista wstępnie zdefiniowanych atrybutów pliku

Funkcja Zapobieganie utracie danych zawiera zestaw wstępnie zdefiniowanych atrybutów pliku. Listy takiej nie można modyfikować ani usuwać. Lista ma własne wbudowane warunki, które określają, czy szablon powinien wywoływać naruszenie reguły.

Lista wstępnie zdefiniowanych atrybutów pliku umożliwia ograniczanie dostępu do rejestratorów danych (CD/DVD).

Szczegółowe informacje zawiera sekcja *Blokowanie dostępu do rejestratorów danych (CD/DVD) na stronie 11-36*.

Tworzenie listy atrybutów plików

Procedura

1. Przejdź do opcji **Agenci** > **Zapobieganie utracie danych** > **Identyfikatory danych**.
2. Kliknij kartę **atrybut pliku**.
3. Kliknij przycisk **Dodaj**.

   Zostanie wyświetlony nowy ekran.

4. Wpisz nazwę listy atrybutów plików. Długość nazwy nie może przekraczać 100 bajtów. Nazwa nie może zawierać następujących znaków:

   - > < * ^ | & ? \ /

5. Wpisz opis, którego długość nie przekracza 256 bajtów.

6. Wybierz preferowane, rzeczywiste typy plików.

7. Jeśli żądany typ pliku nie znajduje się na liście, wybierz **Rozszerzenia pliku**, a następnie wpisz typ rozszerzenia pliku. Funkcja Zapobieganie utracie danych sprawdza pliki o określonych rozszerzeniach, ale nie sprawdza ich prawdziwych rodzajów pliku. Wytyczne podczas określania rozszerzenia pliku:

   - Każde rozszerzenie musi zaczynać się znakiem gwiazdki (*), następnie występuje kropka (.) i rozszerzenie. Gwiazdka jest symbolem wieloznacznym stanowiącym rzeczywistą nazwę pliku. Przykładowo: `*.pol` oznacza zarówno nazwę `12345.pol`, jak i `test.pol`.

   - W rozszerzeniach można używać symboli wieloznacznych. Znak zapytania (?) możne oznaczać jeden znak, a gwiazdka (*) może oznaczać co najmniej dwa znaki. Przykłady:

     - `*.*m` może oznaczać następujące nazwy plików: `ABC.dem`, `ABC.prm`, `ABC.sdcm`

     - `*.m*r` może oznaczać następujące nazwy plików: `ABC.mgdr`, `ABC.mtp2r`, `ABC.mdmr`

     - `*.fm?` może oznaczać następujące nazwy plików: `ABC.fme`, `ABC.fml`, `ABC.fmp`

   - Podczas dodawania znaku gwiazdki na końcu rozszerzenia należy zachować ostrożność, ponieważ może ona oznaczać części nazwy pliku i niepowiązane rozszerzenia. Na przykład: ciąg `*.do*` odpowiada plikowi `abc.doctor_john.jpg` oraz plikowi `abc.donor12.pdf`.

   - Rozszerzenia plików można rozdzielać znakiem średnika (;). Po średniku nie trzeba dodawać spacji.

8. Wpisz minimalny i maksymalny rozmiar pliku w bajtach. Obie wartości muszą być liczbami całkowitymi większymi od zera.

9. Kliknij przycisk **Zapisz**.

10. Zostanie wyświetlony komunikat przypominający o konieczności wdrożenia ustawień na agentach. Kliknij **Zamknij**.

11. Na ekranie **Identyfikatory danych DLP** kliknij polecenie **Zastosuj do wszystkich agentów**.

Importowanie listy atrybutów plików

Użyj tej opcji, jeśli istnieje prawidłowo sformatowany plik `.dat` zawierający listy atrybutów plików. Plik można wygenerować, eksportując listy atrybutów plików z serwera, do którego aktualnie uzyskujesz dostęp, lub z innego serwera.

Uwaga

Pliki `.dat` z atrybutami plików wygenerowane przez tę wersję funkcji Zapobieganie utracie danych nie są obsługiwane przez poprzednie wersje.

Procedura

1. Przejdź do opcji **Agenci** > **Zapobieganie utracie danych** > **Identyfikatory danych**.

2. Kliknij kartę **atrybut pliku**.

3. Kliknij przycisk **Importuj**, a następnie znajdź plik `.dat` zawierający listy atrybutów plików.

4. Kliknij przycisk **Otwórz**.

   Zostanie wyświetlony komunikat z informacją o powodzeniu importowania. Jeśli lista atrybutów plików do zaimportowania już istnieje, zostanie pominięta.

5. Kliknij przycisk **Zastosuj do wszystkich agentów**.

Słowa kluczowe

Słowa kluczowe to specjalne słowa lub wyrażenia. Do listy słów kluczowych można dodać powiązane słowa kluczowe, aby zidentyfikować określone typy danych. Na przykład w certyfikacie medycznym mogą wystąpić słowa kluczowe „prognoza", „grupa krwi", „szczepionka" i „lekarz". Aby uniemożliwić transmisję plików certyfikatów medycznych, można użyć tych słów kluczowych w regule DLP, a następnie skonfigurować funkcję Zapobieganie utracie danych w celu blokowania plików zawierających te słowa kluczowe.

Powszechnie używane słowa można połączyć w celu utworzenia znaczących słów kluczowych. Na przykład angielskie słowa „end", „read", „if i „at" można połączyć w celu utworzenia słów kluczowych, które występują w kodzie źródłowym, takich jak „END-IF", „END-READ" i „AT END".

Istnieje możliwość użycia wstępnie zdefiniowanych i niestandardowych listy słów kluczowych. Szczegółowe informacje zawiera sekcja *Wstępnie zdefiniowane listy słów kluczowych na stronie 11-15* i *Niestandardowe listy słów kluczowych na stronie 11-16*.

Wstępnie zdefiniowane listy słów kluczowych

Funkcja Zapobieganie utracie danych zawiera zestaw wstępnie zdefiniowanych list słów kluczowych. Nie można ich modyfikować ani usuwać. Każda lista ma własne wbudowane warunki, które określają, czy szablon powinien wywoływać naruszenie reguły.

Pełną lista zdefiniowanych wcześniej list słów kluczowych w funkcji Zapobieganie utracie danych zawiera dokument *Listy modułu Ochrona danych* pod adresem http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Jak działa lista słów kluczowych

Warunek z liczbą słów kluczowych

Każda lista słów kluczowych wymaga, aby przed wywołaniem naruszenia w dokumencie została odnaleziona pewna liczba słów kluczowych.

Warunek z liczbą słów kluczowych zawiera następujące warunki:

- **Wszystkie**: w dokumencie muszą się znajdować wszystkie słowa kluczowe.
- **Dowolne**: w dokumencie muszą się znajdować dowolne ze słów kluczowych.
- **Określona liczba**: w dokumencie musi się znajdować określona liczba słów kluczowych. Gdy liczba słów kluczowych przekracza tę liczbę, funkcja Zapobieganie utracie danych wywoła naruszenie.

Warunek odległości

Niektóre listy zawierają dodatkowy warunek „odległości". „Odległość określa maksymalną liczbę znaków między pierwszym znakiem jednego słowa kluczowego oraz pierwszym znakiem kolejnego. Poniżej znajduje się przykład.

F**irst Name:_John_ L**ast Name:_Smith_

Lista **Formularze - Imię, Nazwisko** ma odległość o wartości 50 oraz wprowadzone często używane nazwy pól „Imię" i „Nazwisko". W powyższym przykładzie funkcja Zapobieganie utracie danych zgłosi naruszenie. Liczba znaków między literą „F" w słowie „First Name" oraz „L" w słowie „Last Name" wynosi osiem (8)

Poniżej znajduje się przykład wpisu, który nie wywoła naruszenia.

The f**irst name of our new employee from Switzerland is John. His l**ast name is Smith.

W powyższym przykładzie zostanie zgłoszone naruszenie. Liczba znaków między literą „F" w słowie „First Name" oraz „L" w słowie „Last Name" wynosi dziewięćdziesiąt jeden (61). Przekracza to wartość odległości i nie stanowi powoduje wywołania naruszenia.

Niestandardowe listy słów kluczowych

Niestandardowe listy słów kluczowych należy utworzyć, jeśli żadne wstępnie zdefiniowane listy słów kluczowych nie spełniają wymagań użytkownika.

Istnieje wiele kryteriów, z których można wybierać podczas tworzenia list słów kluczowych. Lista słów kluczowych musi spełniać wybrane kryteria, zanim funkcja Zapobieganie utracie danych zastosuje je w regule. Wybierz jedno z następujących kryteriów dla każdej listy słów kluczowych:

- **Dowolne słowo kluczowe**
- **Wszystkie słowa kluczowe**
- **Wszystkie słowa kluczowe zawierające do <x> znaków**
- **Wynik połączony dla słów kluczowych przekracza próg**

Szczegółowe informacje o regułach kryteriów znajdują się w temacie *Niestandardowe kryteria listy słów kluczowych na stronie 11-17*.

Niestandardowe kryteria listy słów kluczowych

TABELA 11-3. Kryteria dla listy słów kluczowych

KRYTERIA	REGUŁA
Dowolne słowo kluczowe	Plik musi zawierać co najmniej jedno słowo kluczowe z listy słów kluczowych.
Wszystkie słowa kluczowe	Plik musi zawierać wszystkie słowa kluczowe z listy słów kluczowych.

Kryteria	Reguła
Wszystkie słowa kluczowe zawierające do <x> znaków	Plik musi zawierać wszystkie słowa kluczowe z listy słów kluczowych. Ponadto każda para słów kluczowych musi znajdować się w odległości <x> znaków od siebie. Na przykład 3 słowa kluczowe to WEB, DISK i USB, a określona liczba znaków to 20. Jeśli funkcja zapobiegania utracie danych wykryje wszystkie słowa kluczowe w kolejności DISK, WEB i USB, liczba znaków od "D" (w wyrazie DISK) do "W" (w wyrazie WEB) oraz od "W" do "U" (w wyrazie USB) może wynieść maksymalnie 20. Z tymi kryteriami zgodne są następujące dane: DISK####WEB############USB Następujące dane nie są zgodne z kryteriami: DISK******************WEB****USB (23 znaki między "D" a "W") Podczas określania liczby znaków należy pamiętać, że mała liczba (na przykład 10) spowoduje przyspieszenie czasu skanowania, ale spowoduje objęcie relatywnie niewielkiego obszaru. Może to zmniejszyć prawdopodobieństwo wykrycia poufnych danych, szczególnie w dużych plikach. W miarę zwiększania liczby zwiększa się również obejmowany obszar, ale czas skanowania może się wydłużyć.
Wynik połączony dla słów kluczowych przekracza próg	Plik musi zawierać co najmniej jedno słowo kluczowe z listy słów kluczowych. Jeśli zostanie wykryte tylko jedno słowo kluczowe, jego wynik musi wyższy od progu. W przypadku kilku słów kluczowych ich wynik połączony musi być wyższy od progu. Do każdego słowa kluczowego należy przypisać wynik od 1 do 10. Bardzo poufne słowo lub wyrażenie, takie jak „podwyżka pensji” dla działu kadr, powinno mieć relatywnie wysoki wynik. Słowa lub wyrażenia, które nie mają tak dużego znaczenia, powinny mieć niższe wyniki. Podczas konfigurowania progu należy rozważyć wyniki przypisane do słów kluczowych. Jeśli na przykład istnieje pięć słów kluczowych, a trzy z nich mają wysoki priorytet, próg może być równy lub niższy niż połączony wynik trzech słów kluczowych o wysokim priorytecie. Oznacza to, że wykrycie tych trzech słów kluczowych wystarczy, aby określić plik jako poufny.

Tworzenie listy słów kluczowych

Procedura

1. Przejdź do opcji **Agenci** > **Zapobieganie utracie danych** > **Identyfikatory danych**.
2. Kliknij kartę **słowo kluczowe**.
3. Kliknij przycisk **Dodaj**.

   Zostanie wyświetlony nowy ekran.
4. Wpisz nazwę listy słów kluczowych. Długość nazwy nie może przekraczać 100 bajtów. Nazwa nie może zawierać następujących znaków:

   - > < * ^ | & ? \ /
5. Wpisz opis, którego długość nie przekracza 256 bajtów.
6. Wybierz jedno z następujących kryteriów i skonfiguruj dodatkowe ustawienia dla wybranych kryteriów:

   - **Dowolne słowo kluczowe**
   - **Wszystkie słowa kluczowe**
   - **Wszystkie słowa kluczowe zawierające do <x> znaków**
   - **Wynik połączony dla słów kluczowych przekracza próg**
7. Aby ręcznie dodać słowa kluczowe do listy:

   a. Wpisz słowo kluczowe o długości od 3 do 40 bajtów i określ, czy wielkość znaków ma znaczenie.

   b. Kliknij przycisk **Dodaj**.
8. Aby dodać słowa kluczowe przy użyciu opcji „Importuj”:

Uwaga

Użyj tej opcji, jeśli istnieje prawidłowo sformatowany plik `.csv` zawierający słowa kluczowe. Plik można wygenerować, eksportując słowa kluczowe z serwera, do którego aktualnie uzyskujesz dostęp, lub z innego serwera.

a. Kliknij przycisk **Importuj**, a następnie znajdź plik `.csv` zawierający słowa kluczowe.

b. Kliknij przycisk **Otwórz**.

Zostanie wyświetlony komunikat z informacją o powodzeniu importowania. Jeśli słowo kluczowe do zaimportowania już istnieje na liście, zostanie pominięte.

9. Aby usunąć słowa kluczowe, wybierz je i kliknij przycisk **Usuń**.

10. Aby wyeksportować słowa kluczowe:

Uwaga

Użyj funkcji eksportowania, aby utworzyć kopię zapasową wybranych szablonów lub zaimportować je na inny serwer. Zostaną wyeksportowane wszystkie słowa kluczowe z listy. Nie jest możliwe eksportowanie pojedynczych słów kluczowych.

a. Kliknij **Eksportuj**.

b. Zapisz wynikowy plik `.csv` w preferowanej lokalizacji.

11. Kliknij przycisk **Zapisz**.

12. Zostanie wyświetlony komunikat przypominający o konieczności wdrożenia ustawień na agentach. Kliknij **Zamknij**.

13. Na ekranie **Identyfikatory danych DLP** kliknij polecenie **Zastosuj do wszystkich agentów**.

Importowanie listy słów kluczowych

Użyj tej opcji, jeśli istnieje prawidłowo sformatowany plik `.dat` zawierający listy słów kluczowych. Plik można wygenerować, eksportując listy słów kluczowych z serwera, do którego aktualnie uzyskujesz dostęp, lub z innego serwera.

Uwaga

Pliki `.dat` z listami słów kluczowych, wygenerowane przez tę wersję funkcji Zapobieganie utracie danych, nie są obsługiwane przez poprzednie wersje.

Procedura

1. Przejdź do opcji **Agenci** > **Zapobieganie utracie danych** > **Identyfikatory danych**.
2. Kliknij kartę **słowo kluczowe**.
3. Kliknij przycisk **Importuj**, a następnie znajdź plik `.dat` zawierający listy słów kluczowych.
4. Kliknij przycisk **Otwórz**.

   Zostanie wyświetlony komunikat z informacją o powodzeniu importowania. Jeśli lista słów kluczowych do zaimportowania już istnieje, zostanie pominięta.
5. Kliknij przycisk **Zastosuj do wszystkich agentów**.

Szablony Zapobieganie utracie danych

Szablon DLP łączy identyfikatory danych DLP oraz operatory logiczne (I, Lub, Oprócz) w celu utworzenia instrukcji warunku. Regule usługi DLP będą podlegać tylko pliki lub dane, które spełniają określoną instrukcję warunku.

Na przykład, musi to być plik programu Microsoft Word (atrybut pliku) I musi zawierać określone terminy prawnicze (słowa kluczowe) I musi zawierać numery identyfikatorów (wyrażenia), aby podlegał regule „Umowy o pracę”. Ta reguła umożliwia pracownikom działu kadr przesyłanie pliku poprzez wydrukowanie, dzięki czemu wydrukowana kopia

może zostać podpisana przez pracownika. Transmisja przez wszystkie inne możliwe kanały, takie jak poczta elektroniczna, jest zablokowana.

Własne szablony można utworzyć, jeśli skonfigurowano identyfikatory danych DLP. Można również używać wstępnie zdefiniowanych szablonów. Szczegółowe informacje zawiera sekcja *Niestandardowe szablony DLP na stronie 11-22* i *Wstępnie zdefiniowane szablony DLP na stronie 11-22*.

Uwaga

Nie jest możliwe usunięcie szablonu, który jest używane przez regułę DLP. Przed usunięciem szablonu należy usunąć go z reguły.

Wstępnie zdefiniowane szablony DLP

Funkcja Zapobieganie utracie danych zawiera zestaw wstępnie zdefiniowanych szablonów, których można używać w celu zapewnienia zgodności z różnymi przepisami. Zdefiniowanych wcześniej szablonów nie można modyfikować ani usuwać.

- **GLBA**: ustawa Gramm-Leach-Billey Act
- **HIPAA**: ustawa Health Insurance Portability and Accountability Act
- **PCI-DSS**: Payment Card Industry Data Security Standard (standard zabezpieczeń branży kart płatniczych)
- **SB-1386**: ustawa senacka 1386
- **US PII**: amerykańskie dane osobowe

Szczegółową listę wszystkich wstępnie zdefiniowanych szablonów i przykłady danych podlegających ochronie zawiera dokument *Listy modułu Ochrona danych* pod adresem http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Niestandardowe szablony DLP

Własne szablony należy utworzyć, jeśli skonfigurowano identyfikatory danych. Szablon łączy identyfikatory danych oraz operatory logiczne (I, Lub, Oprócz) w celu utworzenia instrukcji warunku.

Więcej informacji o wyrażeniach warunkowych oraz operatorach logicznych i przykłady ich zastosowań zawiera dokument *Instrukcje warunków i operatory logiczne na stronie 11-23*.

Instrukcje warunków i operatory logiczne

Funkcja Zapobieganie utracie danych wartościuje instrukcje warunków od lewej do prawej strony. Podczas konfigurowania instrukcji warunków należy ostrożnie używać operatorów logicznych. Nieprawidłowe użycie spowoduje powstanie błędnej instrukcji warunku, co doprowadzi do uzyskania nieoczekiwanych wyników.

Poniższa tabela zawiera przykłady.

TABELA 11-4. Przykładowe instrukcje warunków

INSTRUKCJA WARUNKU	INTERPRETACJA I PRZYKŁAD
[Identyfikator danych 1] **I** [Identyfikator danych 2] **Oprócz** [Identyfikator danych 3]	Plik musi spełniać [Identyfikator danych 1] i [Identyfikator danych 2], lecz nie [Identyfikator danych 3]. Na przykład: Plik musi być [dokumentem Adobe PDF] i musi zawierać [adres e-mail], ale nie może zawierać [wszystkich słów kluczowych z listy słów kluczowych].
[Identyfikator danych 1] **Lub** [Identyfikator danych 2]	Plik musi spełniać [Identyfikator danych 1] lub [Identyfikator danych 2] Na przykład: Plik musi być [dokumentem Adobe PDF] lub [dokumentem Microsoft Word].
Oprócz [Identyfikator danych 1]	Plik nie może spełniać warunku [Identyfikator danych 1]. Na przykład: Plik nie może być [plikiem multimedialnym].

Jak pokazuje ostatni przykład w tabeli, pierwszy identyfikator danych w instrukcji warunku może mieć operator „Oprócz”, jeśli plik nie może spełniać żadnych identyfikatorów danych w instrukcji. Jednak w większości przypadków pierwszy identyfikator danych nie ma operatora.

Tworzenie szablonu

Procedura

1. Przejdź do opcji **Agenci** > **Szablony Zapobieganie utracie danych** > **Szablony DLP**.
2. Kliknij przycisk **Dodaj**.

   Zostanie wyświetlony nowy ekran.
3. Wpisz nazwę szablonu. Długość nazwy nie może przekraczać 100 bajtów. Nazwa nie może zawierać następujących znaków:

   - > < * ^ | & ? \ /
4. Wpisz opis, którego długość nie przekracza 256 bajtów.
5. Wybierz identyfikatory danych i kliknij ikonę „Dodaj”.

   Podczas wybierania definicji:

   - Aby wybrać wiele pozycji, naciśnij i przytrzymaj klawisz CTRL, a następnie wybierz identyfikatory danych.
   - Użyj funkcji wyszukiwania, aby znaleźć określoną definicję. Można wpisać pełną lub częściową nazwę identyfikatora danych.
   - Każdy szablon może zawierać maksymalnie 30 identyfikatorów danych.
6. Aby utworzyć nowe wyrażenie, kliknij pozycję **wyrażenia**, a następnie kliknij przycisk **Dodaj nowe wyrażenie**. Na wyświetlonym ekranie skonfiguruj ustawienia wyrażenia.
7. Aby utworzyć nową listę atrybutów plików, kliknij pozycję **Atrybuty plików**, a następnie kliknij przycisk **Dodaj nowy atrybut pliku**. Na wyświetlonym ekranie skonfiguruj ustawienia listy atrybutów plików.
8. Aby utworzyć nową listę słów kluczowych, kliknij pozycję **Słowa kluczowe**, a następnie kliknij przycisk **Dodaj nowe słowo kluczowe**. Na wyświetlonym ekranie skonfiguruj ustawienia listy słów kluczowych.

9. Jeśli wybrano wyrażenie, wpisz liczbę wystąpień wyrażenia, zanim funkcja Zapobieganie utracie danych zastosuje wyrażenie do reguły.

10. Wybierz operator logiczny dla każdej definicji.

Uwaga

Podczas konfigurowania instrukcji warunków należy ostrożnie używać operatorów logicznych. Nieprawidłowe użycie spowoduje powstanie błędnej instrukcji warunku, co doprowadzi do uzyskania nieoczekiwanych wyników. Przykłady prawidłowego użycia zawiera sekcja *Instrukcje warunków i operatory logiczne na stronie 11-23*.

11. Aby usunąć identyfikator danych z listy wybranych identyfikatorów, kliknij ikonę kosza.

12. Poniżej obszaru **Podgląd** sprawdź instrukcję warunku i wprowadź zmiany, jeśli są one wymagane.

13. Kliknij przycisk **Zapisz**.

14. Zostanie wyświetlony komunikat przypominający o konieczności wdrożenia ustawień na agentach. Kliknij **Zamknij**.

15. Na ekranie **Szablony DLP** kliknij polecenie **Zastosuj do wszystkich agentów**.

Importowanie szablonów

Użyj tej opcji, jeśli istnieje prawidłowo sformatowany plik `.dat` zawierający szablony. Plik można wygenerować, eksportując szablony z serwera, do którego aktualnie uzyskujesz dostęp, lub z innego serwera.

Uwaga

Aby zaimportować szablony DLP z programu OfficeScan 10.6, należy wykonać import powiązanych identyfikatorów danych (znanych wcześniej jako definicje). Funkcja Zapobieganie utracie danych nie pozwala na import szablonów, w których nie ma powiązanych identyfikatorów danych.

Procedura

1. Przejdź do opcji **Agenci** > **Szablony Zapobieganie utracie danych** > **Szablony DLP**.
2. Kliknij przycisk **Importuj**, a następnie znajdź plik `.dat` zawierający szablony.
3. Kliknij przycisk **Otwórz**.

   Zostanie wyświetlony komunikat z informacją o powodzeniu importowania. Jeśli szablon do zaimportowania już istnieje, zostanie pominięty.
4. Kliknij przycisk **Zastosuj do wszystkich agentów**.

Kanały DLP

Użytkownicy mogą przesyłać informacje poufne za pomocą różnych kanałów. Program OfficeScan może monitorować następujące kanały:

- **Kanały sieciowe**: Informacje poufne są przesyłane za pomocą protokołów sieciowych, takich jak HTTP i FTP.
- **Kanały systemu i aplikacji**: Informacje poufne są przesyłane za pomocą lokalnych aplikacji i urządzeń peryferyjnych punktu końcowego.

Kanały sieciowe

Program OfficeScan może monitorować transmisję danych za pomocą następujących kanałów:

- Klienci e-mail
- FTP
- HTTP i HTTPS
- Aplikacje do wiadomości błyskawicznych
- Protokół SMB

- Poczta przez sieć Web

Aby określić transmisje danych przeznaczone do monitorowania, program OfficeScan sprawdza zakres transmisji, który należy skonfigurować. W zależności od wybranego zakresu program OfficeScan będzie monitorować wszystkie transmisje danych lub tylko transmisje poza siecią lokalną (LAN).

Informacje na temat zakresu transmisji dostępne są w temacie *Zakres transmisji i cele kanałów sieciowych na stronie 11-31*.

Klienci e-mail

Program OfficeScan monitoruje wiadomości e-mail przesyłane za pomocą różnych agentów poczty e-mail. Program agenci sprawdza temat, treść i załączniki wiadomości e-mail pod kątem identyfikatorów danych. Listę obsługiwanych agentów poczty e-mail zawiera dokument *Listy modułu Ochrona danych* pod adresem:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Monitorowanie jest wykonywane, kiedy użytkownik podejmuje próbę wysłania wiadomości e-mail. Jeśli wiadomość e-mail zawiera identyfikatory danych, program OfficeScan umożliwi wysłanie lub zablokowanie tej wiadomości.

Można określić niemonitorowane wewnętrzne domeny e-mail oraz monitorowane poddomeny.

- **Niemonitorowane domeny poczty e-mail**: Program OfficeScan natychmiast umożliwia transmisję wiadomości e-mail przesyłanych do domen niemonitorowanych.

  Uwaga

  Transmisja danych jest dozwolona dla tych monitorowanych i niemonitorowanych poddomen e-mail, dla których wykonywana jest operacja Monitoruj. Jedyną różnicą jest to, że w przypadku niemonitorowanych domen e-mail, program OfficeScan nie rejestruje transmisji, podczas gdy dla monitorowanych domen e-mail, transmisja jest zawsze rejestrowana.

- **Niemonitorowane domeny poczty e-mail**: Kiedy program OfficeScan wykryje wiadomości e-mail przesyłane do monitorowanej domeny, sprawdza on operację

w kontekście reguły. W zależności od operacji transmisja jest blokowana lub umożliwiana.

Uwaga

Jeśli jako kanał monitorowany wybrano agentów poczty e-mail, wiadomość e-mail musi być zgodna z regułą, aby była monitorowana. Jednak wiadomość e-mail przesłana do monitorowanej poddomeny e-mail jest monitorowana automatycznie, nawet jeśli nie jest zgodna z regułą.

Domeny można określić przy użyciu jednego z następujących formatów, oddzielając wiele domen przecinkami:

- Format X400, np. /O=Trend/OU=USA, /O=Trend/OU=Chiny
- Domeny e-mail, np. `example.com`

W przypadku wiadomości e-mail wysyłanych za pomocą protokołu SMTP program OfficeScan sprawdza, czy docelowy serwer SMTP znajduje się na poniższych listach:

1. Monitorowane miejsca docelowe
2. Niemonitorowane miejsca docelowe

Uwaga

Szczegółowe informacje na temat monitorowanych i niemonitorowanych miejsc docelowych zawiera sekcja *Definiowanie monitorowanych i niemonitorowanych miejsc docelowych na stronie 11-44*.

3. Niemonitorowane domeny e-mail
4. Monitorowane poddomeny e-mail

Oznacza to, że jeśli wiadomość e-mail zostanie wysłana do serwera SMTP znajdującego się na liście monitorowanych miejsc docelowych, to wiadomość e-mail jest monitorowana. Jeśli serwer SMTP nie znajduje się na liście monitorowanych miejsc docelowych, program OfficeScan sprawdza inne listy.

W przypadku widomości e-mail wysyłanych za pomocą innych protokołów program OfficeScan sprawdza tylko poniższe listy:

1. Niemonitorowane domeny e-mail
2. Monitorowane poddomeny e-mail

FTP

Kiedy program OfficeScan wykryje, że klient FTP próbuje przesłać pliki na serwer FTP, sprawdzana jest obecność identyfikatorów danych w plikach. W tym momencie nie jest przesyłany żaden plik. W zależności od reguły kontroli zasobów cyfrowych program OfficeScan umożliwi lub zablokuje przesyłanie pliku.

Jeśli zostanie skonfigurowana reguła blokująca przesyłanie plików, należy pamiętać o następujących kwestiach:

- Kiedy program OfficeScan zablokuje przesyłanie plików, niektóre klienty FTP będą ponawiać próby ich przesłania. W takim przypadku program OfficeScan zakończy działanie klienta FTP, aby zapobiec próbom ponownego przesłania. Użytkownicy nie otrzymają powiadomienia po zamknięciu klienta FTP. Należy poinformować ich o tej sytuacji podczas wprowadzania reguł DLP.
- Jeśli plik do przesłania spowoduje nadpisanie pliku na serwerze FTP, plik na serwerze FTP może zostać usunięty.

Listę obsługiwanych klientów FTP zawiera dokument *Listy modułu Ochrona danych* pod adresem:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

HTTP i HTTPS

Program OfficeScan monitoruje dane do przesłania za pośrednictwem protokołów HTTP i HTTPS. W przypadku protokołu HTTPS program OfficeScan sprawdza dane przed ich zaszyfrowaniem i przesłaniem.

Listę obsługiwanych przeglądarek i aplikacji internetowych zawiera dokument *Listy modułu Ochrona danych* pod adresem:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Aplikacje do wiadomości błyskawicznych

Program OfficeScan monitoruje wiadomości i pliki przesyłane przez użytkowników przy użyciu aplikacji do wiadomości błyskawicznych. Wiadomości i pliki odbierane przez użytkowników nie są monitorowane.

Listę obsługiwanych aplikacji do wiadomości błyskawicznych zawiera dokument *Listy modułu Ochrona danych* pod adresem:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Kiedy program OfficeScan zablokuje wiadomość lub plik przesłany za pomocą aplikacji AOL Instant Messenger, MSN, Windows Messenger lub Windows Live Messenger, zamyka także aplikację. W przeciwnym razie aplikacja zawiesi się i użytkownicy będą zmuszeni do jej zamknięcia. Użytkownicy nie otrzymają powiadomienia po zamknięciu aplikacji. Należy poinformować ich o tej sytuacji podczas wprowadzania reguł DLP.

Protokół SMB

Program OfficeScan monitoruje transmisje danych za pośrednictwem protokołu SMB (Server Message Block), który umożliwia dostęp do udostępnionych plików. Kiedy inny użytkownik próbuje skopiować lub odczytać udostępniony plik użytkownika, program OfficeScan sprawdza, czy plik jest zasobem cyfrowym lub zawiera taki zasób, a następnie zezwala na operację lub ją blokuje.

Uwaga

Operacja Kontrola urządzeń ma wyższy priorytet niż operacja kontroli zasobów cyfrowych. Jeśli na przykład kontrola urządzeń nie zezwala na przenoszenie plików na zmapowanych dyskach sieciowych, transmisja danych poufnych nie zostanie wykonana, nawet jeśli jest dozwolona przez funkcję DLP.

Szczegółowe informacje o operacjach kontroli urządzeń zawiera temat *Uprawnienia urządzeń pamięci masowej na stronie 10-4*.

Listę aplikacji, które program OfficeScan monitoruje pod kątem dostępu współdzielonego do pliku, zawiera dokument *Listy modułu Ochrona danych*:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Poczta przez sieć Web

Usługi poczty e-mail przez sieć Web przesyłają dane za pośrednictwem protokołu HTTP. Jeśli program OfficeScan wykryje dane wychodzące z obsługiwanych usług, sprawdzi dane pod kątem obecności identyfikatorów danych.

Listę obsługiwanych usług poczty e-mail przez sieć Web zawiera dokument *Listy modułu Ochrona danych* pod adresem:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Zakres transmisji i cele kanałów sieciowych

Zakres transmisji i cele kanałów sieciowych definiują transmisję danych w kanałach sieciowych, które muszą być monitorowane przez program OfficeScan. W przypadku transmisji, które powinny być monitorowane, program OfficeScan sprawdza obecność identyfikatorów danych przed zapewnieniem lub zablokowaniem transmisji.
W przypadku transmisji, które nie powinny być monitorowane, program OfficeScan nie sprawdza obecności identyfikatorów danych i natychmiast zezwala na transmisję.

Zakres transmisji: Wszystkie transmisje

Program OfficeScan monitoruje dane przesyłane z zewnątrz komputera hosta.

Uwaga

Firma Trend Micro zalecana wybranie tego zakresu dla agentów zewnętrznych.

Aby nie monitorować transmisji danych do określonych celów poza komputerem-hostem, należy zdefiniować:

- **Niemonitorowane miejsca docelowe**: : Program OfficeScan nie monitoruje danych przesyłanych do tych miejsc docelowych.

  Uwaga

  Transmisja danych jest dozwolona dla tych monitorowanych i niemonitorowanych miejsc docelowych, dla których wykonywana jest operacja „Monitoruj". Jedyną różnicą jest to, że w przypadku niemonitorowanych miejsc docelowych, program OfficeScan nie rejestruje transmisji, podczas gdy dla monitorowanych, transmisja jest zawsze rejestrowana.

- **Monitorowane miejsca docelowe**: : Są to określone cele w grupie niemonitorowanych miejsc docelowych, które powinny być monitorowane. Monitorowane miejsca docelowe:
  - są opcjonalne, jeśli określono niemonitorowane miejsca docelowe;
  - Konfiguracja nie jest możliwa, jeśli niemonitorowane miejsca docelowe nie zostały zdefiniowane.

Na przykład:

Poniższe adresy IP przypisano do działu prawnego firmy:

- `10.201.168.1` do `10.201.168.25`

Tworzona jest regula, która monitoruje transmisję świadectw pracy dla wszystkich pracowników z wyjątkiem pełnoetatowych pracowników działu prawnego. W tym celu jako zakres transmisji należy wybrać opcję **Wszystkie transmisje**, a następnie:

OPCJA	CZYNNOŚCI
Opcja 1	1. Dodać adresy `10.201.168.1`–`10.201.168.25` do niemonitorowanych miejsc docelowych. 2. Dodać adresy IP pracowników niepełnoetatowych działu prawnego do monitorowanych miejsc docelowych. Przyjmuje się, że istnieją 3 adresy IP: `10.201.168.21`–`10.201.168.23`.

OPCJA	CZYNNOŚCI
Opcja 2	Dodać adresy IP pracowników pełnoetatowych działu prawnego do niemonitorowanych miejsc docelowych: • `10.201.168.1-10.201.168.20` • `10.201.168.24-10.201.168.25`

Instrukcja dotycząca definiowania monitorowanych i niemonitorowanych miejsc docelowych dostępna jest w sekcji *Definiowanie monitorowanych i niemonitorowanych miejsc docelowych na stronie 11-44*.

Zakres transmisji: Tylko transmisje poza siecią lokalną (LAN)

Program OfficeScan monitoruje dane przesyłane do dowolnych obiektów docelowych poza siecią lokalną.

Uwaga

Firma Trend Micro zalecana wybranie tego zakresu dla agentów wewnętrznych.

„Sieć" oznacza sieć firmową lub lokalną. Obejmuje ona bieżącą sieć (adres IP punktu końcowego i maskę sieci) i następujące standardowe, prywatne adresy IP:

- Klasa A: `10.0.0.0` do `10.255.255.255`
- Klasa B: `172.16.0.0` do `172.31.255.255`
- Klasa C: `192.168.0.0` do `192.168.255.255`

Po wybraniu tego zakresu transmisji można określić następujące elementy:

- **Niemonitorowane miejsca docelowe**: : Określ miejsca docelowe poza siecią LAN, które są uważane za bezpieczne i dlatego nie powinny być monitorowane.

Uwaga

Transmisja danych jest dozwolona dla tych monitorowanych i niemonitorowanych miejsc docelowych, dla których wykonywana jest operacja „Monitoruj". Jedyną różnicą jest to, że w przypadku niemonitorowanych miejsc docelowych, program OfficeScan nie rejestruje transmisji, podczas gdy dla monitorowanych, transmisja jest zawsze rejestrowana.

- **Monitorowane miejsca docelowe**: : Określ miejsca docelowe w sieci LAN, które będą monitorowane.

Instrukcja dotycząca definiowania monitorowanych i niemonitorowanych miejsc docelowych dostępna jest w sekcji *Definiowanie monitorowanych i niemonitorowanych miejsc docelowych na stronie 11-44*.

Rozwiązywanie konfliktów

Jeśli ustawienia zakresu transmisji oraz monitorowane i niemonitorowane miejsca docelowe powodują konflikt, program OfficeScan uwzględnia następujące priorytety w kolejności najwyższego do najniższego:

- Monitorowane miejsca docelowe
- Niemonitorowane miejsca docelowe
- Zakres transmisji

Kanały systemu i aplikacji

Program OfficeScan monitoruje następujące kanały systemu i aplikacji:

- Cloud storage services
- Rejestratory danych (CD/DVD)
- Aplikacje peer-to-peer
- Szyfrowanie PGP
- Drukarka

- Magazyn wymienny
- Oprogramowanie do synchronizacji (ActiveSync)
- Schowek systemu Windows

Cloud Storage Service

OfficeScan monitoruje pliki, z których użytkownik korzysta w ramach cloud storage services. Listę obsługiwanych cloud storage services zawiera dokument *Listy modułu Ochrona danych* pod adresem:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Uwaga

Funkcja Zapobieganie utracie danych obsługuje szyfrowanie cloud storage service, gdy w punkcie końcowym agenta jest zainstalowany składnik Endpoint Encryption.

Rejestratory danych (CD/DVD)

Program OfficeScan monitoruje dane nagrywane na płytach CD lub DVD. Listę obsługiwanych urządzeń i oprogramowania do nagrywania danych zawiera dokument *Listy modułu Ochrona danych* pod adresem:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Kiedy program OfficeScan wykryje polecenie „nagrywania" zainicjowane przez dowolne z obsługiwanych urządzeń lub programów, a operacja to „Pomiń", nagrywanie danych będzie kontynuowane. W przypadku operacji Blokuj program OfficeScan sprawdza, czy dowolne pliki do nagrania zawierają identyfikator danych. Jeśli program OfficeScan wykryje co najmniej jeden identyfikator danych, nie zostaną nagrane żadne pliki — w tym pliki, które nie zawierają identyfikatorów danych. Program OfficeScan może także uniemożliwić wysunięcie płyty CD lub DVD. Jeśli wystąpi ten problem, należy poinformować użytkowników, aby uruchomili ponownie oprogramowanie lub zresetowali urządzenie.

Program OfficeScan implementuje dodatkowe reguły nagrywania płyt CD/DVD:

- Aby zredukować liczbę fałszywych alarmów, program OfficeScan nie monitoruje następujących plików:

```
.bud    .dll    .gif    .gpd    .htm    .ico    .ini
.jpg    .lnk    .sys    .ttf    .url    .xml
```

- Aby zwiększyć wydajność, nie są monitorowane dwa typy plików używane przez rejestratory danych firmy Roxio (`*.png` i `*.skn`).
- Program OfficeScan nie monitoruje plików w następujących katalogach:

```
*:\autoexec.bat                 *:\Windows
..\Application Data             ..\Cookies
..\Ustawienia lokalne           ..\ProgramData
..\Program Files                ..\Users\*\AppData
..\WINNT
```

- Obrazy ISO utworzone przez urządzenia i oprogramowanie nie są monitorowane.

Blokowanie dostępu do rejestratorów danych (CD/DVD)

Funkcja Kontrola urządzeń może ograniczyć dostęp tylko do tych urządzeń nagrywających CD/DVD, które korzystają z formatu Aktywny system plików. Niektóre aplikacje innych firm, korzystające z formatu głównego, mogą wykonywać operacje odczytu/zapisu nawet wówczas, gdy funkcja Kontrola urządzeń jest włączona. Aby ograniczyć dostęp do urządzeń nagrywających CD/DVD korzystających z formatu dowolnego typu, należy użyć funkcji Zapobieganie utracie danych.

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Ustawienia DLP**.

4. Kliknij kartę **Agenci zewnętrzni**, aby skonfigurować regułę dla agentów zewnętrznych, lub kartę **Agenci wewnętrzni**, aby skonfigurować regułę dla agentów wewnętrznych.

Uwaga

Skonfiguruj ustawienia lokalizacji agenta, jeśli nie zostało to jeszcze zrobione. Agenci używają tych ustawień lokalizacji w celu określenia prawidłowej reguły Zapobieganie utracie danych do zastosowania. Szczegółowe informacje zawiera sekcja *Lokalizacja punktu końcowego na stronie 15-2*.

5. Wybierz jedną z następujących wartości:

   - Jeśli wyświetlana jest karta **Agenci zewnętrzni**, można zastosować ustawienia Zapobieganie utracie danych do agentów wewnętrznych, wybierając opcję **Zastosuj wszystkie ustawienia do agentów wewnętrznych**.
   - Jeśli wyświetlana jest karta **Agenci wewnętrzni**, można zastosować ustawienia Zapobieganie utracie danych do agentów zewnętrznych, wybierając opcję **Zastosuj wszystkie ustawienia do agentów zewnętrznych**.

6. Na karcie **Reguły** kliknij opcję **Dodaj**.
7. Wybierz opcję **Włącz tę regułę**.
8. Podaj nazwę reguły.
9. Kliknij kartę **Szablon**.
10. Wybierz z listy szablon **Wszystkie rozszerzenia plików** i kliknij przycisk **Dodaj**.
11. Kliknij kartę **Kanał**.
12. W sekcji **Kanały systemu i aplikacji** wybierz opcję **Rejestratory danych (CD/DVD)**.
13. Kliknij kartę **Operacja**.
14. Wybierz operację **Blokuj**.
15. Kliknij przycisk **Zapisz**.
16. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

- **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Aplikacje peer-to-peer

Program OfficeScan monitoruje pliki udostępniane przez użytkowników przy użyciu aplikacji peer-to-peer.

Listę obsługiwanych aplikacji peer-to-peer zawiera dokument *Listy modułu Ochrona danych* pod adresem:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Szyfrowanie PGP

Program OfficeScan monitoruje dane do zaszyfrowania za pomocą oprogramowania do szyfrowania PGP. Program OfficeScan sprawdza dane przed ich zaszyfrowaniem.

Listę obsługiwanych programów do szyfrowania PGP zawiera dokument *Listy modułu Ochrona danych* pod adresem:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Drukarka

Program OfficeScan monitoruje operacje drukarki zainicjowane z różnych aplikacji.

Program OfficeScan nie blokuje operacji drukarki dla nowych plików, które nie zostały zapisane, ponieważ drukowane informacje są w tym momencie zapisane tylko w pamięci.

Listę obsługiwanych aplikacji, które mogą zainicjować operacje drukarki, zawiera dokument *Listy modułu Ochrona danych* pod adresem:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Magazyn wymienny

OfficeScan monitoruje transmisje danych na wymienne urządzenia pamięci masowych lub w ich obrębie. Działania związane z transmisją danych obejmują:

- Utworzenie pliku na urządzeniu
- Skopiowanie pliku z hosta na urządzenie
- Zamknięcie zmodyfikowanego pliku na urządzeniu
- Zmodyfikowanie informacji o pliku (takich jak rozszerzenie pliku) na urządzeniu

Jeśli plik do przesłania zawiera identyfikator danych, program OfficeScan blokuje lub zezwala na transmisję.

Uwaga

- Operacja Kontrola urządzeń ma wyższy priorytet niż operacja kontroli zasobów cyfrowych. Jeśli na przykład kontrola urządzeń nie zezwala na kopiowanie plików na wymienne urządzenie pamięci masowej, transmisja poufnych informacji nie zostanie wykonana, nawet jeśli jest dozwolona przez funkcję DLP.
- Funkcja Zapobieganie utracie danych obsługuje szyfrowanie wymiennych urządzeń pamięci masowej, gdy w punkcie końcowym agenta jest zainstalowany składnik Szyfrowanie punktu końcowego.

Listę obsługiwanych przenośnych urządzeń pamięci masowej i aplikacji umożliwiających transmisję danych zawiera dokument *Listy modułu Ochrona danych* pod adresem:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Obsługa transmisji plików na wymienne urządzenie pamięci masowej jest bardzo prostym procesem. Na przykład użytkownik, który tworzy plik w programie Microsoft

Word, chce zapisać plik na kartę SD (typ pliku, w jakim użytkownik zapisuje plik, nie ma znaczenia). Jeśli plik zawiera zasób cyfrowy, który nie powinien zostać przesłany, program OfficeScan uniemożliwi zapisanie pliku.

W przypadku transmisji plików w obrębie urządzenia program OfficeScan najpierw utworzy kopię zapasową pliku (jeśli jego rozmiar nie przekracza 75 MB) w katalogu `%WINDIR%\system32\dgagent\temp` przed jego przetworzeniem. Program OfficeScan usunie plik zapasowy, jeśli transmisja pliku zostanie dozwolona. Jeśli program OfficeScan zablokuje transmisję, istnieje możliwość, że plik zostanie usunięty. W takim przypadku program OfficeScan skopiuje kopię zapasową pliku do folderu zawierającego oryginalny plik.

Program OfficeScan umożliwia zdefiniowanie wyjątków. Program OfficeScan zawsze zezwala na transmisję danych do tych urządzeń i wewnątrz nich. Istnieje możliwość identyfikowania urządzeń wg producentów i opcjonalnego określania modeli i numerów seryjnych.

Porada

Użyj narzędzia Lista urządzeń w celu wyszukania urządzeń podłączonych do punktów końcowych. Narzędzie dostarcza informacje o producencie, modelu i numerze seryjnym każdego urządzenia. Szczegółowe informacje zawiera sekcja *Narzędzie Lista urządzeń na stronie 10-14*.

Oprogramowanie do synchronizacji (ActiveSync)

Program OfficeScan monitoruje dane przesyłane do urządzenia mobilnego za pośrednictwem oprogramowania do synchronizacji.

Listę obsługiwanych programów do synchronizacji zawiera dokument *Listy modułu Ochrona danych* pod adresem:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Jeśli dane mają źródłowy adres IP 127.0.0.1 i są przesyłane przez port 990 lub 5678 (porty używane do synchronizacji), program OfficeScan sprawdza, czy dane stanowią identyfikator cyfrowy, zanim zablokuje lub zezwoli na transmisję.

Kiedy program OfficeScan zablokuje plik przesyłany przez port 990, w folderze docelowym urządzenia mobilnego może zostać utworzyć plik o tej samej nazwie

zawierający zniekształcone znaki. Dzieje się tak, ponieważ fragmenty pliku zostały skopiowane na urządzenie, zanim program OfficeScan zablokował transmisję.

Schowek systemu Windows

Program OfficeScan monitoruje dane przesyłane do schowka systemu Windows, zanim zablokuje lub zezwoli na transmisję.

Program OfficeScan może także monitorować operacje schowka między hostem a oprogramowaniem VMWare lub Remote Desktop. Monitorowanie jest wykonywane w obiekcie z agentem OfficeScan. Na przykład Agent OfficeScan w maszynie wirtualnej VMware może uniemożliwić przesłanie danych schowka maszyny wirtualnej do hosta. Analogicznie, host z agentem OfficeScan może nie skopiować danych schowka do punktu końcowego, do którego dostęp jest uzyskiwany za pomocą programu Pulpit zdalny.

Czynności Zapobieganie utracie danych

Kiedy funkcja Zapobieganie utracie danych wykrywa identyfikator transmisji danych, sprawdzane są reguły DLP dla wykrytych identyfikatorów danych oraz wykonywane operacje skonfigurowane dla reguł.

Poniższa tabela zawiera czynności z zakresu funkcji Zapobieganie utracie danych

TABELA 11-5. Czynności Zapobieganie utracie danych

OPERACJA	OPIS
Operacje	
Pomiń	Funkcja Zapobieganie utracie danych umożliwia i rejestruje transmisję.
Blokuj	Funkcja Zapobieganie utracie danych blokuje i rejestruje transmisję.
Operacje dodatkowe	

Operacja	Opis
Powiadom użytkownika agenta	Funkcja Zapobieganie utracie danych wyświetla powiadomienie programu, aby poinformować użytkownika transmisji danych o umożliwieniu lub zablokowaniu transmisji.
Dane rekordów	Niezależnie od operacji podstawowej funkcja Zapobieganie utracie danych zapisze informacje poufne w lokalizacji `<Folder instalacji klienta>\DLPLite\Forensic`. Wybierz tę operację, aby ocenić informacje poufne oznaczone przez funkcję Zapobieganie utracie danych. Zarejestrowane informacje poufne mogą zużywać zbyt dużo miejsca na dysku twardym. Dlatego też firma Trend Micro zaleca, aby wybrać tę opcję tylko w przypadku poufnych informacji.

Operacja	Opis
Szyfrowanie obsługiwanych kanałów z użyciem określonego klucza/hasła (dostępne tylko wówczas, gdy zainstalowany jest składnik Szyfrowanie punktu końcowego) **Uwaga** Ta opcja jest dostępna wyłącznie dla kanałów magazynu wymiennego i cloud storage service oraz po wybraniu operacji **Zezwól**.	Jeśli wraz z agentem OfficeScan zainstalowany jest składnik Trend Micro Endpoint Encryption, funkcja Zapobieganie utracie danych może automatycznie szyfrować pliki przed zezwoleniem użytkownikowi na ich przekazanie do innej lokalizacji. Jeśli składnik Szyfrowanie punktu końcowego nie jest zainstalowany, funkcja Zapobieganie utracie danych wykonuje na plikach operację Blokuj. Wybierz jeden z następujących kluczy szyfrowania lub stałe hasło: • **Klucz użytkownika**: Zwany także **kluczem lokalnym**, jest unikatowy dla każdego użytkownika i pozwala na dostęp do zaszyfrowanego pliku tylko użytkownikowi, który utworzył ten plik. • **Klucz wspólny**: Klucz ten to **klucz grupowy** lub **klucz korporacyjny**, konfigurowany przez administratora składnika Endpoint Encryption z użyciem konsoli MMC serwera PolicyServer. • **Stałe hasło**: Użytkownicy ręcznie podają stałe hasło z użyciem monitu ekranowego. Składnik Szyfrowanie punktu końcowego tworzy pakiet samorozpakowujący się, do którego użytkownicy uzyskują dostęp na każdym punkcie końcowym po podaniu hasła deszyfrowania. **Ważne** • Aby możliwe było szyfrowanie danych, na docelowym punkcie końcowym musi być zainstalowany składnik Szyfrowanie punktu, na którym użytkownik musi się zalogować. • Zaszyfrowane pliki na urządzeniach USB są poddawane skanowaniu funkcji Zapobieganie utracie danych, kiedy użytkownicy próbują odszyfrować pliki. Odszyfrowanie plików zawierających wrażliwe dane na urządzeniu USB powoduje wywołanie protokołu szyfrowania USB, przez co system wymaga ponownego zaszyfrowania wrażliwych danych. Aby zapobiec próbom ponownego szyfrowania danych przez program OfficeScan, należy przenieść zaszyfrowane pliki na dysk lokalny przed podjęciem próby dostępu do danych. • Zapobieganie utracie danych blokuje próby przekazania plików do cloud storage przy korzystaniu z klienta sieci Web. Przed przekazaniem plików z użyciem klienta sieci

Operacja	Opis
Usprawiedliwienie użytkownika **Uwaga** Ta opcja jest dostępna wyłącznie po wybraniu operacji **Blokuj**.	Funkcja Zapobieganie utracie danych monituje użytkownika przed wykonaniem operacji “Blokuj”. Użytkownik może pominąć operację “Blokuj”, podając wyjaśnienie, dlaczego przesłanie poufnych danych jest bezpieczne. Dostępne przyczyny usprawiedliwienia to: • **To jest część normalnego procesu biznesowego.** • **Mój przełożony zatwierdził transfer danych.** • **Dane w tym pliku nie są poufne.** • **Inna**: Użytkownicy podają alternatywne wyjaśnienie w przedstawionym polu tekstowym.

Wyjątki funkcji Zapobieganie utracie danych

Wyjątki DLP są stosowane do całej reguły, włącznie ze zdefiniowanymi w niej regułami. Funkcja Zapobieganie utracie danych stosuje ustawienia wyjątków do wszystkich transmisji przed rozpoczęciem skanowania zasobów cyfrowych. Jeśli transmisja jest zgodna z jedną z reguł wyjątków, Funkcja Zapobieganie utracie danych natychmiast dopuszcza transmisję lub skanuje ją w zależności od typu wyjątku.

Definiowanie monitorowanych i niemonitorowanych miejsc docelowych

Zdefiniuj monitorowane i niemonitorowane miejsca docelowe na podstawie zakresu transmisji skonfigurowanego na karcie **Kanał**. Szczegółowe informacje o sposobie definiowania monitorowanych i niemonitorowanych miejsce docelowych dla ustawienia **Wszystkie transmisje** zawiera sekcja *Zakres transmisji: Wszystkie transmisje na stronie 11-31*. Szczegółowe informacje o sposobie definiowania monitorowanych i niemonitorowanych miejsce docelowych dla ustawienia **Tylko transmisje poza siecią lokalną (LAN)** zawiera sekcja *Zakres transmisji: Tylko transmisje poza siecią lokalną (LAN) na stronie 11-33*.

Podczas definiowania monitorowanych i niemonitorowanych miejsc docelowych należy postępować zgodnie z poniższymi wytycznymi:

1. Zdefiniuj każde miejsce docelowe za pomocą:
   - Adres IP
   - Nazwa hosta
   - FQDN
   - Adres sieciowy i maska podsieci, na przykład 10.1.1.1/32

   Uwaga

   W przypadku maski podsieci funkcja Zapobieganie utracie danych obsługuje tylko porty CIDR. Oznacza to, że można tylko wpisać liczbę taką jak np. 32 zamiast ciągu 255.255.255.0.

2. Aby wskazać poszczególne kanały, dołącz domyślne lub sprecyzowane przez firmę numery portów dla tych kanałów. Np. port 21 jest zazwyczaj przeznaczony do obsługi ruchu FTP, port 80 – do HTTP, a port 443 – do HTTPS. Użyj średnika, aby oddzielić miejsce docelowe od numerów portów.
3. Możesz także dołączyć zakresy portów. Aby uwzględnić wszystkie porty, należy zignorować zakres portów.

   Przykłady miejsc docelowych z numerami portów i zakresami portów:
   - 10.1.1.1:80
   - host:5-20
   - host.domena.com:20
   - 10.1.1.1/32:20
4. Poszczególne miejsca docelowe należy rozdzielać przecinkami.

Reguły rozpakowywania

Pliki znajdujące się w skompresowanych archiwach można skanować pod kątem obecności zasobów cyfrowych. Aby określić pliki do skanowania, skompresowane pliki są sprawdzane przez funkcję Zapobieganie utracie danych za pomocą następujących reguł:

- **Rozmiar rozpakowanego pliku przekracza: __ MB (1-512 MB)**
- **Liczba warstw kompresji przekracza: __ (1-20)**
- **Liczba plików do skanowania przekracza: __ (1-2000)**

Zasada 1: Maksymalny rozmiar rozpakowanego pliku

Skompresowany plik - po rozpakowaniu - musi być zgodny z określonym limitem.

Przykład: wybrano limit 20 MB.

Scenariusz 1: jeśli rozmiar pliku `archive.zip` po rozpakowaniu wynosi 30 MB, żaden z plików znajdujących się w pliku `archive.zip` nie będzie skanowany. Pozostałe dwie reguły nie są już sprawdzane.

Scenariusz 2: rozmiar pliku `my_archive.zip` po rozpakowaniu wynosi 10 MB:

- Jeśli plik `my_archive.zip` nie zawiera plików skompresowanych, program OfficeScan pomija regułę 2 i przechodzi do reguły 3.
- Jeśli plik `my_archive.zip` zawiera pliki skompresowane, rozmiar wszystkich rozpakowanych plików musi się zawierać w określonym limicie. Przykładowo: jeśli plik `my_archive.zip` zawiera pliki `AAA.rar`, `BBB.zip` i `EEE.zip`, a plik `EEE.zip` zawiera plik `222.zip`:

`my_archive.zip`			= 10 MB po rozpakowaniu
	`\AAA.rar`		= 25MB po rozpakowaniu
	`\BBB.zip`		= 3MB po rozpakowaniu
	`\EEE.zip`		= 1MB po rozpakowaniu
		`\222.zip`	= 2MB po rozpakowaniu

Pliki `my_archive.zip`, `BBB.zip`, `EEE.zip`, and `222.zip` zostaną sprawdzone przez regułę 2, ponieważ łączy rozmiar tych plików zawiera się w limicie 20 MB. Plik `AAA.rar` zostanie pominięty.

Zasada 2: Maksymalna liczba warstw kompresji

Pliki odpowiadające określonej liczbie warstw zostaną oznaczone do skanowania.

Na przykład:

```
my_archive.zip
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
                                        \222.zip            \333.txt
```

Jeśli wybrany zostanie limit wynoszący dwie warstwy:

- Program OfficeScan zignoruje plik `333.txt`, ponieważ znajduje się on w trzeciej warstwie.
- Program OfficeScan oznaczy następujące pliki do skanowania, a następnie sprawdzi regułę 3:
  - `DDD.txt` (w pierwszej warstwie)
  - `CCC.xls` (w drugiej warstwie)
  - `111.pdf` (w drugiej warstwie)

Zasada 3: Maksymalna liczba plików do skanowania

Program OfficeScan skanuje pliki do określonego limitu. Program OfficeScan skanuje pliki i foldery w kolejności numerycznej i alfabetycznej.

Korzystając z przykładu dla reguły 2: program OfficeScan oznaczył do skanowania następujące wyróżnione pliki:

```
my_archive.zip
                    \BBB.zip            \CCC.xls
```

```
                    \DDD.txt

                    \EEE.zip            \111.pdf

                                        \222.zip            \333.txt
```

Dodatkowo plik `my_archive.zip` zawiera folder o nazwie `7Folder`, który nie został sprawdzony przez regułę 2. Ten folder zawiera pliki `FFF.doc` i `.GGG.ppt`. Aktualnie przeznaczonych do skanowania jest 5 plików, jak przedstawiono poniżej:

```
my_archive.zip

                    \7Folder            \FFF.doc

                    \7Folder            \GGG.ppt

                    \BBB.zip            \CCC.xls

                    \DDD.txt

                    \EEE.zip            \111.pdf

                                        \222.zip            \333.txt
```

Jeśli wybrany zostanie limit wynoszący 4 pliki, to następujące pliki zostaną przeskanowane:

- `FFF.doc`
- `GGG.ppt`
- `CCC.xls`
- `DDD.txt`

Uwaga

Dla plików które zawierają pliki osadzone, program OfficeScan wyodrębnia zawartość plików osadzonych.

Jeśli zawartość wyodrębniona jest tekstem, plik host (np. `123.doc`) i pliki osadzone (np. `abc.txt` lub `xyz.xls`) są liczone jako jeden plik.

Jeśli zawartość wyodrębniona nie jest tekstem, plik host (np. `123.doc`) i pliki osadzone (np. `abc.exe`) są liczone oddzielnie.

Wydarzenia uruchamiające reguły rozpakowywania

Następujące zdarzenia uruchamiają reguły rozpakowywania:

TABELA 11-6. Wydarzenia uruchamiające reguły rozpakowywania

Skompresowany plik przeznaczony do przekazania odpowiada regule i operacją dla skompresowanego pliku jest Pomiń (transmisja pliku jest wykonywana).	Przykładowo: aby monitorować pliki ZIP przekazywane przez użytkowników, zdefiniowano atrybut pliku (. ZIP), dodano go do szablonu, szablon użyto w regule, a następnie ustawiono operację **Pomiń**. **Uwaga** Jeżeli wybrano operację Zablokuj, cały skompresowany plik nie jest przekazywany, a zatem nie ma potrzeby skanowania plików w nim zawartych.
Skompresowany plik przeznaczony do przekazania nie odpowiada regule.	W tym przypadku program OfficeScan będzie nadal rozpakowywał pliki w celu określenia, który z plików zawartych w archiwum powinien zostać przeskanowany do zasobów cyfrowych i czy wykonać przekazanie całego pliku skompresowanego.

Oba zdarzenia mają ten sam wynik. Gdy program OfficeScan napotka plik skompresowany:

- Jeśli reguła 1 nie jest spełniona, program OfficeScan pozwala na przekazanie całego skompresowanego pliku.
- Jeśli zasada 1 jest spełniona, sprawdzane są dwie pozostałe. Program OfficeScan pozwala na przekazanie całego skompresowanego pliku, jeśli:
  - Wszystkie przeskanowane pliki nie pasują do reguły.
  - Wszystkie przeskanowane pliki pasują do reguły, a operacją jest **Pomiń**.

    Przekazanie całego skompresowanego pliku jest blokowane, jeżeli przynajmniej jeden przeskanowany plik pasuje do reguły, a operacją jest **Blokuj**.

Konfiguracja reguł Zapobieganie utracie danych

Tworzenie reguł Zapobieganie utracie danych można rozpocząć po skonfigurowaniu identyfikatorów danych i umieszczeniu ich w szablonach.

Oprócz identyfikatorów danych i szablonów, podczas tworzenia reguł należy skonfigurować kanały i operacje. Szczegółowe informacje o regułach zawiera temat *Reguły Zapobieganie utracie danych na stronie 11-3*.

Tworzenie reguły Zapobieganie utracie danych

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Ustawienia DLP**.
4. Kliknij kartę **Agenci zewnętrzni**, aby skonfigurować regułę dla agentów zewnętrznych, lub kartę **Agenci wewnętrzni**, aby skonfigurować regułę dla agentów wewnętrznych.

Uwaga

Skonfiguruj ustawienia lokalizacji agenta, jeśli nie zostało to jeszcze zrobione. Agenci używają tych ustawień lokalizacji w celu określenia prawidłowej reguły Zapobieganie utracie danych do zastosowania. Szczegółowe informacje zawiera sekcja *Lokalizacja punktu końcowego na stronie 15-2*.

5. Wybierz **Włącz Zapobieganie utracie danych**.

6. Wybierz jedną z następujących wartości:

   - Jeśli wyświetlana jest karta **Agenci zewnętrzni**, można zastosować ustawienia Zapobieganie utracie danych do agentów wewnętrznych, wybierając opcję **Zastosuj wszystkie ustawienia do agentów wewnętrznych**.

   - Jeśli wyświetlana jest karta **Agenci wewnętrzni**, można zastosować ustawienia Zapobieganie utracie danych do agentów zewnętrznych, wybierając opcję **Zastosuj wszystkie ustawienia do agentów zewnętrznych**.

7. Na karcie **Reguły** kliknij opcję **Dodaj**.

   Reguła może zawierać do 40 reguł.

8. Skonfiguruj ustawienia reguły.

   Szczegółowe informacje o tworzeniu reguł DLP zawarto w temacie *Tworzenie reguł Zapobieganie utracie danych na stronie 11-52*.

9. Kliknij kartę **Wyjątki** i skonfiguruj wymagane ustawienia wyjątków.

   Szczegółowe informacje o dostępnych ustawieniach wyjątków zawiera sekcja *Wyjątki funkcji Zapobieganie utracie danych na stronie 11-44*.

10. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

    - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.

- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Tworzenie reguł Zapobieganie utracie danych

Uwaga

Funkcja Zapobieganie utracie danych przetwarza reguły i szablony według priorytetu. Jeśli reguła jest ustawiona na operację "Pomiń", funkcja Zapobieganie utracie danych przetwarza następną regułę na liście. Jeśli reguła jest ustawiona na operację "Blokuj" lub "Usprawiedliwienie użytkownika", funkcja Zapobieganie utracie danych blokuje lub akceptuje działanie użytkownika i nie przetwarza dalej danej reguły/szablonu.

Procedura

1. Wybierz opcję **Włącz tę regułę**.
2. Podaj nazwę reguły.

   Skonfiguruj ustawienia szablonu:
3. Kliknij kartę **Szablon**.
4. Wybierz szablony z listy **Dostępne szablony** i kliknij przycisk **Dodaj**.

   Podczas wybierania szablonów:

   - Aby wybrać wiele pozycji, kliknij nazwy szablonów, co spowoduje podświetlenie nazwy.
   - Użyj funkcji wyszukiwania, aby znaleźć określony szablon. Można wpisać pełną lub częściową nazwę szablonu.

   Uwaga

   Każda reguła może zawierać maksymalnie 200 szablonów.
5. Jeśli preferowany szablon nie został znaleziony na liście **Dostępne szablony**:

a. Kliknąć przycisk **Dodaj nowy szablon**.

Zostanie wyświetlony ekran **Szablony Zapobieganie utracie danych**.

Instrukcje dotyczące dodawania szablonów na ekranie **Szablony Zapobieganie utracie danych** zawiera temat *Szablony Zapobieganie utracie danych na stronie 11-21*.

b. Po utworzeniu szablonu wybierz go, a następnie kliknij przycisk **Dodaj**.

Uwaga

Podczas sprawdzania szablonów program OfficeScan używa reguły „pierwsze dopasowanie". Oznacza to, że jeśli plik lub dane pasują do definicji w szablonie, program OfficeScan nie będzie już sprawdzić innych szablonów. Priorytet zależy od kolejności szablonów na liście.

Skonfiguruj ustawienia kanału:

6. Kliknij kartę **Kanał**.

7. Wybierz kanały dla reguły.

Szczegółowe informacje na temat kanałów zawierają sekcje *Kanały sieciowe na stronie 11-26* i *Kanały systemu i aplikacji na stronie 11-34*.

8. Jeśli wybrano dowolny z kanałów sieciowych, wybierz zakres transmisji:

- **Wszystkie transmisje**
- **Tylko transmisje poza siecią lokalną (LAN)**

Szczegółowe informacje o zakresie transmisji, działaniu miejsc docelowych w zależności od zakresu transmisji i prawidłowym definiowaniu miejsc docelowych zawarto w temacie *Zakres transmisji i cele kanałów sieciowych na stronie 11-31*.

9. W przypadku wybrania opcji **Klienty e-mail**:

a. Kliknij pozycję **Wyjątki**.

b. Określ monitorowane i niemonitorowane wewnętrzne domeny e-mail.

Szczegółowe informacje na temat monitorowanych i niemonitorowanych domen e-mail zawarto w temacie *Klienci e-mail na stronie 11-27*.

10. W przypadku wybrania opcji **Magazyn wymienny**:

    a. Kliknij pozycję **Wyjątki**.

    b. Dodaj niemonitorowane wymienne urządzenia pamięci masowej, określając je wg producentów. Model i numer seryjny urządzenia są opcjonalne.

       Lista dozwolonych urządzeń USB pozwala na używanie gwiazdki (*) jako symbolu wieloznacznego. W celu włączenia wszystkich urządzeń, które spełniają pozostałe pola, zastąp wszystkie pola z gwiazdką (*).

       Na przykład ciąg [producent]-[model]-* dopuszcza wszystkie urządzenia określonego producenta i typu modelu niezależnie od numeru seryjnego

    c. Aby dodać więcej urządzeń, kliknij ikonę plus (+).

Porada

Użyj narzędzia Lista urządzeń w celu wyszukania urządzeń podłączonych do punktów końcowych. Narzędzie dostarcza informacje o producencie, modelu i numerze seryjnym każdego urządzenia. Szczegółowe informacje zawiera sekcja *Narzędzie Lista urządzeń na stronie 10-14*.

Skonfiguruj ustawienia operacji:

11. Kliknij kartę **Operacja**.

12. Wybierz operację podstawową i operacje dodatkowe.

Szczegółowe informacje na temat operacji zawiera sekcja *Czynności Zapobieganie utracie danych na stronie 11-41*.

Uwaga

Funkcja Zapobieganie utracie danych obsługuje szyfrowanie tylko poufnych danych zawartych na wymiennych urządzeniach pamięci masowej i w cloud storage services. Funkcja Zapobieganie utracie danych wykonuje operację "Zezwól" bez szyfrowania na wszystkich kanałach, które nie obsługują szyfrowania. Aby możliwe było szyfrowanie danych, na docelowym punkcie końcowym musi być zainstalowany składnik Szyfrowanie punktu, na którym użytkownik musi się zalogować.

13. Po skonfigurowaniu ustawień **Szablon**, **Kanał** i **Operacja** kliknij przycisk **Zapisz**.

Importowanie, eksportowanie i kopiowanie reguł DLP

Administratorzy mogą zaimportować wcześniej zdefiniowane reguły (zawarte w poprawnie sformatowanym pliku `.dat`) lub wyeksportować listę skonfigurowanych reguł DLP. Skopiowanie reguły DLP umożliwia administratorowi zmodyfikowanie zawartości wcześniej zdefiniowanej reguły, co oszczędza czas.

W poniższej tabeli przedstawiono sposób działania każdej funkcji.

TABELA 11-7. Funkcje importowania, eksportowania i kopiowania reguł DLP

FUNKCJA	OPIS
Importuj	Zaimportowanie listy reguł powoduje dołączenie nieistniejących reguł do listy istniejących reguł DLP. Funkcja Zapobieganie utracie danych pomija reguły, które już istnieją na liście docelowej. Funkcja Zapobieganie utracie danych zachowuje wszystkie wcześniej skonfigurowane ustawienia każdej reguły, włącznie ze stanem włączenia lub wyłączenia.
Eksportuj	Eksportowanie listy zasad powoduje wyeksportowanie całej listy do pliku `.dat`, którą administratorzy mogą następnie zaimportować i wdrożyć dla innych domen lub agentów. Funkcja Zapobieganie utracie danych zapisuje ustawienia wszystkich reguł na podstawie bieżącej konfiguracji. **Uwaga** • Administratorzy muszą zapisać lub zastosować wszystkie nowe albo zmodyfikowane reguły przed wyeksportowaniem listy. • Funkcja Zapobieganie utracie danych nie eksportuje żadnych wyjątków skonfigurowanych dla reguł, a jedynie ustawienia skonfigurowane dla wszystkich reguł.

FUNKCJA	OPIS
Kopiuj	Skopiowanie reguły powoduje utworzenie dokładnej repliki bieżących ustawień konfiguracji dla reguły. Administratorzy muszą wpisać nową nazwę reguły, a następnie mogą dokonać wszelkich zmian w konfiguracji, jakie są wymagane dla nowej reguły.

Powiadomienia dotyczące Zapobieganie utracie danych

Program OfficeScan zawiera zestaw domyślnych powiadomień informujących administratorów programu OfficeScan i użytkowników agentów o transmisji zasobów cyfrowych.

Szczegółowe informacje o powiadomieniach wysyłanych do administratorów zawiera temat *Powiadomienia dotyczące Zapobieganie utracie danych dla administratorów na stronie 11-56*.

Szczegółowe informacje o powiadomieniach wysyłanych do użytkowników agentów zawiera sekcja *Powiadomienia dotyczące Zapobieganie utracie danych dla użytkowników agentów na stronie 11-60*.

Powiadomienia dotyczące Zapobieganie utracie danych dla administratorów

Program OfficeScan można skonfigurować w celu wysyłania do administratorów powiadomienia po wykryciu transmisji zasobów cyfrowych lub tylko po zablokowaniu transmisji.

Program OfficeScan zawiera zestaw domyślnych powiadomień programu informujących administratorów o transmisji zasobów cyfrowych. Możesz zmodyfikować powiadomienia i skonfigurować dodatkowe ustawienia powiadamiania zgodnie z potrzebami.

Uwaga

Program OfficeScan może wysyłać powiadomienia za pomocą poczty elektronicznej, pułapki SNMP i dzienników zdarzeń systemu Windows NT. Ustawienia należy skonfigurować, jeśli program OfficeScan wysyła powiadomienia za pomocą tych kanałów. Szczegółowe informacje zawiera sekcja *Ustawienia powiadamiania administratorów na stronie 14-37*.

Konfiguracja powiadamiania dotyczącego Zapobieganie utracie danych dla administratorów

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Administrator**.
2. Na karcie **Kryteria**:
   a. Przejdź do sekcji **Transmisje zasobów cyfrowych**.
   b. Określ, czy powiadomienia mają być wysyłane po wykryciu transmisji zasobów cyfrowych (transmisja może być dozwolona albo zablokowana) lub tylko po zablokowaniu transmisji.
3. Na karcie **Poczta elektroniczna**:
   a. Przejdź do sekcji **Transmisje zasobów cyfrowych**.
   b. Wybierz opcję **Włącz powiadamianie za pomocą wiadomości e-mail**.
   c. Wybierz opcję **Wyślij powiadomienia do użytkowników z uprawnieniami do domeny drzewa agentów**.

      Administracja oparta na rolach umożliwia przyznanie użytkownikom uprawnień do domeny drzewa agentów. Jeżeli nastąpi transmisja na dowolnym agencie należącym do określonej domeny, zostaną wysłane wiadomości na adresy e-mail użytkowników z uprawnieniami do domeny. Przykłady znajdują się w poniższej tabeli:

TABELA 11-8. Domeny i uprawnienia w drzewie agentów

DOMENA DRZEWA AGENTÓW	ROLE Z UPRAWNIENIAMI DO DOMENY	KONTO UŻYTKOWNIKA Z ROLĄ	ADRES E-MAIL DLA KONTA UŻYTKOWNIKA
Domena A	Administrator (wbudowany)	konto główne	mary@xyz.com
	Rola_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domena B	Administrator (wbudowany)	konto główne	mary@xyz.com
	Rola_02	admin_jane	jane@xyz.com

Jeśli Agent OfficeScan należący do Domeny A wykryje transmisję zasobów cyfrowych, wiadomość e-mail zostanie wysłana na adresy mary@xyz.com, john@xyz.com i chris@xyz.com.

Jeśli transmisję wykryje Agent OfficeScan należący do Domeny B, wiadomość e-mail zostanie wysłana na adresy mary@xyz.com i jane@xyz.com.

Uwaga

Po włączeniu tej opcji, wszyscy użytkownicy z uprawnieniami do domeny muszą mieć odpowiedni adres e-mail. Powiadomienie e-mail nie zostanie wysłane do użytkowników bez adresu e-mail. Użytkowników i adresy e-mail można skonfigurować na ekranie **Administracja** > **Zarządzanie kontami** > **Konta użytkowników**.

d. Wybierz opcję **Wysyłaj powiadomienia na następujące adresy e-mail** i wpisz adresy e-mail.

e. Zaakceptuj lub zmień domyślny temat i wiadomość. Do przedstawienia danych w polach **Temat** i **Wiadomość**.

TABELA 11-9. Zmienne w powiadomieniach dotyczących Zapobieganie utracie danych

ZMIENNA	OPIS
%USER%	Użytkownik zalogowany na punkcie końcowym, na którym wykryto transmisję
%COMPUTER%	Punkt końcowy, na którym wykryto transmisję
%DOMAIN%	Domena punktu końcowego
%DATETIME%	Data i godzina wykrycia transmisji
%CHANNEL%	Kanał, na którym wykryto transmisję
%TEMPLATE%	Szablon zasobów cyfrowych, który wywołał wykrywanie
%RULE%	Nazwa reguły, które wywołała wykrycie **Uwaga** Aby wyświetlić nazwę reguły w wiadomości, dodaj tę zmienną w polu **Wiadomość**.

4. Na karcie **Pułapka SNMP**:

   a. Przejdź do sekcji **Transmisje zasobów cyfrowych**.

   b. Wybierz opcję **Włącz powiadamianie przez pułapkę SNMP**.

   c. Zaakceptuj lub zmień domyślną wiadomość. Do przedstawienia danych w polu **Wiadomość**. Szczegółowe informacje można znaleźć w części *Tabela 11-9: Zmienne w powiadomieniach dotyczących Zapobieganie utracie danych na stronie 11-59*.

5. Na karcie **Dziennik zdarzeń Windows NT**:

   a. Przejdź do sekcji **Transmisje zasobów cyfrowych**.

   b. Wybierz opcję **Włącz powiadamianie przez rejestr zdarzeń NT**.

   c. Zaakceptuj lub zmień domyślną wiadomość. Dane w polu **Wiadomość** można przedstawiać za pomocą znaczników. Szczegółowe informacje można

znaleźć w części *Tabela 11-9: Zmienne w powiadomieniach dotyczących Zapobieganie utracie danych na stronie 11-59*.

6. Kliknij przycisk **Zapisz**.

Powiadomienia dotyczące Zapobieganie utracie danych dla użytkowników agentów

Program OfficeScan może wyświetlać powiadomienia na komputerach agentów natychmiast po dozwoleniu lub zablokowaniu transmisji zasobów cyfrowych.

Aby powiadamiać użytkowników o dozwoleniu lub zablokowaniu transmisji zasobów cyfrowych, wybierz opcję **Powiadom użytkownika agenta** podczas tworzenia reguły funkcji Zapobieganie utracie danych. Instrukcje dotyczące tworzenia reguły zawiera temat *Konfiguracja reguł Zapobieganie utracie danych na stronie 11-50*.

Konfiguracja powiadamiania dotyczącego Zapobieganie utracie danych dla agentów

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Agent**.
2. Na liście rozwijanej **Typ** wybierz opcję **Transmisje zasobów cyfrowych**.
3. Zaakceptuj lub zmień domyślną wiadomość.
4. Kliknij przycisk **Zapisz**.

Dzienniki Zapobieganie utracie danych

Agenci rejestrują transmisje zasobów cyfrowych (zablokowane i dozwolone transmisje) i natychmiast wysyłają dzienniki na serwer. Jeśli agent nie może wysłać dzienników, ponawia próbę po 5 minutach.

Aby dzienniki nie zajmowały zbyt dużo miejsca na dysku twardym, można je ręcznie usunąć lub skonfigurować harmonogram ich usuwania. Dodatkowe informacje dotyczące dzienników zarządzania zawiera sekcja *Zarządzanie dziennikiem na stronie 14-41*.

Wyświetlanie dzienników Zapobieganie utracie danych

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami** lub **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, albo wybierz określone domeny lub agentów.
3. Kliknij **Dzienniki** > **Dzienniki Zapobieganie utracie danych** lub **Wyświetl dzienniki** > **Dzienniki Zapobieganie utracie danych**.
4. Określ kryteria dziennika i kliknij przycisk **Wyświetl dzienniki**.
5. Wyświetl dzienniki.

   Dziennik zawiera następujące informacje:

TABELA 11-10. Informacje dziennika Zapobieganie utracie danych

KOLUMNA	OPIS
Data i godzina	Data i godzina zarejestrowania zdarzenia przez funkcję Zapobieganie utracie danych
Użytkownik	Nazwa użytkownika zalogowanego na punkcie końcowym
Punkt końcowy	Nazwa punktu końcowego, na którym funkcja Zapobieganie utracie danych wykryła transmisję
Domena	Domena punktu końcowego
IP	Adres IP punktu końcowego

KOLUMNA	OPIS
Nazwa reguły	Nazwy reguły, które wywołały zdarzenie **Uwaga** Reguły utworzone w poprzedniej wersji programu OfficeScan wyświetlają domyślnie nazwę LEGACY_DLP_Policy.
Kanał	Kanał, na którym nastąpiła transmisja
Proces	Proces, który umożliwił transmisję zasobu cyfrowego (proces zależny od kanału) Szczegółowe informacje zawiera sekcja *Procesy według kanału na stronie 11-62*.
Źródło	Źródło pliku zawierającego zasób cyfrowy lub kanał (jeśli źródło jest niedostępne)
Przeznaczenie	Wybrane miejsce docelowe pliku zawierającego zasób cyfrowy lub kanał (jeśli źródło jest niedostępne)
Operacja	Operacja dokonana dla transmisji
Szczegóły	Łącze zawierające dodatkowe szczegóły dotyczące transmisji Szczegółowe informacje zawiera sekcja *Dane szczegółowe dziennika Zapobieganie utracie danych na stronie 11-65*.

6. Aby zapisać dzienniki w formacie CSV (plik z tekstem oddzielanym przecinkami), kliknij opcję **Eksportuj do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Procesy według kanału

Poniższa tabela zawiera procesy wyświetlane w kolumnie **Proces** w dziennikach funkcji Zapobieganie utracie danych.

TABELA 11-11. Procesy według kanału

KANAŁ	PROCES
Oprogramowanie do synchronizacji (ActiveSync)	Pełna ścieżka i nazwa procesu oprogramowania do synchronizacji Przykład: `C:\Windows\system32\WUDFHost.exe`
Rejestrator danych (CD/DVD)	Pełna ścieżka i nazwa procesu rejestratora danych Przykład: `C:\Windows\Explorer.exe`
Schowek systemu Windows	Nie dotyczy
Klient wiadomości e-mail: Lotus Notes	Pełna ścieżka i nazwa procesu dla programu Lotus Notes Przykład: `C:\Program Files\IBM\Lotus\Notes\nlnotes.exe`
Klient wiadomości e-mail: Microsoft Outlook	Pełna ścieżka i nazwa procesu dla programu Microsoft Outlook Przykład: `C:\Program Files\Microsoft Office\Office12\OUTLOOK.EXE`
Wiadomości e-mail: wszystkie klienty używające protokołu SMTP	Pełna ścieżka i nazwa procesu dla klienta wiadomości e-mail Przykład: `C:\Program Files\Mozilla Thunderbird\thunderbird.exe`
Magazyn wymienny	Nazwa procesu aplikacji, która przesłała dane na urządzenie pamięci masowej lub w jego obrębie Przykład: `explorer.exe`
FTP	Pełna ścieżka i nazwa procesu dla klienta FTP Przykład: `D:\Program Files\FileZilla FTP Client\filezilla.exe`

Kanał	Proces
HTTP	„Aplikacja HTTP”
HTTPS	Pełna ścieżka i nazwa procesu przeglądarki lub aplikacji Przykład: `C:\Program Files\Internet Explorer\iexplore.exe`
Aplikacja do wiadomości błyskawicznych	Pełna ścieżka i nazwa procesu aplikacji do wiadomości błyskawicznych Przykład: `C:\Program Files\Skype\Phone\Skype.exe`
Aplikacja do wiadomości błyskawicznych: MSN	• Pełna ścieżka i nazwa procesu dla programu MSN Przykład: `C:\Program Files\Windows Live\Messenger\ msnmsgr.exe` • „Aplikacja HTTP”, jeśli dane są przesyłane z poziomu okna rozmowy
Aplikacja peer-to-peer	Pełna ścieżka i nazwa procesu aplikacji peer-to-peer Przykład: `D:\Program Files\BitTorrent\bittorrent.exe`
Szyfrowanie PGP	Pełna ścieżka i nazwa procesu oprogramowania do szyfrowania PGP Przykład: `C:\Program Files\PGP Corporation\PGP Desktop\ PGPmnApp.exe`
Drukarka	Pełna ścieżka i nazwa procesu aplikacji, która zainicjowała operację drukarki Przykład: `C:\Program Files\Microsoft Office\Office12\ WINWORD.EXE`

Kanał	Proces
Protokół SMB	Pełna ścieżka i nazwa procesu aplikacji, z której uzyskano dostęp do udostępnianego pliku (kopiowanie lub tworzenie nowego pliku) Przykład: `C:\Windows\Explorer.exe`
Poczta przez sieć Web (tryb HTTP)	„Aplikacja HTTP”
Poczta przez sieć Web (tryb HTTPS)	Pełna ścieżka i nazwa procesu przeglądarki lub aplikacji Przykład: `C:\Program Files\Mozilla Firefox\firefox.exe`

Dane szczegółowe dziennika Zapobieganie utracie danych

Ekran **Dane szczegółowe dziennika Zapobieganie utracie danych** zawiera dodatkowe szczegóły dotyczące transmisji zasobów cyfrowych. Dane szczegółowe transmisji różnią się w zależności od kanału i procesu, przy użyciu których program OfficeScan wykrył zdarzenie.

Poniższa tabela zawiera wyświetlane szczegóły.

Tabela 11-12. Dane szczegółowe dziennika Zapobieganie utracie danych

Szczegóły	Opis
Data i godzina	Data i godzina zarejestrowania zdarzenia przez funkcję Zapobieganie utracie danych
ID naruszenia	Unikatowy identyfikator zdarzenia
Użytkownik	Nazwa użytkownika zalogowanego na punkcie końcowym
Punkt końcowy	Nazwa punktu końcowego, na którym funkcja Zapobieganie utracie danych wykryła transmisję
Domena	Domena punktu końcowego
IP	Adres IP punktu końcowego

Szczegóły	Opis
Kanał	Kanał, na którym nastąpiła transmisja
Proces	Proces, który umożliwił transmisję zasobu cyfrowego (proces zależny od kanału) Szczegółowe informacje zawiera sekcja *Procesy według kanału na stronie 11-62*.
Źródło	Źródło pliku zawierającego zasób cyfrowy lub kanał (jeśli źródło jest niedostępne)
Nadawca wiadomości e-mail	Adres e-mail, z którego pochodzi transmisja
Temat wiadomości e-mail	Temat wiadomości e-mail zawierającej zasób cyfrowy
Odbiorca wiadomości e-mail	Docelowe adresy e-mail wiadomości e-mail
URL	Adres URL strony lub witryny Web
Użytkownik FTP	Nazwa użytkownika wprowadzona podczas logowania się na serwer FTP
Klasa pliku	Typ pliku, w którym funkcja Zapobieganie utracie danych wykryła zasób cyfrowy
Reguła/szablon	Lista dokładnych nazw reguł i szablonów, które wywołały wykrywanie **Uwaga** Każda reguła może zawierać wiele szablonów, które wywołały wykrywanie. Nazwy szablonów są oddzielone przecinkami.
Operacja	Operacja dokonana dla transmisji
Przyczyna usprawiedliwienia użytkownika	Podana przez użytkownika przyczyna kontynuacji przesyłania poufnych danych

Włączanie rejestracji w dzienniku diagnostycznym w module Ochrona danych

Procedura

1. Uzyskaj plik `logger.cfg` od dostawcy usług obsługi technicznej.
2. Dodaj następujące dane w kluczu `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite` (systemy 32-bitowe) lub `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\DlpLite` (systemy 64-bitowe):
   - **Typ**: `ciąg`
   - **Nazwa**: `debugcfg`
   - **Wartość**: `C:\Log\logger.cfg`
3. Utwórz folder o nazwie "Log" w katalogu `C:\`.
4. Skopiuj plik `logger.cfg` do folderu "Log".
5. Zastosuj ustawienia ochrony przed utratą danych oraz kontroli urządzeń z poziomu konsoli Web, aby rozpocząć pobieranie informacji dla dzienników.

Uwaga

Wyłącz rejestrowanie diagnostyki w module Ochrona danych, usuwając pozycję `debugcfg` z klucza rejestru i uruchamiając ponownie punkt końcowy.

Rozdział 12

Korzystanie z usług Web Reputation

W tym rozdziale przedstawiono zagrożenia internetowe i wykorzystanie programu OfficeScan do ochrony sieci i komputerów przed tymi zagrożeniami.

Rozdział składa się z następujących tematów:

Informacje o zagrożeniach internetowych

Wiele zagrożeń pochodzi z Internetu. Zagrożenia internetowe są skomplikowane oraz oparte na wielu plikach i technologiach. Nie jest to jeden plik ani jedna metoda. Na przykład twórcy zagrożeń internetowych wciąż zmieniają używane wersje lub odmiany. Ponieważ zagrożenie takie znajduje się w określonym miejscu w witrynie internetowej, a nie na zarażonym punkcie końcowym, twórca zagrożenia wciąż modyfikuje jego kod, aby uniknąć wykrycia.

W ostatnim czasie osoby, które kiedyś określano mianem hakerów, autorów wirusów, spamerów i autorów oprogramowania spyware, są obecnie nazywane przestępcami komputerowymi. Zagrożenia internetowe pomagają tym osobom realizować jeden z dwóch celów. Pierwszy cel to kradzież informacji w celu jej sprzedania. Następstwem takiego działania jest wyciek poufnych informacji, który należy traktować jako utratę tożsamości. Zarażony punkt końcowy może się również stać wektorem przeprowadzenia ataku typu phish lub realizacji innych operacji mających na celu przechwycenie danych. Zagrożenie tego typu może zmniejszyć skłonność użytkowników do realizacji transakcji w Internecie, ponieważ narusza wiarygodność witryn. Drugi cel przestępców komputerowych to przechwycenie zasobów komputera w celu wykorzystania ich do realizacji działań przynoszących zyski. Operacje takie jak wysyłanie spamu czy wymuszenie informacje są przeprowadzane w formie rozproszonych ataków typu „odmowa usługi" lub metod typu „pay-per-click".

Usługi ostrzegania kontaktu Command & Control

Usługi ostrzegania kontaktu Trend Micro Command & Control (C&C) zapewniają ulepszone możliwości wykrywania i ostrzegania w celu ograniczenia szkód powodowanych przez zaawansowane, trwałe zagrożenia i ukierunkowane ataki. Usługi ostrzegania kontaktu C&C są zintegrowane z usługami Web Reputation Services, które określają operację wykonywaną dla wykrytych adresów wywołań zwrotnych na podstawie poziomu zabezpieczeń usług Web Reputation.

Lista adresów IP C&C umożliwia dalsze zwiększenie liczby wykrytych wywołań zwrotnych C&C dzięki użyciu silnika kontroli zawartości sieciowej w celu identyfikacji kontaktów C&C w dowolnym kanale sieciowym.

Szczegółowe informacje na temat konfiguracji poziomu zabezpieczeń usługi Web Reputation Services zawiera sekcja *Konfiguracja usługi Reguła Web Reputation na stronie 12-6*.

TABELA 12-1. Funkcje usług ostrzegania kontaktu C&C

FUNKCJA	OPIS
Lista Global Intelligence	Infrastruktura Trend Micro Smart Protection Network kompiluje listę Global Intelligence na podstawie źródeł z całego świata, a następnie testuje i ocenia poziom zagrożenia każdego adresu wywołania zwrotnego C&C. Usługi Web Reputation Services używają listy Global Intelligence w połączeniu z ocenami reputacji złośliwych witryn internetowych w celu zapewnienia wyższego poziomu zabezpieczeń przed zaawansowanymi zagrożeniami. Poziom zabezpieczeń usług Web Reputation określa operację wykonywaną dla złośliwych witryn internetowych lub serwerów C&C na podstawie przypisanych poziomów ryzyka.
Lista Virtual Analyzer	serwery Smart Protection umożliwiają integrację z usługą Virtual Analyzer w celu uzyskania listy serwerów Virtual Analyzer C&C. Usługa Virtual Analyzer ocenia potencjalne zagrożenia w bezpiecznym środowisku, a następnie przypisuje poziom ryzyka do przeanalizowanych zagrożeń przy użyciu zaawansowanej heurystyki i metod testowania zachowania. Usługa Virtual Analyzer zapełnia listę Virtual Analyzer wszystkimi zagrożeniami, które podejmują próbę nawiązania połączenia z potencjalnym serwerem C&C. Lista Virtual Analyzer jest w dużym stopniu specyficzna dla firmy i zapewnia bardziej dostosowaną ochronę przed ukierunkowanymi atakami. Program OfficeScan pobiera listę z usługi Virtual Analyzer i może oceniać wszystkie możliwe zagrożenia C&C serwery Smart Protection pobierają listę z usługi Deep Discovery Advisor i mogą oceniać wszystkie możliwe zagrożenia C&C przy użyciu listy Global Intelligence i lokalnej listy Virtual Analyzer. Aby uzyskać szczegółowe informacje na temat list podjrzanych obiektów usługi Virtual Analyzer, patrz *Konfigurowanie ustawień listy podejrzanych obiektów na stronie 14-34*.

FUNKCJA	OPIS
Usługa podejrzanego połączenia	Usługa podejrzanego połączenia zarządza zdefiniowaną przez użytkownika listą adresów IP oraz globalną listą adresów IP C&C, a także monitoruje zachowanie połączeń nawiązywanych przez punkty końcowe z potencjalnymi serwerami C&C. Szczegółowe informacje zawiera sekcja *Usługa podejrzanego połączenia na stronie 8-5*.
Powiadomienia administratora	Administratorzy mogą włączyć odbieranie szczegółowych powiadomień z możliwością dostosowania w przypadku wykrycia wywołania zwrotnego C&C. Szczegółowe informacje zawiera sekcja *Konfigurowanie powiadomień o wywołaniach zwrotnych C&C dla administratorów na stronie 12-16*.
Powiadomienia agenta	Administratorzy mogą włączyć wysyłanie do użytkowników końcowych szczegółowych powiadomień z możliwością dostosowania w przypadku wykrycia wywołania zwrotnego C&C w punkcie końcowym. Szczegółowe informacje zawiera sekcja *Powiadomienia ostrzegania kontaktu C&C dla użytkowników agenta na stronie 12-19*.
Powiadomienia o przełamaniach	Administratorzy mogą dostosować powiadomienia o epidemiach dotyczące zdarzeń wywołania zwrotnego C&C oraz określić, czy epidemia występuje w jednym punkcie końcowym, czy w całej sieci. Szczegółowe informacje zawiera sekcja *Epidemie wywołań zwrotnych C&C na stronie 12-20*.
Dzienniki wywołań zwrotnych C&C	Dzienniki zapewniają szczegółowe informacje dotyczące wszystkich zdarzeń wywołania zwrotnego C&C. Szczegółowe informacje zawiera sekcja *Wyświetlanie dzienników wywołań zwrotnych C&C na stronie 12-24*.

Usługa Web Reputation

Technologia Web Reputation rejestruje informacje na temat wiarygodności domen internetowych, przypisując im ocenę reputacji na podstawie czynników takich jak czas działania witryny internetowej, historyczne zmiany jej lokalizacji oraz inne symptomy

podejrzanych działań wykryte za pomocą mechanizmów analizy zachowania złośliwego oprogramowania. Na podstawie zgromadzonych informacji skanuje witryny i blokuje użytkownikom dostęp do zarażonych lokalizacji.

Agenci OfficeScan wysyłają zapytania do źródeł programu Smart Protection w celu sprawdzenia reputacji witryn internetowych, do których użytkownik próbuje uzyskać dostęp. Reputacja witryny internetowej zależy od określonej reguły Web Reputation zastosowanej na punkcie końcowym. W zależności od używanej reguły agent Agent OfficeScan blokuje lub zezwala na dostęp do witryny internetowej.

Uwaga

Szczegółowe informacje o źródłach Smart Protection zawiera temat *Lista źródeł Smart Protection na stronie 4-23*.

Do listy zatwierdzonych lub zablokowanych adresów URL należy dodać adresy, które uważane są za bezpieczne lub niebezpieczne. Kiedy agent Agent OfficeScan wykryje próbę dostępu do takich witryn internetowych, automatycznie zezwala na dostęp lub blokuje go. Zapytanie do źródeł programu Smart Protection nie jest już wysyłane.

Reguły Web Reputation

Reguły usługi Web Reputation określają, czy program OfficeScan ma blokować dostęp do witryny sieci Web.

Reguły można skonfigurować dla agentów wewnętrznych i zewnętrznych. Administratorzy programu OfficeScan z reguły wprowadzają ściślejsze reguły dla agentów zewnętrznych.

Reguły to szczegółowe ustawienia w drzewie agentów OfficeScan. Można egzekwować określone reguły w celu zastosowania do grup agentów lub poszczególnych agentów. Można także zastosować jedną regułę do wszystkich agentów.

Po wdrożeniu reguł agenci używają kryteriów lokalizacji, które zostały ustawione na ekranie **Lokalizacja punktu końcowego** (patrz *Lokalizacja punktu końcowego na stronie 15-2*), aby określić swoją lokalizację i reguły do zastosowania. Agenci zmieniają reguły przy każdej zmianie lokalizacji.

Konfiguracja usługi Reguła Web Reputation

Jeśli w organizacji skonfigurowano serwer proxy obsługujący komunikację HTTP, a przed uzyskaniem dostępu do Internetu jest wymagane uwierzytelnianie, na tym ekranie należy określić poświadczenia uwierzytelniania serwera proxy.

Instrukcje dotyczące konfigurowania ustawień serwera proxy zawiera temat *Zewnętrzny serwer proxy dla agentów OfficeScan na stronie 15-53*.

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. Wybierz elementy docelowe w drzewie agentów.
   - Aby skonfigurować regułę dla agentów z systemem Windows, wybierz ikonę domeny głównej (), określone domeny lub agentów.

     Uwaga

     W przypadku wybrania domeny głównej lub konkretnych domen ustawienie zostanie zastosowane tylko do agenci działających w systemie Windows. Ustawienie nie zostanie zastosowane do agentów działających na dowolnej platformie Windows Server, nawet jeśli stanowią część domeny.
   - Aby skonfigurować regułę dla agentów działających na platformie Windows Server, wybierz określonego agenta.
3. Kliknij kolejno opcje **Ustawienia** > **Web Reputation Settings**.
4. Kliknij kartę **Agenci zewnętrzni**, aby skonfigurować regułę dla agentów zewnętrznych, lub kartę **Agenci wewnętrzni**, aby skonfigurować regułę dla agentów wewnętrznych.

Porada

Skonfiguruj ustawienia lokalizacji agenta, jeśli nie zostało to jeszcze zrobione. Agenci będą używać tych ustawień w celu określenia swojej lokalizacji i zastosowania właściwej reguły usługi Web Reputation. Szczegółowe informacje zawiera sekcja *Lokalizacja punktu końcowego na stronie 15-2*.

5. Wybierz opcję **Włącz reguły usługi Web Reputation w następujących systemach operacyjnych**.

   Systemy operacyjne wyświetlone na ekranie są zależne od elementów docelowych wybranych w kroku 1.

   Porada

   Firma Trend Micro zaleca wyłączenie usługi Web Reputation w przypadku agentów wewnętrznych, jeśli jest już używany produkt firmy Trend Micro obsługujący usługę Web Reputation (na przykład InterScan Web Security Virtual Appliance).

   Kiedy reguła usługi Web Reputation jest włączona:

   - Agenci zewnętrzni wysyłają zapytania usługi Web Reputation do sieci Smart Protection Network.
   - Agenci wewnętrzni wysyłają zapytania usługi Web Reputation do:
     - Używaj serwerów Smart Protection, jeśli włączona jest opcja **Wysyłaj zapytania do Serwer Smart Protection**. Aby uzyskać szczegółowe informacje na temat tej opcji, patrz krok 7.
     - Smart Protection Network, jeśli wyłączona jest opcja **Wysyłaj zapytania do Serwer Smart Protection**.

6. Wybierz opcję **Włącz tryb oceny**.

   Uwaga

   W trybie oceny agenci umożliwiają dostęp do wszystkich witryn internetowych, ale rejestrują dostęp do witryn internetowych, które zostałyby zablokowane, gdyby ocena była wyłączona. Firma Trend Micro stworzyła tryb oceny, aby użytkownik mógł najpierw ocenić witryny internetowe, a następnie podjąć działanie na podstawie dokonanej oceny. Na przykład można dodać bezpieczne witryny internetowe do listy dozwolonych witryn.

7. Wybierz **Sprawdź adresy URL HTTPS**.

   Komunikacja za pomocą protokołu HTTPS korzysta z certyfikatów w celu identyfikacji serwerów. Zapewnia to szyfrowanie danych i zapobiega kradzieży oraz

podsłuchiwaniu. Protokół HTTPS pozwala na bezpieczniejsze oglądanie witryn internetowych, jednak nie gwarantuje całkowitego bezpieczeństwa. Zaatakowane witryny mogą zawierać złośliwe informacje i kraść dane osobowe, nawet mimo prawidłowych certyfikatów. Ponadto certyfikaty są stosunkowo łatwe do uzyskania, dzięki czemu można łatwo skonfigurować zainfekowane serwery WWW, które używają protokołu HTTPS.

Należy włączyć sprawdzanie adresów URL protokołu HTTPS w celu zmniejszenia narażenia na działanie zaatakowanych i złośliwych witryn, które korzystają z protokołu HTTPS. Program OfficeScan monitoruje ruch HTTPS w następujących przeglądarkach:

TABELA 12-2. Obsługiwane przeglądarki dla ruchu HTTPS

PRZEGLĄDARKA	WERSJA
Microsoft Internet Explorer	• 8.x • 9.x • 10.x • 11.x
Mozilla Firefox	3.5 lub nowszy

Ważne

- Skanowanie za pomocą protokołu HTTPS obsługuje tylko platformy Windows 8, Windows 8.1, Windows 10 i Windows 2012 działające w trybie pulpitu.
- Po włączeniu skanowania HTTPS po raz pierwszy w programach Agenci OfficeScan użytkownicy muszą włączyć wymagany dodatek w przeglądarce, zanim będzie można wykonać skanowanie HTTPS.
  - Program Firefox

    W przypadku Agenci OfficeScan z systemem Windows 7, 8, 8.1, 10, Server 2008 R2 lub Server 2012 użytkownicy muszą włączyć dodatek `Trend Micro Osprey Firefox Extension 2.0.0.1077` w oknie wyskakującym przeglądarki (lub na ekranie **Dodatki** > **Rozszerzenia**).

    W przypadku Agenci OfficeScan z systemem Windows XP, Vista, Server 2003 lub Server 2008 użytkownicy muszą włączyć dodatek `Trend Micro NSC Firefox Extension 5.82.0.1092` w oknie wyskakującym przeglądarki (lub na ekranie **Dodatki** > **Rozszerzenia**).
  - Program Internet Explorer 9, 10 i 11

    W przypadku Agenci OfficeScan z systemem Windows 7, 8, 8.1, 10, Server 2008 R2 lub Server 2012 użytkownicy muszą włączyć dodatek `Trend Micro Osprey Plugin Class` w oknie wyskakującym przeglądarki.

    W przypadku Agenci OfficeScan z systemem Windows XP, Vista, Server 2003 lub Server 2008 użytkownicy muszą włączyć dodatek `TmIEPlugInBHO Class` w oknie wyskakującym przeglądarki.

  Dodatkowe informacje na temat konfigurowania ustawień programu Internet Explorer dla usługi Web Reputation zawierają następujące artykuły bazy wiedzy:

  - http://esupport.trendmicro.com/solution/en-us/1060643.aspx
  - http://esupport.trendmicro.com/solution/en-us/1095350.aspx

8. Wybierz opcję **Skanuj tylko często używane porty HTTP**, aby ograniczyć skanowanie ruchu przez usługę Web Reputation do portów 80, 81 i 8080. W domyślnej konfiguracji program OfficeScan skanuje ruch przesyłany przez wszystkie porty.

Uwaga

Nieobsługiwana w systemach Windows 7, 8, 8.1 i 10 ani Windows Server 2008 R2, 2012 i nowszych.

9. Wybierz opcję **Wysyłaj zapytania do serwerów Smart Protection**, aby agenci wewnętrzni wysyłali zapytania usługi Web Reputation do serwerów Smart Protection.

   - Jeśli włączysz to ustawienie:
     - Agenci odwołują się do listy źródeł Smart Protection w celu określenia serwerów Smart Protection, do których mają wysyłać zapytania.

       Aby uzyskać szczegółowe informacje o listach źródeł programu Smart Protection, patrz *Lista źródeł Smart Protection na stronie 4-23*.

     - Upewnij się, że serwery Smart Protection są dostępne. Jeśli wszystkie serwery Smart Protection są niedostępne, agenci nie wysyłają zapytań do sieci Smart Protection Network. Jedynymi pozostałymi źródłami danych o usłudze Web Reputation dla agentów są listy dozwolonych i zablokowanych adresów URL (skonfigurowane w kroku 10).
     - Jeśli chcesz, aby agenci łączyli się z serwerami Smart Protection przez serwer proxy, określ ustawienia serwera proxy na karcie **Administracja** > **Ustawienia** > **Serwer proxy > Wewnętrzny serwer proxy**.
     - Upewnij się, że serwery Smart Protection są regularnie aktualizowane, aby zachować bieżący poziom zabezpieczeń.
     - Agenci nie będą blokować niesprawdzonych stron internetowych. serwery Smart Protection nie przechowują danych o usłudze Web Reputation dla tych stron internetowych.
   - Jeśli wyłączysz to ustawienie:
     - Agenci wysyłają zapytania usługi Web Reputation do sieci Smart Protection Network. Aby wysyłać zapytania, punkty końcowe agentów muszą mieć połączenie z Internetem.
     - Jeśli połączenie z siecią Smart Protection Network wymaga uwierzytelniania na serwerze proxy, określ poświadczenia

uwierzytelniania w obszarze **Administracja** > **Ustawienia** > **Serwer proxy > Zewnętrzny serwer proxy (karta)** > **Połączenie agenta OfficeScan z serwerami Trend Micro**.

- Agenci będą blokować niesprawdzone strony internetowe, jeśli w kroku 11 zostanie wybrana opcja **Blokuj strony, które nie zostały przetestowane przez firmę Trend Micro**.

10. Wybierz jeden z dostępnych poziomów zabezpieczeń usługi Web Reputation: **Wysoki**, **Średni** lub **Niski**

Uwaga

Poziomy zabezpieczeń określają, czy program OfficeScan umożliwia dostęp do adresu URL czy go blokuje. Na przykład, jeśli zostanie ustawiony Niski poziom zabezpieczeń, program OfficeScan blokuje tylko adresy URL uznawane za zagrożenie internetowe. Podniesienie poziomu zabezpieczeń zwiększa nie tylko prawdopodobieństwo wykrycia zagrożenia internetowego, lecz również liczbę fałszywych alarmów.

11. Po wyłączeniu w kroku 9 opcji **Wyślij zapytania do Serwer Smart Protection** można wybrać opcję **Blokuj strony, które nie zostały przetestowane przez firmę Trend Micro**.

Uwaga

Mimo tego, że firma Trend Micro aktywnie sprawdza strony internetowe pod względem bezpieczeństwa, użytkownicy mogą napotkać niesprawdzoną stronę, odwiedzając nowe lub mniej popularne witryny internetowe. Zablokowanie dostępu do niesprawdzonych stron może zwiększyć bezpieczeństwo, ale jednocześnie uniemożliwić wyświetlanie bezpiecznych stron.

12. Wybierz opcję **Blokuj strony zawierające złośliwy skrypt**, aby identyfikować luki w zabezpieczeniach przeglądarki i złośliwe skrypty, a także aby zapobiegać wykorzystaniu takich zagrożeń w celu naruszenia bezpieczeństwa przeglądarki internetowej.

Program OfficeScan wykorzystuje zarówno sygnaturę zapobiegania wykorzystaniu luki w zabezpieczeniach przeglądarki, jak i sygnaturę analizatora skryptów do analizowania i blokowania stron internetowych przed narażeniem systemu na niebezpieczeństwo.

TABELA 12-3. Przeglądarki obsługiwane przez funkcję zapobiegania wykorzystaniu luki w zabezpieczeniach przeglądarki

PRZEGLĄDARKA	WERSJA
Microsoft Internet Explorer	• 7.x • 8.x • 9.x • 10.x • 11.x

Ważne

Funkcja zapobiegania wykorzystaniu luki w zabezpieczeniach przeglądarki wymaga włączenia usługi zaawansowanej ochrony.

Aby uruchomić usługę zaawansowanej ochrony, przejdź do opcji **Agenci** > **Zarządzanie agentami** i kliknij kolejno **Ustawienia** > **Ustawienia dodatkowej usługi**.

Po pierwszym włączeniu funkcji zapobiegania wykorzystaniu luki w zabezpieczeniach przeglądarki na Agenci OfficeScan użytkownicy muszą włączyć wymagany dodatek w przeglądarce, zanim ta funkcja zacznie działać. W przypadku Agenci OfficeScan z przeglądarką Internet Explorer 9, 10 lub 11 użytkownicy muszą włączyć dodatek `Trend Micro IE Protection` w oknie wyskakującym przeglądarki.

13. Skonfiguruj listy dozwolonych i zablokowanych elementów.

Uwaga

Lista dozwolonych adresów ma pierwszeństwo przed listą zablokowanych adresów. Gdy adres URL pasuje do wpisu na liście dozwolonych, agenci zawsze zezwalają na dostęp do adresu URL, nawet jeśli znajduje się on na liście zablokowanych.

a. Wybierz opcję **Włącz listę dozwolonych/zablokowanych adresów**.

b. Wpisz adres URL.

Znak wieloznaczny (*) można dodać w dowolnym miejscu adresu URL.

Na przykład:

- Zapisz `www.trendmicro.com/*` oznacza zaakceptowanie wszystkich stron w witrynie internetowej firmy Trend Micro.
- Zapis `*.trendmicro.com/*` oznacza zaakceptowanie wszystkich stron w poddomenach witryny `trendmicro.com`.

Można wpisać adresy URL zawierające adresy IP. Jeśli adres URL zawiera adres IPv6, należy umieścić go w nawiasach.

c. Kliknij opcję **Dodaj do listy dozwolonych** lub **Dodaj do listy zablokowanych**.

d. Aby wyeksportować listę do pliku `.dat`, kliknij przycisk **Eksportuj**, a następnie kliknij przycisk **Zapisz**.

e. Jeśli masz listę wyeksportowaną z innego serwera i chcesz ją zaimportować na ten ekran, kliknij polecenie **Importuj** i wskaż plik `.dat`. Lista zostanie wczytana.

Ważne

Usługa Web Reputation nie wykonuje żadnego skanowania adresów znajdujących się na listach dozwolonych i zablokowanych.

---

14. W celu przesłania zgłoszenia dotyczącego usługi Web Reputation należy użyć adresu URL podanego w sekcji **Ponowna ocena adresu URL**. W przeglądarce internetowej zostanie otwarty system zapytań usługi Web Reputation firmy Trend Micro.

15. Wybierz, czy Agent OfficeScan ma możliwość wysyłania dzienników Web Reputation na serwer. Aby przeanalizować adresy URL blokowane przez program OfficeScan i podjąć odpowiednie działania względem adresów URL uznanych za bezpieczne, należy zezwolić agentom na wysyłanie dzienników.

16. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

- **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.

- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Powiadamianie użytkowników Agenta o zagrożeniach internetowych

Program OfficeScan może wyświetlić powiadomienie programu na punkcie końcowym agenta OfficeScan natychmiast po zablokowaniu adresu URL naruszającego regułę Web Reputation. Należy włączyć opcję wysyłania powiadomień programu i w razie potrzeby zmodyfikować treść powiadomienia programu.

Włączanie powiadomień programu o zagrożeniach internetowych

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Kliknij kartę **Inne ustawienia**.
5. W sekcji **Ustawienia usługi Web Reputation** wybierz opcję **Wyświetl powiadomienie, gdy witryna sieci Web zostanie zablokowana**.
6. W sekcji **Ustawienia wywołania zwrotnego C&C** wybierz opcję **Wyświetl powiadomienie, gdy zostanie wykryte wywołanie zwrotne C&C**.
7. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do

istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.

- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Modyfikowanie powiadomień o zagrożeniach internetowych

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Agent**.
2. Z listy rozwijanej **Typ** wybierz typ powiadomienia o zagrożeniach internetowych, który ma zostać zmodyfikowany:
   - **Naruszenia usługi Web Reputation**
   - **Wywołania zwrotne C&C**
3. Zmodyfikuj domyślny komunikat, wpisując treść w odpowiednim polu.
4. Kliknij przycisk **Zapisz**.

Powiadomienia o wywołaniach zwrotnych C&C dla administratorów

Program OfficeScan zawiera domyślne powiadomienia informujące administratorów programu OfficeScan o wykryciu wywołań zwrotnych C&C. Można zmodyfikować powiadomienia i skonfigurować dodatkowe ustawienia powiadamiania zgodnie z potrzebami.

Konfigurowanie powiadomień o wywołaniach zwrotnych C&C dla administratorów

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Administrator**.
2. Na karcie **Kryteria**:
   a. Przejdź do sekcji **Wywołania zwrotne C&C**.
   b. Określ, czy powiadomienia mają być wysyłane po wykryciu wywołania zwrotnego C&C przez program OfficeScan (operacja może być blokowana albo rejestrowana) lub tylko w przypadku, gdy poziom ryzyka adresu wywołania zwrotnego jest wysoki.
3. Na karcie **Poczta elektroniczna**:
   a. Przejdź do sekcji **Wywołania zwrotne C&C**.
   b. Wybierz opcję **Włącz powiadamianie za pomocą wiadomości e-mail**.
   c. Wybierz opcję **Wyślij powiadomienia do użytkowników z uprawnieniami do domeny drzewa agentów**.

      Administracja oparta na rolach umożliwia przyznanie użytkownikom uprawnień do domeny drzewa agentów. Jeżeli nastąpi transmisja na dowolnym agencie należącym do określonej domeny, zostaną wysłane wiadomości na adresy e-mail użytkowników z uprawnieniami do domeny. Przykłady znajdują się w poniższej tabeli:

TABELA 12-4. Domeny i uprawnienia w drzewie agentów

DOMENA DRZEWA AGENTÓW	ROLE Z UPRAWNIENIAMI DO DOMENY	KONTO UŻYTKOWNIKA Z ROLĄ	ADRES E-MAIL DLA KONTA UŻYTKOWNIKA
Domena A	Administrator (wbudowany)	konto główne	mary@xyz.com
	Rola_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domena B	Administrator (wbudowany)	konto główne	mary@xyz.com
	Rola_02	admin_jane	jane@xyz.com

Jeśli Agent OfficeScan należący do Domeny A wykryje wywołanie zwrotne C&C, wiadomość e-mail zostanie wysłana na adresy mary@xyz.com, john@xyz.com i chris@xyz.com.

Jeśli wywołanie zwrotne C&C wykryje Agent OfficeScan należący do Domeny B, wiadomość e-mail zostanie wysłana na adresy mary@xyz.com i jane@xyz.com.

Uwaga

Po włączeniu tej opcji, wszyscy użytkownicy z uprawnieniami do domeny muszą mieć odpowiedni adres e-mail. Powiadomienie e-mail nie zostanie wysłane do użytkowników bez adresu e-mail. Użytkowników i adresy e-mail można skonfigurować na ekranie **Administracja** > **Zarządzanie kontami** > **Konta użytkowników**.

d. Wybierz opcję **Wysyłaj powiadomienia na następujące adresy e-mail** i wpisz adresy e-mail.

e. Zaakceptuj lub zmień domyślny temat i wiadomość. Do przedstawienia danych w polach **Temat** i **Wiadomość**.

TABELA 12-5. Zmienne znaczników dla powiadomień o wywołaniach zwrotnych C&C

ZMIENNA	OPIS
%CLIENTCOMPUTER%	Docelowy punkt końcowy, który wysłał wywołanie zwrotne
%IP%	Adres IP docelowego punktu końcowego
%DOMAIN%	Domena komputera
%DATETIME%	Data i godzina wykrycia transmisji
%CALLBACKADDRESS%	Adres wywołania zwrotnego serwera C&C
%CNCRISKLEVEL%	Poziom ryzyka serwera C&C
%CNCLISTSOURCE%	Wskazuje źródło listy C&C
%ACTION%	Wykonana operacja

4. Na karcie **Pułapka SNMP**:
   a. Przejdź do sekcji **Wywołania zwrotne C&C**.
   b. Wybierz opcję **Włącz powiadamianie przez pułapkę SNMP**.
   c. Zaakceptuj lub zmień domyślną wiadomość. Do przedstawienia danych w polu **Wiadomość**. Szczegółowe informacje można znaleźć w części *Tabela 12-5: Zmienne znaczników dla powiadomień o wywołaniach zwrotnych C&C na stronie 12-18*.
5. Na karcie **Dziennik zdarzeń Windows NT**:
   a. Przejdź do sekcji **Wywołania zwrotne C&C**.
   b. Wybierz opcję **Włącz powiadamianie przez rejestr zdarzeń NT**.
   c. Zaakceptuj lub zmień domyślną wiadomość. Dane w polu **Wiadomość** można przedstawiać za pomocą znaczników. Szczegółowe informacje można znaleźć w części *Tabela 12-5: Zmienne znaczników dla powiadomień o wywołaniach zwrotnych C&C na stronie 12-18*.

6. Kliknij przycisk **Zapisz**.

Powiadomienia ostrzegania kontaktu C&C dla użytkowników agenta

Program OfficeScan może wyświetlić powiadomienie na komputerach agentów OfficeScan natychmiast po zablokowaniu adresu URL serwera C&C. Należy włączyć opcję wysyłania powiadomień programu i w razie potrzeby zmodyfikować treść powiadomienia programu

Włączanie powiadomienia o wywołaniach zwrotnych C&C

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Kliknij kartę **Inne ustawienia**.
5. W sekcji **Ustawienia wywołania zwrotnego C&C** wybierz opcję **Wyświetl powiadomienie, gdy zostanie wykryte wywołanie zwrotne C&C**.
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.

- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Modyfikowanie powiadomień o wywołaniach zwrotnych C&C

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Agent**.
2. Na liście rozwijanej **Typ** wybierz opcję **Wywołania zwrotne C&C**.
3. Zmodyfikuj domyślny komunikat, wpisując treść w odpowiednim polu.
4. Kliknij przycisk **Zapisz**.

Epidemie wywołań zwrotnych C&C

Zdefiniuj epidemię wywołań zwrotnych C&C według liczby, źródła i poziomu ryzyka wywołań zwrotnych.

Program OfficeScan zawiera domyślne powiadomienie informujące administratorów OfficeScan o epidemii. Można zmodyfikować powiadomienie programu zgodnie z potrzebami.

Uwaga

Program OfficeScan może wysyłać powiadomienia o epidemii wywołań zwrotnych C&C za pomocą poczty e-mail. Należy skonfigurować ustawienia poczty e-mail, aby umożliwić pomyślne wysyłanie powiadomień e-mail przez program OfficeScan. Szczegółowe informacje zawiera sekcja *Ustawienia powiadamiania administratorów na stronie 14-37*.

Konfigurowanie kryteriów i powiadomień o epidemii wywołań zwrotnych C&C

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Epidemia**.

2. Na karcie **Kryteria** skonfiguruj następujące opcje:

Opcja	Opis
Ten sam zaatakowany host	Wybierz, aby zdefiniować przełamanie na podstawie liczby wykrytych wywołań zwrotnych dla punktu końcowego
Poziom ryzyka C&C	Określ, czy należy wyzwolić powiadomienie o epidemii dla wszystkich wywołań zwrotnych C&C, czy tylko dla źródeł wysokiego ryzyka
Operacja	Wybierz opcję **Dowolne działanie**, **Zarejestrowano** lub **Zablokowano**
Przypadki wykrycia	Wskaż wymaganą liczbę wykryć, która definiuje przełamanie
Okres	Wskaż liczbę godzin, w ciągu której musi wystąpić określona liczba wykryć

Porada

Firma Trend Micro zaleca zaakceptowanie domyślnych wartości na tym ekranie.

3. Na karcie **E-mail**:

   a. Przejdź do sekcji **Wywołania zwrotne C&C**.

   b. Wybierz opcję **Włącz powiadamianie za pomocą wiadomości e-mail**.

   c. Określ odbiorców wiadomości e-mail.

   d. Zaakceptuj lub zmień domyślny temat i wiadomość. Dane w polach **Temat** i **Wiadomość** można przedstawiać za pomocą znaczników.

TABELA 12-6. Zmienne znaczników dla powiadomień o epidemiach wywołań zwrotnych C&C

ZMIENNA	OPIS
%C	Liczba dzienników wywołań zwrotnych C&C
%T	Okres gromadzenia dzienników wywołań zwrotnych C&C

e. Wybierz dodatkowe informacje o wywołaniu zwrotnym C&C, które mają zostać dołączone do wiadomości e-mail.

4. Na karcie **Pułapka SNMP**:

   a. Przejdź do sekcji **Wywołania zwrotne C&C**.

   b. Wybierz opcję **Włącz powiadamianie przez pułapkę SNMP**.

   c. Zaakceptuj lub zmień domyślną wiadomość. Dane w polu **Wiadomość** można przedstawiać za pomocą znaczników. Szczegółowe informacje można znaleźć w części *Tabela 12-6: Zmienne znaczników dla powiadomień o epidemiach wywołań zwrotnych C&C na stronie 12-22*.

5. Na karcie **Dziennik zdarzeń systemu Windows NT**:

   a. Przejdź do sekcji **Wywołania zwrotne C&C**.

   b. Wybierz opcję **Włącz powiadamianie przez rejestr zdarzeń NT**.

   c. Zaakceptuj lub zmień domyślną wiadomość. Dane w polu **Wiadomość** można przedstawiać za pomocą znaczników. Szczegółowe informacje można znaleźć w części *Tabela 12-6: Zmienne znaczników dla powiadomień o epidemiach wywołań zwrotnych C&C na stronie 12-22*.

6. Kliknij przycisk **Zapisz**.

Dzienniki zagrożenia internetowego

Agentów wewnętrznych i zewnętrznych można skonfigurować w celu wysyłania dzienników Web Reputation na serwer. Umożliwia to analizę adresów URL, które są

blokowane przez program OfficeScan, i podjęcie odpowiednich czynności odnośnie adresów URL uznawanych za bezpieczne.

Aby dzienniki nie zajmowały zbyt dużo miejsca na dysku twardym, można je ręcznie usunąć lub skonfigurować harmonogram ich usuwania. Dodatkowe informacje dotyczące dzienników zarządzania zawiera sekcja *Zarządzanie dziennikiem na stronie 14-41*.

Wyświetlanie dzienników usługi Web Reputation

Procedura

1. Przejdź do opcji **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa** lub **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Wyświetl dzienniki** > **Dzienniki Web Reputation** lub **Dzienniki** > **Dzienniki Web Reputation**.
4. Określ kryteria dziennika i kliknij przycisk **Wyświetl dzienniki**.
5. Wyświetl dzienniki. Dziennik zawiera następujące informacje:

ELEMENT	OPIS
Data i godzina	Godzina wykrycia
Punkt końcowy	Punkt końcowy, na którym nastąpiło wykrycie
Domena	Domena punktu końcowego, na którym nastąpiło wykrycie
URL	Adres URL zablokowany przez usługi Web Reputation Services
Poziom ryzyka	Poziom zagrożenia adresu URL
Opis	Opis zagrożenia bezpieczeństwa

Element	Opis
Proces	Proces, za pośrednictwem którego podjęto próbę kontaktu (ścieżka\nazwa_aplikacji)
Operacja	Operacja przeprowadzona po wykryciu

6. Jeśli występują adresy URL, które nie powinny być blokowane, kliknij przycisk **Dodaj do listy dozwolonych**, aby dodać witrynę sieci Web do listy dozwolonych adresów URL.

7. Aby zapisać dzienniki jako plik rozdzielany przecinkami (CSV), kliknij opcję **Eksportuj wszystkie do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Wyświetlanie dzienników wywołań zwrotnych C&C

Procedura

1. Przejdź do opcji **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa** lub **Agenci** > **Zarządzanie agentami**.

2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.

3. Kliknij polecenie **Wyświetl dzienniki** > **Dzienniki wywołania zwrotnego C&C** lub **Dzienniki** > **Dzienniki wywołania zwrotnego C&C**.

4. Określ kryteria dziennika i kliknij przycisk **Wyświetl dzienniki**.

5. Wyświetl dzienniki. Dziennik zawiera następujące informacje:

Element	Opis
Data i godzina	Godzina wykrycia
Użytkownik	Użytkownik zalogowany w momencie wykrycia
Zaatakowany host	Punkt końcowy, z którego pochodzi wywołanie zwrotne

ELEMENT	OPIS
Adres IP	Adres IP zaatakowanego hosta
Domena	Domena punktu końcowego, na którym nastąpiło wykrycie
Adres wywołania zwrotnego	Adres, na który punkt końcowy wysłał wywołanie zwrotne
Źródło listy C&C	Źródło listy C&C, która zidentyfikowała serwer C&C
Poziom ryzyka C&C	Poziom ryzyka serwera C&C
Protokół	Protokół internetowy używany do transmisji
Proces	Proces, który zainicjował transmisję (ścieżka \nazwa_aplikacji)
Operacja	Operacja dokonana dla wywołania zwrotnego

6. Jeśli usługa Web Reputation zablokowała adres URL, który nie powinien być blokowany, kliknij przycisk **Dodaj do listy dozwolonych usługi Web Reputation**, aby dodać adres do listy dozwolonych usługi Web Reputation.

Uwaga

Program OfficeScan może dodawać adresy URL tylko do listy dozwolonych usługi Web Reputation. W przypadku wykryć dokonanych przez globalną listę adresów IP C&C lub listę programu Virtual Analyzer (IP) C&C należy ręcznie dodać te adresy IP do zdefiniowanej przez użytkownika listy dozwolonych adresów IP C&C.

Szczegółowe informacje zawiera sekcja *Konfigurowanie globalnych, zdefiniowanych przez użytkownika list adresów IP na stronie 8-6*.

7. Aby zapisać dzienniki jako plik rozdzielany przecinkami (CSV), kliknij opcję **Eksportuj wszystkie do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Rozdział 13

Korzystanie z zapory OfficeScan

W tym rozdziale przedstawiono funkcje i konfiguracje zapory OfficeScan.

Rozdział składa się z następujących tematów:

Zapora programu OfficeScan — informacje

Zapora programu OfficeScan chroni agentów i serwery w sieci korzystając z kontroli stanowej — wysoce skutecznego skanowania wirusów sieciowych. Za pomocą centralnej kontroli zarządzania można utworzyć zasady filtrowania połączeń według aplikacji, adresu IP, numeru portu lub protokołu, a następnie zastosować te zasady do różnych grup użytkowników.

Uwaga

Zaporę programu OfficeScan można również uruchomić, skonfigurować i stosować na punktach końcowych z systemem Windows XP, na których włączona jest także zapora systemu Windows. Wskazane jest jednak ostrożne dobieranie reguł, tak aby uniknąć konfliktów między zaporami i uzyskania nieoczekiwanych wyników. Szczegółowe informacje na temat zapory systemu Windows zawiera dokumentacja firmy Microsoft.

W zaporze programu OfficeScan są dostępne następujące ważne funkcje:

Filtrowanie ruchu

Zapora programu OfficeScan filtruje cały przychodzący i wychodzący ruch sieciowy, umożliwiając blokowanie określonego typu ruchu rozpoznawanego na podstawie następujących kryteriów:

- Kierunek (przychodzący/wychodzący)
- Protokoły (TCP/UDP/ICMP/ICMPv6)
- Porty docelowe
- Źródłowe i docelowe punkty końcowe

Filtrowanie aplikacji

Zapora programu OfficeScan filtruje ruch przychodzący i wychodzący konkretnych aplikacji, umożliwiając im uzyskiwanie dostępu do sieci. Należy jednak pamiętać, że dostęp do połączenia sieciowego zależy również od reguł skonfigurowanych przez administratora.

Lista zatwierdzonego bezpiecznego oprogramowania

Na liście certyfikowanego bezpiecznego oprogramowania znajdują się aplikacje, które mogą pomijać reguły poziomów zabezpieczeń zapory. Jeśli wybrano średni lub wysoki poziom zabezpieczeń, program OfficeScan zezwala aplikacjom na uruchamianie i uzyskiwanie dostępu do sieci.

Dzięki włączeniu zapytania do listy usługi Certified Safe Software można otrzymać dokładniejszą listę. Ta lista jest dynamicznie aktualizowana przez firmę Trend Micro.

Uwaga

Funkcja ta współpracuje z usługą monitorowanie zachowań. Przed włączeniem globalnego ustawienia Lista zatwierdzonego bezpiecznego oprogramowania należy się upewnić, że włączono usługę zapobiegania nieautoryzowanym zmianom oraz usługę Certified Safe Software Service.

Skanowanie w poszukiwaniu wirusów sieciowych

Zapora OfficeScan sprawdza również każdy pakiet pod kątem występowania wirusów sieciowych. Szczegółowe informacje zawiera sekcja *Wirusy i złośliwe oprogramowanie na stronie 7-2*.

Niestandardowe profile i reguły bezpieczeństwa

Zapora programu OfficeScan zapewnia możliwość skonfigurowania reguł, aby blokować lub przepuszczać określone rodzaje ruchu sieciowego. Wystarczy przypisać reguły do jednego lub większej liczby profili, które następnie można zastosować do określonych agentów OfficeScan. Metoda ta pozwala organizować i konfigurować ustawienia zapory dla agentów w bardzo szerokim zakresie.

Kontrola stanowa

Zapora programu OfficeScan to zapora stanowa, która monitoruje wszystkie połączenia z agentem OfficeScan i zapamiętuje wszystkie stany tych połączeń. Identyfikuje specyficzne warunki połączenia, przewiduje, jakie działania powinny nastąpić, a także wykrywa zakłócenia połączenia. Oznacza to, że efektywne korzystanie z zapory wiąże się nie tylko z zastosowaniem profilów i reguł, lecz także z analizą połączeń i filtrowaniem pakietów przesyłanych przez obszar zapory.

System wykrywania włamań (IDS)

Zapora OfficeScan zawiera również system wykrywania intruzów (IDS). Po uruchomieniu system IDS wspomaga identyfikację sygnatur w pakietach sieciowych, które mogą wskazywać na atak na urządzenie typu Agent OfficeScan. Zapora OfficeScan umożliwia zapobieganie następującym znanym typom ataków:

Atak	Opis
Zbyt duży fragment	Atak typu Denial of Service, w którym haker kieruje ponadwymiarowy pakiet TCP/UDP do docelowego urządzenia typu punkt końcowy. Może to spowodować przepełnienie bufora urządzenia typu punkt końcowy i zablokowanie urządzenia typu punkt końcowy lub jego ponowne uruchomienie.
Atak Ping of Death	Atak typu Denial of Service, w którym haker kieruje ponadwymiarowy pakiet ICMP/ICMPv6 do docelowego urządzenia typu punkt końcowy. Może to spowodować przepełnienie bufora urządzenia typu punkt końcowy i zablokowanie urządzenia typu punkt końcowy lub jego ponowne uruchomienie.

Atak	Opis
Skonfliktowane ARP	Rodzaj ataku, w którym haker wysyła żądanie ARP (Address Resolution Protocol), w którym adres IP lokalizacji źródłowej i docelowej jest taki sam jak adres urządzenia typu punkt końcowy. Docelowe urządzenie typu punkt końcowy nieprzerwanie wysyła odpowiedź ARP (własny adres MAC) do samego siebie, co powoduje awarie oraz blokowanie komputera.
Atak typu SYN flood	Atak typu Denial of Service, w którym program wysyła do urządzenia typu punkt końcowy wiele pakietów synchronizacji TCP (SYN), powodując nieprzerwane wysyłanie przez to urządzenie typu punkt końcowy odpowiedzi oznaczających potwierdzenie synchronizacji (SYN/ACK). Może to wyczerpać pamięć urządzenia typu punkt końcowy, co prowadzi do jego awarii.
Nakładające się fragmenty	Podobnie jak w przypadku ataku typu Teardrop, w tym ataku typu Denial of - do urządzenia typu punkt końcowy wysyłane są pokrywające się fragmenty TCP. Powoduje to nadpisanie informacji nagłówka w pierwszym fragmencie TCP, co może spowodować przejście fragmentu przez zaporę. Zapora może zezwolić na przepuszczenie do docelowego urządzenia typu punkt końcowy następujących po sobie fragmentów ze złośliwym kodem.
Atak typu Teardrop	Podobnie jak w przypadku ataku opartego na pokrywających się fragmentach, w tym ataku typu Denial of Service używane są fragmenty adresu IP. Myląca wartość offsetu w drugim lub dalszym fragmencie IP może spowodować awarię systemu operacyjnego urządzenia typu punkt końcowy podczas próby ponownego złożenia fragmentów.
Niewielki fragment	Rodzaj ataku, w którym niewielki rozmiar fragmentu TCP wymusza dołączenie informacji nagłówka z pierwszego pakietu TCP do następnego fragmentu. Może to spowodować zignorowanie przez routery filtrujące ruch następnych fragmentów mogących zawierać złośliwy kod.
Pofragmentowany IGMP	Atak typu Denial of Service, w którym pofragmentowane pakiety IGMP wysyłane są do docelowego urządzenia typu punkt końcowy, które nie jest w stanie poprawnie ich przetworzyć. Może to spowodować zablokowanie urządzenia typu punkt końcowy lub spowolnienie jego pracy.

Atak	Opis
Atak typu LAND	Typ ataku, w którym pakiety synchronizacji IP (SYN) o takim samym adresie źródłowym i docelowym są wysyłane do urządzenia typu punkt końcowy, powodując wysyłanie przez to urządzenie typu punkt końcowy odpowiedzi oznaczających potwierdzenie synchronizacji (SYN/ACK) do samego siebie. Może to spowodować zablokowanie urządzenia typu punkt końcowy lub spowolnienie jego pracy.

Monitorowanie epidemii naruszeń zapory

Zapora programu OfficeScan wysyła dostosowane komunikaty alarmowe do określonych odbiorców, gdy ilość naruszeń zapory przekroczy pewne progi, co może sygnalizować atak.

Uprawnienia do zapory agenta OfficeScan

Użytkownikom agenta OfficeScan można przydzielić uprawnienie do wyświetlania ustawień zapory na konsoli agenta OfficeScan. Użytkownikom można także przydzielić uprawnienia do włączania lub wyłączania zapory, systemu wykrywania intruzów oraz do przesyłania powiadomień programu o naruszeniu zapory.

Włączanie lub wyłączanie zapory programu OfficeScan

Podczas instalacji serwera OfficeScan wyświetlany jest monit o włączenie lub wyłączenie zapory programu OfficeScan.

Jeśli po włączeniu zapory podczas instalacji zaobserwowano wpływ na wydajność, szczególnie na platformach serwerowych (Windows Server 2003, Windows Server 2008 i Windows Server 2012), należy rozważyć wyłączenie zapory.

Jeśli podczas instalacji wyłączono zaporę, ale konieczne jest jej włączenie w celu ochrony agenta przed atakami, należy najpierw przeczytać wytyczne i instrukcje w temacie *Usługi agenta OfficeScan na stronie 15-7*.

Zaporę można włączyć lub wyłączyć na wszystkich lub na wybranych punktach końcowych agenta OfficeScan.

Włączanie lub wyłączanie zapory OfficeScan na wybranych punktach końcowych

Użyj jednej z poniższych metod, aby włączyć lub wyłączyć zaporę w konsoli internetowej.

METODA	PROCEDURA
Utworzenie nowej reguły i zastosowanie jej na agentach OfficeScan	1. Utwórz nową regułę, która włącza/wyłącza zaporę. Opis poszczególnych etapów tworzenia nowej reguły znajduje się w *Dodawanie wytyczne dla zapory sieciowej na stronie 13-11*. 2. Zastosuj regułę na agentach OfficeScan.
włączenie/ wyłączenie usługi zapory z poziomu konsoli Web.	Szczegółowe kroki zawiera temat *Usługi agenta OfficeScan na stronie 15-7*. **Uwaga** Wyłączenie usługi zapory powoduje automatyczne wyłączenie wszystkich wytyczne dla zapory sieciowej na wybranych agentach.

Użyj jednej z poniższych metod, aby włączyć lub wyłączyć zaporę na wybranych punktach końcowych.

METODA	PROCEDURA
Włączanie/ wyłączanie sterownika zapory	1. Otwórz okno **Właściwości połączenia sieciowego**. 2. Zaznacz lub usuń zaznaczenie pola wyboru **Ogólny sterownik zapory firmy Trend Micro** obok karty sieciowej.
Włączanie/ wyłączanie usługi zapory	1. Otwórz wiersz polecenia i wpisz `services.msc`. 2. Uruchom lub zatrzymaj **Zaporę OfficeScan NT** z poziomu konsoli Microsoft Management Console (MMC).

Włączanie lub wyłączanie zapory OfficeScan na wszystkich punktach końcowych

Procedura

1. Przejdź do opcji **Administracja** > **Ustawienia** > **Licencja produktu**.
2. Przejdź do sekcji **Usługi dodatkowe**.
3. W wierszu **Dodatkowe usługi** obok wiersza **Zapora punktów końcowych** kliknij opcję **Włącz** lub **Wyłącz**.

Reguły i profile zapory

Zapora programu OfficeScan wykorzystuje reguły i profile do organizowania i dostosowywania metod ochrony punktów końcowych w sieci.

Dzięki integracji z usługą Active Directory oraz administracji opartej na rolach każda rola użytkownika, w zależności od przydzielonych uprawnień, może umożliwiać tworzenie, konfigurowanie lub usuwanie reguł oraz profilów dotyczących wyłącznie odpowiadających im domen.

Porada

Uruchomienie kilku zapór na jednym punkcie końcowym może powodować nieoczekiwane rezultaty. Przed instalacją i włączeniem zapory programu OfficeScan zaleca się odinstalowanie innych zapór istniejących na agentach OfficeScan.

Aby z powodzeniem korzystać z zapory OfficeScan, należy wykonać następujące czynności:

1. Utwórz regułę. Reguła umożliwia określenie poziomu zabezpieczeń, który blokuje lub umożliwia ruch na punktach końcowych w sieci i włącza funkcje zapory.
2. Dodaj wyjątki do reguły. Wyjątki zapewniają agentom OfficeScan możliwość stosowania odstępstw od reguły. Za pomocą wyjątków można określić agentów blokować lub zezwalać na niektóre typy ruchu mimo ustawionego poziomu

zabezpieczeń w regułach. W ramach listy reguł można na przykład zablokować cały ruch niektórych agentów, ale dzięki utworzeniu wyjątku zezwolić na ruch generowany przez protokół HTTP, tak aby agenci mogli uzyskać dostęp do serwera sieci Web.

3. Utwórz i przypisz profile do agentów OfficeScan. Profil zapory zawiera zestaw atrybutów agenta i jest przypisany do reguły. Gdy agent spełnia atrybuty określone w profilu, wyzwalana jest powiązana reguła.

Wytyczne dla zapory sieciowej

Wytyczne dla zapory sieciowej umożliwiają blokowanie lub akceptowanie różnych typów ruchu sieciowego, które nie są skonfigurowane w wyjątku reguły. Reguła określa również, które funkcje zapory są włączone lub wyłączone. Regułę można przypisać do jednego lub wielu profilów zapory.

Dzięki integracji z usługą Active Directory oraz administracji opartej na rolach każda rola użytkownika, w zależności od przydzielonych uprawnień, może umożliwiać tworzenie, konfigurowanie lub usuwanie reguł dotyczących wyłącznie odpowiadających im domen.

Poniższa tabela przedstawia ustawienia dostępne podczas konfigurowania wytycznych dla zapory sieciowej.

Ustawienia	Opis
Poziom zabezpieczeń	Ustawienia ogólne, które blokują lub zezwalają ruch przychodzący i wychodzący na punkt końcowy Agent OfficeScan.
Funkcje zapory	Ustal, czy ma być włączona lub wyłączona zapora OfficeScan, System detekcji intruzów (IDS) oraz powiadamianie programu o naruszeniu zapory. Szczegółowe informacje zawiera sekcja *System wykrywania włamań (IDS) na stronie 13-4*.
Lista zatwierdzonego bezpiecznego oprogramowania	ustal, czy z siecią mogą się łączyć certyfikowane bezpieczne aplikacje. Szczegółowe informacje zawiera sekcja *Lista zatwierdzonego bezpiecznego oprogramowania na stronie 13-3*.

Ustawienia	Opis
Lista wyjątków reguł	lista możliwych do konfiguracji wyjątków związanych z blokowaniem lub umożliwianiem różnych typów ruchu sieciowego.

Uwaga

Użytkownikom końcowym można przyznać uprawnienie do modyfikowania poziomu zabezpieczeń i listy wyjątków reguł podczas tworzenia profilów zapory.

Szczegółowe informacje zawiera sekcja *Dodawanie profilu zapory na stronie 13-21*.

Domyślne wytyczne dla zapory sieciowej

Program OfficeScan zawiera zestaw domyślnych reguł, które można modyfikować i usuwać.

Nazwa reguły	Poziom zabezpieczeń	Agent — ustawienia	Wyjątki	Zalecane użycie
Nieograniczony dostęp	Niskie	Włącz zaporę	Brak	Użyj, aby zezwolić agentom na nieograniczony dostęp do sieci
Porty komunikacyjne programu Trend Micro Control Manager	Niskie	Włącz zaporę	Zezwala na przychodzący i wychodzący ruch TCP/UDP bez ograniczeń przez porty 80 i 10319	Użyj, gdy agenci są wyposażeni w instalację agenta MCP
Konsola programu ScanMail for Microsoft Exchange	Niskie	Włącz zaporę	Zezwala na przychodzący i wychodzący ruch TCP bez ograniczeń przez port 16372	Użyj, gdy jest wymagane uzyskanie dostępu agentów do konsoli programu ScanMail

Nazwa reguły	Poziom zabezpieczeń	Agent — ustawienia	Wyjątki	Zalecane użycie
Konsola InterScan Messaging Security Suite (IMSS)	Niskie	Włącz zaporę	Zezwala na przychodzący i wychodzący ruch TCP bez ograniczeń przez port 80	Użyj, gdy jest wymagane uzyskanie dostępu agentów do konsoli programu IMSS

Dodawanie wytyczne dla zapory sieciowej

Procedura

1. Przejdź do opcji **Agenci** > **Zapora** > **Reguły**.
2. Aby dodać nową regułę, kliknij przycisk **Dodaj**.

   Jeśli nowa reguła, którą chcesz utworzyć, ma podobne ustawienia, jak istniejąca reguła, zaznacz tę regułę i kliknij polecenie **Kopiuj**.
3. Wpisz nazwę listy reguł.
4. Wybierz poziom bezpieczeństwa.

   Wybrany poziom bezpieczeństwa nie będzie dotyczyć ruchu spełniającego kryteria wyjątku od wytyczne dla zapory sieciowej.
5. Wybierz funkcje zapory, które mają być wykorzystane dla reguły.

   - Powiadomienie programu o naruszeniu zapory jest wyświetlane po zablokowaniu przez zaporę pakietu wychodzącego. Aby zmienić komunikat ostrzeżenia, patrz: *Modyfikowanie treści powiadomienia programu od zapory na stronie 13-30*.
   - Jeśli administrator włączy wszystkie funkcje zapory i przyzna użytkownikom programu Agent OfficeScan uprawnienie do konfigurowania ustawień zapory, użytkownicy mogą włączać/wyłączać funkcje oraz modyfikować ustawienia zapory w konsoli programu Agent OfficeScan.

OSTRZEŻENIE!

Konsoli Web programu OfficeScan nie można używać do zastępowania ustawień konsoli agenta OfficeScan, które są konfigurowane przez użytkownika.

- Jeżeli funkcje te nie zostaną uaktywnione, ustawienia zapory konfigurowane za pomocą konsoli Web programu OfficeScan zostaną wyświetlone pod sekcją **Lista kart sieciowych** w konsoli agenta OfficeScan.
- Informacje wyświetlane w konsoli agenta OfficeScan w obszarze **Ustawienia** na karcie **Zapora** zawsze odzwierciedlają ustawienia skonfigurowane z poziomu konsoli agenta OfficeScan, a nie z poziomu konsoli Web serwera.

6. Włącz lokalną lub globalną listę certyfikowanego bezpiecznego oprogramowania.

Uwaga

Przed włączeniem tej usługi należy się upewnić, że włączono usługę zapobiegania nieautoryzowanym zmianom oraz usługę Certified Safe Software.

7. W obszarze Wyjątek wybierz wyjątki od wytyczne dla zapory sieciowej. Wyjątki od reguł zawarte w tym miejscu są oparte na szablonie wyjątków zapory. Szczegółowe informacje można znaleźć w części *Edytowanie szablonu wyjątków zapory na stronie 13-14*.

- Istniejące wyjątki od reguł można modyfikować, klikając nazwę wyjątku reguły i zmieniając ustawienia na stronie, która zostanie wyświetlona.

Uwaga

Zmodyfikowany wyjątek od reguły będzie mieć zastosowanie wyłącznie do nowo utworzonych reguł. Aby modyfikacje wyjątku reguły były trwałe, te same modyfikacje należy wprowadzić do szablonu wyjątku zapory.

- Aby utworzyć nowy wyjątek od reguły, kliknij opcję **Dodaj**. Określ ustawienia na stronie, która zostanie wyświetlona.

Uwaga

Wyjątek od reguły również będzie mieć zastosowanie wyłącznie do nowo utworzonych reguł. Aby zastosować ten wyjątek od reguły do innych reguł, należy dodać go najpierw do listy wyjątków od reguł w szablonie wyjątku zapory.

8. Kliknij przycisk **Zapisz**.

Modyfikowanie istniejącej wytyczne dla zapory sieciowej

Procedura

1. Przejdź do opcji **Agenci** > **Zapora** > **Reguły**.
2. Kliknij regułę.
3. Należy zmodyfikować następujące opcje:
   - Nazwa reguły
   - Poziom zabezpieczeń
   - Funkcje zapory, które mają być wykorzystane dla reguły
   - Stan listy usługi Certified Safe Software
   - Wyjątki od wytyczne dla zapory sieciowej, które mają zostać uwzględnione w określonej regule
     - Edytuj istniejący wyjątek od reguły (kliknij nazwę wyjątku od reguły i zmień ustawienia na stronie, która zostanie wyświetlona)
     - Aby utworzyć nowy wyjątek od reguły, kliknij opcję **Dodaj**. Określ ustawienia na stronie, która zostanie wyświetlona.
4. Aby zastosować modyfikacje istniejącej reguły, kliknij przycisk **Zapisz**.

Edytowanie szablonu wyjątków zapory

Szablon wyjątków zapory zawiera wyjątki od reguły, które można konfigurować, aby zezwalać lub blokować różnego typu ruch sieciowy w zależności od numerów portów i adresów IP punktów końcowych agenta OfficeScan. Po utworzeniu wyjątku od reguły, należy przeprowadzić edycję reguł, których on dotyczy.

Określ, którego typu wyjątku od reguły chcesz użyć. Dostępne są dwa typy:

- **Ograniczające**

  Blokuje tylko określone rodzaje ruchu sieciowego i jest stosowane do reguł, które zezwalają na każdy ruch sieciowy. Przykładem ograniczającego wyjątku od reguły jest blokowanie portów agenta OfficeScan narażonych na atak, na przykład portów często wykorzystywanych przez trojany.

- **Dopuszczające**

  Zezwala tylko na określone rodzaje ruchu sieciowego i jest stosowane do reguł, które blokują każdy ruch sieciowy. Przykładem wyjątku dopuszczającego jest zezwolenie agentom OfficeScan na dostęp tylko do serwera OfficeScan i serwera sieci Web. W tym celu, należy zezwolić na ruch sieciowy z portu zaufanego (używanego do komunikacji z serwerem OfficeScan) oraz portu, którego Agent OfficeScan używa do komunikacji przez protokół HTTP.

  Port nasłuchiwania agenta OfficeScan: **Agenci** > **Zarządzanie agentami** > **Stan**.Agent OfficeScan Numer portu znajduje się w obszarze **Informacje podstawowe**.

  Port nasłuchiwania serwera: **Administracja** > **Ustawienia** > **Połączenie agenta**. Numer portu znajduje się w obszarze **Ustawienia połączenia agenta**.

  Program OfficeScan zawiera zestaw domyślnych wyjątków wytyczne dla zapory sieciowej, które można modyfikować i usuwać.

TABELA 13-1. Domyślne wyjątki wytyczne dla zapory sieciowej

NAZWA WYJĄTKU	OPERACJA	PROTOKÓŁ	PORT	KIERUNEK
DNS	Zezwól	TCP/UDP	53	Przychodzące i wychodzące

Nazwa wyjątku	Operacja	Protokół	Port	Kierunek
NetBIOS	Zezwól	TCP/UDP	137, 138, 139, 445	Przychodzące i wychodzące
HTTPS	Zezwól	TCP	443	Przychodzące i wychodzące
HTTP	Zezwól	TCP	80	Przychodzące i wychodzące
Telnet	Zezwól	TCP	23	Przychodzące i wychodzące
SMTP	Zezwól	TCP	25	Przychodzące i wychodzące
FTP	Zezwól	TCP	21	Przychodzące i wychodzące
POP3	Zezwól	TCP	110	Przychodzące i wychodzące
LDAP	Zezwól	TCP/UDP	389	Przychodzące i wychodzące

Uwaga

Domyślne wyjątki są stosowane do wszystkich agentów. Jeśli wyjątek domyślny ma być stosowany jedynie wobec niektórych agentów, należy edytować wyjątek i określić, do których adresów IP agentów ma mieć zastosowanie.

Bez aktualizacji wcześniejszej wersji OfficeScan wyjątek protokołu LDAP nie jest dostępny. Jeśli ten wyjątek nie jest widoczny na liście wyjątków, należy go dodać ręcznie.

Dodawanie wyjątku do wytyczne dla zapory sieciowej

Procedura

1. Przejdź do opcji **Agenci** > **Zapora** > **Reguły**.

2. Kliknij opcję **Edytuj szablon wyjątku**.
3. Kliknij przycisk **Dodaj**.
4. Wprowadź nazwę wyjątku od reguły.
5. Wybierz typ aplikacji. Można wybrać wszystkie aplikacje lub określić ścieżkę do aplikacji lub klucze rejestru.

   Uwaga

   Sprawdź nazwę i pełną ścieżkę. W wyjątkach nie mogą być używane znaki wieloznaczne.

6. Wybierz operację, jaką ma wykonywać program OfficeScan w przypadku ruchu sieciowego (blokowanie lub umożliwianie ruchu, który spełnia kryteria wyjątku), oraz kierunek ruchu (ruch sieciowy na punktach końcowych agentów OfficeScan — przychodzący lub wychodzący).
7. Wybierz typ protokołu sieciowego: TCP, UDP, ICMP lub ICMPv6.
8. Określ porty na punkcie końcowym agenta OfficeScan, względem których zostanie wykonana operacja.
9. Wybierz adresy IP punktów końcowych agentów OfficeScan, które należy uwzględnić w wyjątku. Na przykład po wybraniu opcji Zablokuj cały ruch sieciowy (ruch przychodzący i wychodzący) i wpisaniu adresu IP pojedynczego punktu końcowego żaden agent OfficeScan, którego dotyczy ten wyjątek reguły, nie będzie mógł wysyłać ani odbierać danych z tego adresu IP.
   - **Wszystkie adresy IP**: powoduje uwzględnienie wszystkich adresów IP.
   - **Pojedynczy adres IP**: wpisz adres IPv4 lub IPv6 bądź nazwę hosta.
   - **Zakres (dla IPv4 lub IPv6)**: wpisz zakres adresów IPv4 lub IPv6.
   - **Zakres (dla IPv6)**: wpisz prefiks adresu IPv6 i długość.
   - **Maska podsieci**: wpisz adres IPv4 i jego maskę podsieci.
10. Kliknij przycisk **Zapisz**.

Modyfikowanie wyjątku do wytyczne dla zapory sieciowej

Procedura

1. Przejdź do opcji **Agenci** > **Zapora** > **Reguły**.
2. Kliknij opcję **Edytuj szablon wyjątku**.
3. Kliknij wyjątek reguły.
4. Należy zmodyfikować następujące opcje:
   - Nazwa wyjątku od reguły
   - Typ, nazwa lub ścieżka aplikacji
   - Operacja dotycząca ruchu sieciowego, jaką wykona program OfficeScan, i kierunek tego ruchu
   - Rodzaj protokołu sieciowego
   - Numery portów wyjątku od reguły
   - Agent OfficeScan Adresy IP agentów OfficeScan
5. Kliknij przycisk **Zapisz**.

Zapisywanie ustawień listy wyjątków

Procedura

1. Przejdź do opcji **Agenci** > **Zapora** > **Reguły**.
2. Kliknij opcję **Edytuj szablon wyjątku**.
3. Kliknij jedną z poniższych opcji zapisu:
   - **Zapisz zmiany szablonu**: zapisuje szablon wyjątków z bieżącymi wyjątkami od reguł i ustawieniami. Opcja ta powoduje zastosowanie szablonu wyłącznie do przyszłych reguł, a nie istniejących reguł.

- **Zapisz i zastosuj dla istniejących list reguł**: zapisuje szablon wyjątków z bieżącymi wyjątkami od reguł i ustawieniami. Opcja ta powoduje zastosowanie szablonu do istniejących i przyszłych reguł.

Profile zapory

Profile zapory pozwalają na elastyczny wybór atrybutów, które musi posiadać agent lub grupa agentów przed zastosowaniem reguły. Role użytkowników mogą tworzyć, konfigurować oraz usuwać profile w określonych domenach.

Użytkownicy korzystający z wbudowanego konta administratora lub użytkownicy z pełnymi uprawnieniami do zarządzania mogą również włączyć opcję **Nadpisz poziom zabezpieczeń/listę wyjątków agenta**, aby zastąpić ustawienia profilu agenta OfficeScan ustawieniami serwera.

Profile obejmują:

- **Powiązana reguła**: każdy profil korzysta z jednej reguły.
- **Atrybuty agenta**: Agenci OfficeScan z jednym lub wieloma poniższymi atrybutami stosują powiązaną regułę:
  - **Adres IP**: dowolny Agent OfficeScan o określonym adresie IP, adres IP zawarty w określonym zakresie adresów IP lub adres IP należący do określonej podsieci.
  - **Domena**: dowolny Agent OfficeScan należący do określonej domeny OfficeScan
  - **Punkt końcowy**: Agent OfficeScan o określonej nazwie punktu końcowego.
  - **Platforma**: dowolny Agent OfficeScan obsługujący określoną platformę.
  - **Nazwa logowania**: punkty końcowe agenta OfficeScan, na których zalogowali się określeni użytkownicy.
  - **Opis karty sieciowej**: dowolny punkt końcowy z pasującym opisem karty sieciowej.
  - **Stan połączenia agenta**: czy Agent OfficeScan jest online, czy offline.

Uwaga

Agent OfficeScan jest online, jeśli może się połączyć z serwerem OfficeScan lub dowolnym serwerem odniesienia. Agent offline nie może się połączyć z żadnym serwerem.

Program OfficeScan zawiera domyślny profil o nazwie „ Wszystkie profile agentów", który wykorzystuje regułę „Pełny dostęp". Ten profil domyślny można zmodyfikować lub usunąć. Można również tworzyć nowe profile. Wszystkie domyślne i tworzone przez użytkowników profile zapory, w tym reguły przypisane do poszczególnych profilów oraz bieżące stany profilów, są wyświetlane na liście profilu zapory w konsoli Web. Można zarządzać listą profili i instalować wszystkie profile na agentach OfficeScan. Agenci OfficeScan przechowują wszystkie profile zapory na punktach końcowych agenta OfficeScan.

Konfigurowanie listy profili zapory

Procedura

1. Przejdź do opcji **Agenci** > **Zapora** > **Profile**.
2. Dla użytkowników korzystających z wbudowanego konta administratora lub użytkowników z pełnymi uprawnieniami do zarządzania można dodatkowo włączyć opcję **Nadpisz poziom zabezpieczeń/listę wyjątków agenta**, aby zastąpić ustawienia profilu agenta OfficeScan ustawieniami serwera.
3. Aby dodać nowy profil, kliknij przycisk **Dodaj**. Aby edytować istniejący profil, wybierz nazwę profilu.

   Zostanie wyświetlony ekran konfiguracji profilu. Patrz *Dodawanie i edytowanie profili zapory na stronie 13-21* Aby uzyskać więcej informacji.
4. Aby usunąć istniejący profil, zaznacz pole wyboru znajdujące się obok określonej reguły i kliknij przycisk **Usuń**.
5. Aby zmienić kolejność profilów na liście, zaznacz pole wyboru obok profilu przeznaczonego do przeniesienia, a następnie kliknij przycisk **Przesuń w górę** lub **Przesuń w dół**.

   W programie OfficeScan profile zapory są stosowane do agentów OfficeScan w kolejności, w jakiej występują na liście profili. Na przykład, jeżeli agent jest

zgodny z pierwszym profilem, program OfficeScan zastosuje do agenta operacje określone w tym profilu. Program OfficeScan zignoruje inne profile skonfigurowane dla tego agenta.

Porada

Bardziej szczegółowe reguły należy umieścić na górze listy. Na przykład na górze listy można umieścić reguły utworzone dla pojedynczego agenta, w następnej kolejności dotyczące zakresu agentów i domeny sieciowej, a na końcu — wszystkich agentów.

6. Aby zarządzać serwerami odniesienia, kliknij polecenie **Edytuj listę serwerów odniesienia**. Serwery odniesienia to punkty końcowe, które działają jako zamienniki serwera OfficeScan, gdy ten stosuje profile zapory. Serwerem odniesienia może być dowolny punkt końcowy w sieci (dodatkowe informacje na ten temat zawiera sekcja *Serwery odniesienia na stronie 14-35*). Po włączeniu serwerów odniesienia program OfficeScan przyjmuje następujące założenia:

   - Agenci OfficeScan, którzy są połączeni z serwerami odniesienia, są w trybie online, nawet jeśli agenci nie mogą się komunikować z serwerem OfficeScan.
   - Profile zapory zastosowane do agentów OfficeScan w trybie online są także stosowane do agentów OfficeScan podłączonych do serwerów odniesienia.

Uwaga

Listę serwerów odniesienia mogą wyświetlać i konfigurować wyłącznie użytkownicy korzystający z wbudowanego konta administratora i użytkownicy z pełnymi uprawnieniami do zarządzania.

7. Aby zapisać bieżące ustawienia i przypisać profile do agenta OfficeScan:

   a. Włącz lub wyłącz opcję **Nadpisz poziom zabezpieczeń/listę wyjątków agenta**. Ta opcja powoduje zastąpienie wszystkich ustawień skonfigurowanych przez użytkownika.

   b. Kliknij przycisk **Przypisz profil do agentów**. Program OfficeScan przydziela wszystkie profile z listy profili do wszystkich agentów OfficeScan.

8. Aby sprawdzić, czy pomyślnie przypisano profile do agentów OfficeScan:

   a. Przejdź do opcji **Agenci** > **Zarządzanie agentami**. Z rozwijanego pola widoku drzewa agentów wybierz opcję **Widok zapory**.

b. Sprawdź, czy w kolumnie **Zapora** drzewa agentów znajduje się zielony znacznik wyboru. Jeżeli reguła przypisana do profilu włącza system wykrywania intruzów, w kolumnie **IDS** jest także widoczny zielony znacznik wyboru.

c. Sprawdź, czy agent stosuje prawidłową regułę zapory. Reguła znajduje się w kolumnie **Reguła zapory** drzewa agentów.

Dodawanie i edytowanie profili zapory

Punkty końcowe agentów OfficeScan mogą wymagać różnych poziomów zabezpieczeń. Profile zapory umożliwiają wskazanie, których punktów końcowych dotyczą powiązane reguły. Ogólnie w przypadku każdej stosowanej reguły jest wymagany jeden profil.

Dodawanie profilu zapory

Procedura

1. Przejdź do opcji **Agenci** > **Zapora** > **Profile**.
2. Kliknij przycisk **Dodaj**.
3. Kliknij opcję **Włącz ten profil**, aby umożliwić programowi OfficeScan instalację tego profilu na agentach OfficeScan.
4. Wpisz nazwę identyfikującą profil i opcjonalnie — opis.
5. Wybierz regułę dla tego profilu.
6. Określ punkty końcowe agentów, na których reguły zostaną zastosowane w programie OfficeScan. Wybierz punkty końcowe w oparciu o następujące kryteria:
   - Adres IP
   - Domena: Kliknij przycisk, aby otworzyć drzewo agent i wybrać domeny.

Uwaga

Domeny mogą wybierać tylko użytkownicy mający pełne uprawnienia dostępu do domeny.

- Nazwa Punkt końcowy: Kliknij przycisk, aby otworzyć drzewo agent i wybrać punkty końcowe Agent OfficeScan.
- Platforma
- Nazwa logowania
- Opis karty NIC: wpisz pełny lub częściowy opis; nie używaj znaków specjalnych.

Porada

Firma Trend Micro zaleca wpisanie producenta karty sieciowej, ponieważ opisy takich kart zwykle zaczynają się od nazwy producenta. Jeśli na przykład wpisano „Intel", wszystkie karty sieciowe wyprodukowane przez firmę Intel spełnią kryteria. Jeśli wpisano nazwę konkretnego modelu karty sieciowej, np. „Intel(R) Pro/100", kryteria spełnią tylko te opisy kart sieciowych, które zaczynają się od „Intel(R) Pro/100".

- Stan połączenia agenta

7. Wybierz, czy należy przyznać użytkownikom uprawnienie do zmiany poziomu zabezpieczeń zapory lub do edycji konfigurowalnej listy wyjątków, aby dopuścić określone typy ruchu.

   Szczegółowe informacje zawiera sekcja *Wytyczne dla zapory sieciowej na stronie 13-9*.

8. Kliknij przycisk **Zapisz**.

Modyfikowanie profilu zapory

Procedura

1. Przejdź do opcji **Agenci** > **Zapora** > **Profile**.

2. Kliknij profil.

3. Kliknij opcję **Włącz ten profil**, aby umożliwić programowi OfficeScan instalację tego profilu na agentach OfficeScan. Należy zmodyfikować następujące opcje:

   - Opis i nazwa profilu
   - Reguła przypisana do profilu
   - Agent OfficeScan punktów końcowych agentów OfficeScan w oparciu o następujące kryteria:
     - Adres IP
     - Domena: kliknij przycisk, aby otworzyć drzewo agentów i wybrać z niego domeny.
     - Nazwa punktu końcowego: kliknij przycisk, aby otworzyć drzewo agentów i wybrać z niego punkty końcoweagentów.
     - Platforma
     - Nazwa logowania
     - Opis karty sieciowej: Wpisz pełny lub częściowy opis; nie używaj symboli wieloznacznych.

       Porada

       Firma Trend Micro zaleca wpisanie producenta karty sieciowej, ponieważ opisy takich kart zwykle zaczynają się od nazwy producenta. Jeśli na przykład wpisano „Intel", wszystkie karty sieciowe wyprodukowane przez firmę Intel spełnią kryteria. Jeśli wpisano nazwę konkretnego modelu karty sieciowej, np. „Intel(R) Pro/100", kryteria spełnią tylko te opisy kart sieciowych, które zaczynają się od „Intel(R) Pro/100".

     - Stan połączenia agenta

4. Kliknij przycisk **Zapisz**.

Uprawnienia do zapory

Umożliwia użytkownikom konfigurowanie własnych ustawień zapory. Wszystkie ustawienia konfigurowane przez użytkowników mogą być zastępowane ustawieniami określonymi na serwerze OfficeScan. Jeśli użytkownik wyłączy na przykład system detekcji intruzów (IDS) i włączy go na serwerze OfficeScan, system IDS na punkcie końcowym agenta OfficeScan pozostanie wyłączony.

Włącz następujące ustawienia, aby umożliwić użytkownikom konfigurowanie zapory:

TABELA 13-2. Uprawnienia do zapory

UPRAWNIENIE	OPIS
Wyświetl ustawienia zapory w konsoli agenta OfficeScan	Opcja **Zapora** umożliwia wyświetlenie ustawień zapory w konsoli agenta OfficeScan.
Zezwalaj użytkownikom na włączanie/ wyłączanie zapory, systemu detekcji intruzów (IDS) oraz powiadomień programu o naruszeniu zapory	Zapora programu OfficeScan chroni agentów i serwery w sieci, korzystając z kontroli stanowej — wysoce skutecznego skanowania wirusów sieciowych i eliminacji. W przypadku przydzielenia użytkownikom uprawnienia do włączania i wyłączania zapory oraz jej funkcji należy ich powiadomić, aby w celu uniknięcia narażenia punktu końcowego na ataki intruzów i hakerów nie wyłączali zapory na zbyt długo. Jeśli uprawnienia nie są przydzielone użytkownikom, ustawienia zapory konfigurowane z poziomu konsoli Web serwera OfficeScan są wyświetlane w konsoli agenta OfficeScan w obszarze Lista kart sieciowych.

UPRAWNIENIE	OPIS
Zezwalaj agentom na wysyłanie dzienników zapory na serwer OfficeScan	Tę opcję należy wybrać, aby analizować ruch, który jest blokowany lub akceptowany przez zaporę programu OfficeScan. Szczegółowe informacje o dziennikach zapory zawiera temat *Dzienniki zapory na stronie 13-30*. Jeżeli wybrana zostanie ta opcja, należy skonfigurować harmonogram wysyłania dzienników w pozycji **Agenci** > **Ustawienia agenta globalnego** na karcie **Ustawienia zabezpieczeń**. Przejdź do sekcji **Ustawienia zapory**. Harmonogram dotyczy tylko agentów mających uprawnienie wysyłania dzienników zapory. Instrukcje zawiera sekcja *Globalne ustawienia zapory na stronie 13-26*.

Przyznawanie uprawnień do zapory

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, albo wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Na karcie **Uprawnienia** przejdź do sekcji **Uprawnienia do zapory**.
5. Wybierz następujące opcje:
   - *Wyświetl kartę Zapora w konsoli agenta OfficeScan na stronie 13-24*
   - *Zezwalaj użytkownikom na włączanie/wyłączanie zapory, systemu detekcji intruzów (IDS) oraz powiadomień programu o naruszeniu zapory na stronie 13-24*
   - *Zezwalaj agentom OfficeScan na wysyłanie dzienników zapory na serwer OfficeScan na stronie 13-25*
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

- **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Globalne ustawienia zapory

Globalne ustawienia zapory można zastosować na agentach OfficeScan, korzystając z różnych sposobów.

- Określone ustawienie zapory można zastosować na wszystkich agentach zarządzanych przez serwer.
- Ustawienie można zastosować tylko na agentach OfficeScan, którzy mają przypisane określone uprawnienia do skanowania. Na przykład harmonogram wysyłania dzienników zapory dotyczy tylko agentów OfficeScan mających uprawnienie wysyłania dzienników zapory na serwer.

Wprowadź następujące potrzebne ustawienia globalne:

- **Wysyłaj dzienniki zapory na serwer**

  Można nadać określonym agentom OfficeScan uprawnienia do wysyłania dzienników zapory do serwera OfficeScan. W tej sekcji opisano konfigurację harmonogramu wysyłania dziennika. Z harmonogramu będą korzystali tylko agenci z uprawnieniem do wysyłania dzienników zapory.

  Informacje na temat uprawnień zapory dostępnych wybranym agentom zawiera sekcja *Uprawnienia do zapory na stronie 13-24*.

- **Aktualizuj sterownik zapory programu OfficeScan tylko po ponownym uruchomieniu systemu**

  Aktywuj agenta OfficeScan w celu aktualizacji ogólnego sterownika zapory po każdym ponownym uruchomieniu punktu końcowego agenta OfficeScan. Z tej

opcji należy korzystać w celu uniknięcia zakłócenia pracy punktu końcowego agenta (takiego jak tymczasowe odłączenie od sieci) w przypadku, gdy aktualizacja ogólnego sterownika zapory odbywa się podczas aktualizacji agenta.

- **Wysyłaj informacje dziennika zapory do serwera OfficeScan co godzinę, aby określić możliwość ostrzeżenia zapory o epidemii**

  Po włączeniu tej opcji Agenci OfficeScan wysyłają liczniki dziennika zapory do serwera OfficeScan co godzinę. Szczegółowe informacje o dziennikach zapory zawiera temat *Dzienniki zapory na stronie 13-30*.

  Program OfficeScan korzysta z liczników dziennika oraz kryteriów epidemii naruszeń zapory do oceny możliwości wystąpienia epidemii. Program OfficeScan wysyła powiadomienia e-mail do administratorów OfficeScan w przypadku wystąpienia epidemii.

- Przejdź do sekcji **Ustawienia usługi Certified Safe Software Service** i włącz usługę Certified Safe Software Service zgodnie z potrzebami.

  Usługa Certified Safe Software przeszukuje centra danych firmy Trend Micro w celu weryfikacji bezpieczeństwa programu wykrytego przez blokowanie działania złośliwego oprogramowania, monitorowanie zdarzeń, zaporę lub skanowanie oprogramowania antywirusowego. Należy włączyć włączyć usługę Certified Safe Software, aby zmniejszyć prawdopodobieństwo fałszywych alarmów.

Uwaga

Przed włączeniem usługi Certified Safe Software Service należy się upewnić, że Agenci OfficeScan mają skonfigurowane prawidłowe ustawienia proxy (szczegółowe informacje zawiera sekcja *Ustawienia serwera proxy agenta OfficeScan na stronie 15-52*). Nieprawidłowe ustawienia serwera proxy lub wadliwe połączenie z Internetem mogą być przyczyną opóźnień lub niepowodzenia odbioru odpowiedzi z centrów danych firmy Trend Micro, przez co monitorowane programy będą sprawiać wrażenie zawieszonych.

Ponadto Agenci OfficeScan korzystający wyłącznie z protokołu IPv6 nie mogą bezpośrednio przeszukiwać centrów danych firmy Trend Micro. Aby umożliwić agentom OfficeScan nawiązanie połączenia z centrami danych firmy Trend Micro, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.

Konfigurowanie globalnych ustawień zapory

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Na karcie **Ustawienia zabezpieczeń** przejdź do sekcji **Ustawienia zapory** i skonfiguruj następujące opcje:
   - *Wysyłaj dzienniki zapory na serwer na stronie 13-26*
   - *Aktualizuj sterownik zapory programu OfficeScan tylko po ponownym uruchomieniu systemu na stronie 13-26*
   - *Wysyłaj informacje dziennika zapory do serwera OfficeScan co godzinę, aby określić możliwość ostrzeżenia zapory o epidemii na stronie 13-27*
3. Na karcie **System** przejdź do sekcji **Ustawienia usługi Certified Safe Software Service** i skonfiguruj następujące opcje:
   - *Włącz usługę Certified Safe Software Service dla monitorowania zachowań, zapory i skanowania oprogramowania antywirusowego na stronie 13-27*
4. Kliknij przycisk **Zapisz**.

Powiadamianie użytkowników agenta OfficeScan o naruszeniu zapory

Program OfficeScan może wyświetlać na punktach końcowych powiadomienie programu natychmiast, gdy zapora programu OfficeScan zablokuje ruch wychodzący naruszający ustalone wytyczne dla zapory sieciowej. Użytkownikom można przydzielić uprawnienie do włączania/wyłączania powiadomień programu.

Uwaga

Powiadamianie można również włączyć podczas konfigurowania określonej wytyczne dla zapory sieciowej. W *Dodawanie wytyczne dla zapory sieciowej na stronie 13-11* znajduje się więcej informacji na temat konfiguracji wytyczne dla zapory sieciowej.

Przydzielanie użytkownikom uprawnień do włączania/wyłączania powiadomień programu

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Na karcie **Uprawnienia** przejdź do sekcji **Uprawnienia do zapory**.
5. Wybierz opcję **Zezwalaj użytkownikom na włączanie/wyłączanie zapory, systemu wykrywania intruzów (IDS) oraz powiadomień programu o naruszeniu zapory**.
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Modyfikowanie treści powiadomienia programu od zapory

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Agent**.
2. Na liście rozwijanej **Typ** wybierz opcję **Naruszenia zapory**.
3. Zmodyfikuj domyślny komunikat w odpowiednim polu.
4. Kliknij przycisk **Zapisz**.

Dzienniki zapory

Dzienniki zapory dostępne na serwerze są przesyłane przez agentów OfficeScan mających uprawnienie do wysyłania dzienników zapory. Niektórym agentom można przydzielić uprawnienie do monitorowania i analizowania ruchu odbywającego się na punktach końcowych, które są blokowane przez zaporę programu OfficeScan.

Informacje na temat uprawnień zapory można znaleźć w *Uprawnienia do zapory na stronie 13-24*.

Aby dzienniki nie zajmowały zbyt dużo miejsca na dysku twardym, można je ręcznie usunąć lub skonfigurować harmonogram ich usuwania. Dodatkowe informacje dotyczące dzienników zarządzania zawiera sekcja *Zarządzanie dziennikiem na stronie 14-41*.

Wyświetlanie dzienników zapory

Procedura

1. Przejdź do opcji **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa** lub **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, albo wybierz określone domeny lub agentów.

3. Kliknij polecenie **Dzienniki** > **Dzienniki zapory** lub **Wyświetl dzienniki** > **Dzienniki zapory**.

4. Aby mieć pewność, że są dostępne najnowsze dzienniki, kliknij polecenie **Powiadom agentów**. Przed przejściem do kolejnego punktu poczekaj chwilę, aż agenci prześlą dzienniki zapory.

5. Określ kryteria dziennika i kliknij przycisk **Wyświetl dzienniki**.

6. Wyświetl dzienniki. Dziennik zawiera następujące informacje:

   - Data i godzina wykrycia naruszenia
   - Punkt końcowy, na którym miało miejsce naruszenie zapory
   - Domena punktu końcowego, na którym miało miejsce naruszenie zapory
   - Adres IP zdalnego hosta
   - Adres IP lokalnego hosta
   - Protokół
   - Numer portu
   - Kierunek: jeżeli ruch przychodzący (odbierany) lub wychodzący (wysyłany) naruszył wytyczne dla zapory sieciowej
   - Proces: wykonywalny program lub usługa pracujące na punkcie końcowym, który spowodował naruszenie zapory
   - Opis: określa faktyczne zagrożenie bezpieczeństwa (takie jak atak wirusa sieciowego lub IDS) lub rodzaj naruszenie wytycznych zapory sieciowej

7. Aby zapisać dzienniki w formacie `CSV` (plik z tekstem oddzielanym przecinkami), kliknij opcję **Eksportuj do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Epidemie naruszeń zapory

Epidemia naruszeń zapory jest definiowana przez liczbę naruszeń zapory a oraz przedział czasu.

Program OfficeScan zawiera domyślne powiadomienie informujące administratorów OfficeScan o epidemii. Można zmodyfikować powiadomienie programu zgodnie z potrzebami.

Uwaga

Program OfficeScan może wysyłać powiadomienia o epidemii naruszeń zapory za pomocą poczty e-mail. Należy skonfigurować ustawienia poczty e-mail, aby umożliwić pomyślne wysyłanie powiadomień e-mail przez program OfficeScan. Szczegółowe informacje zawiera sekcja *Ustawienia powiadamiania administratorów na stronie 14-37*.

Konfiguracja kryteriów epidemii naruszeń zapory oraz opcji powiadamiania

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Epidemia**.
2. Na karcie **Kryteria**:
   a. Przejdź do sekcji **Naruszenia zapory**.
   b. Wybierz polecenie **Monitoruj naruszenia zapory na agentach OfficeScan**
   c. Określ liczbę dzienników IDS, dzienników zapory i dzienników wirusów sieciowych.
   d. Określ przedział czasu wykrywania.

Porada

Firma Trend Micro zaleca zaakceptowanie domyślnych wartości na tym ekranie.

Program OfficeScan wysyła komunikat z powiadomieniem po przekroczeniu określonej liczby dzienników. Jeśli na przykład określono 100 dzienników IDS, 100 dzienników zapory, 100 dzienników wirusów sieciowych i przedział czasu 3 godziny, program OfficeScan wyśle powiadomienie, kiedy serwer otrzyma 301 dzienników w ciągu 3 godzin.

3. Na karcie **E-mail**:

   a. Przejdź do sekcji **Epidemie naruszeń zapory**.

   b. Wybierz opcję **Włącz powiadamianie za pomocą wiadomości e-mail**.

   c. Określ odbiorców wiadomości e-mail.

   d. Zaakceptuj lub zmień domyślny temat i wiadomość. Dane w polach **Temat** i **Wiadomość** można przedstawiać za pomocą znaczników.

TABELA 13-3. Zmienne znaczników dla powiadomień o epidemiach naruszeń zapory

ZMIENNA	OPIS
%A	Przekroczony zakres typu dziennika
%C	Liczba dzienników naruszeń zapory
%T	Okres gromadzenia dzienników naruszeń zapory

4. Kliknij przycisk **Zapisz**.

Testowanie zapory OfficeScan

Aby zapewnić prawidłowe działanie zapory programu OfficeScan, należy przeprowadzić test na pojedynczym agencie OfficeScan lub grupie agentów OfficeScan.

OSTRZEŻENIE!

Testy ustawień programu agenta OfficeScan należy przeprowadzać wyłącznie w środowisku kontrolowanym. Testów nie należy przeprowadzać na punktach końcowych podłączonych do sieci lub do Internetu. Działanie takie może narazić punkty końcowe agenta OfficeScan na zagrożenia ze strony wirusów, ataki hakerów i inne niebezpieczeństwa.

Procedura

1. Utwórz i zapisz regułę testową. Skonfiguruj odpowiednie ustawienia w celu blokowania typów ruchu, które będą testowane. Aby na przykład uniemożliwić agentowi OfficeScan uzyskanie dostępu do Internetu:

   a. Ustaw poziom zabezpieczeń na wartość **Niski** (zezwalaj na cały ruch przychodzący/wychodzący).

   b. Wybierz polecenia **Włącz zaporę oraz Powiadamiaj użytkowników o wystąpieniu naruszenia zapory**.

   c. Utwórz wyjątek blokujący ruch HTTP (lub HTTPS).

2. Utwórz i zapisz profil testowy, zaznaczając agentów, na których będą testowane funkcje zapory. Przypisz regułę testową do profilu testowego.

3. Kliknij polecenie **Przypisz profil do agentów**.

4. Zweryfikuj instalację.

   a. Kliknij opcję **Agenci** > **Zarządzanie agentami**.

   b. Wybierz domenę, do której należy agent.

   c. Z widoku drzewa agentów wybierz opcję **Widok zapory**.

   d. Sprawdź, czy w kolumnie **Zapora** drzewa agentów znajduje się zielony znacznik wyboru. Jeśli dla danego agenta włączono system detekcji intruzów, sprawdź, czy zielony znacznik wyboru znajduje się również w kolumnie **IDS**.

   e. Sprawdź, czy agent stosuje prawidłowe wytyczne dla zapory sieciowej. Reguły znajdują się w kolumnie **Wytyczne dla zapory sieciowej** drzewa agentów.

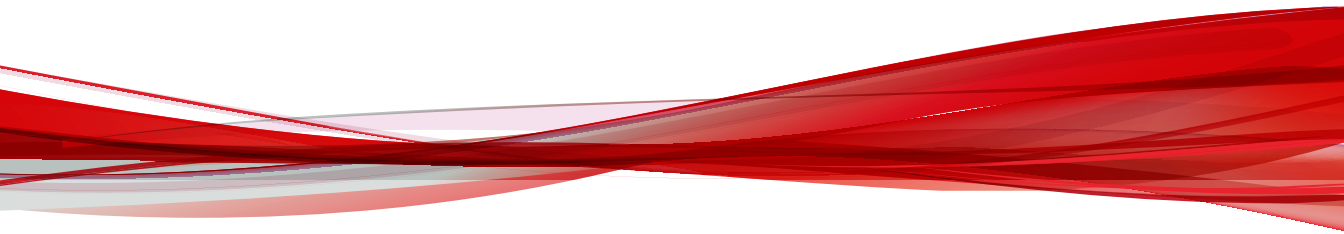
5. W celu przetestowania zapory na punkcie końcowym agenta należy podjąć próbę wysłania lub odebrania typu ruchu skonfigurowanego w regule.

6. W celu przetestowania reguły skonfigurowanej w celu uniemożliwienia agentowi dostępu do Internetu, należy uruchomić przeglądarkę internetową na punkcie końcowym agenta. Jeżeli program OfficeScan skonfigurowano tak, aby w przypadku naruszeń zapory było wyświetlane powiadomienie programu, jest ono

wyświetlane na punkcie końcowym agenta, gdy nastąpi naruszenie ruchu wychodzącego.

Część III

Zarządzanie serwerem OfficeScan i agentami



Rozdział 14

Zarządzanie serwerem OfficeScan

W tym rozdziale przedstawiono zarządzanie serwerami OfficeScan i ich konfigurację.

Rozdział składa się z następujących tematów:

Administracja oparta na rolach

Administracja oparta na rolach umożliwia przyznawanie i kontrolowanie dostępu do konsoli Web programu OfficeScan. Jeśli w organizacji istnieje kilku administratorów OfficeScan, można użyć tej funkcji, aby przydzielić administratorom określone uprawnienia do konsoli Web oraz udzielać im dostępu tylko do niezbędnych narzędzi i uprawnień umożliwiających wykonywanie konkretnych zdań. Można także kontrolować dostęp do drzewa agentów poprzez przydzielenie administratorom jednej lub kilku domen do zarządzania. Ponadto użytkownikom innym niż administratorzy można przyznać uprawnienie dostępu „tylko wyświetlanie" do konsoli Web.

Każdy użytkownik (administrator lub osoba niebędąca administratorem) ma przypisaną określoną rolę. Rola definiuje poziom dostępu do konsoli Web. Użytkownicy logują się do konsoli Web przy użyciu niestandardowych kont użytkowników lub kont usługi Active Directory.

Administracja oparta na rolach dotyczy następujących czynności:

1. Definiowanie roli użytkowników. Szczegółowe informacje zawiera temat *Role użytkowników na stronie 14-3*.

2. Należy skonfigurować konta użytkowników i przydzielić określoną rolę dla każdego konta użytkownika. Szczegółowe informacje zawiera temat *Konta użytkowników na stronie 14-14*.

Działania wykonywane przez wszystkich użytkowników można wyświetlić za pomocą dzienników zdarzeń systemowych. Rejestrowane są następujące działania:

- logowanie w konsoli,
- modyfikacja hasła,
- wylogowywanie z konsoli,
- przekroczenie czasu trwania sesji (użytkownik jest automatycznie wylogowywany).

Role użytkownika

W zależności od przypisanej roli użytkownik może mieć dostęp do różnych elementów menu konsoli Web. Do roli przypisane jest uprawnienie do każdej pozycji menu.

Przypisz uprawnienia do następujących elementów:

Uprawnienia do pozycji menu

Uprawnienia określają poziom dostępu do każdej pozycji menu. Możliwe są następujące uprawnienia do pozycji menu:

- **Konfiguruj**: umożliwia pełny dostęp do pozycji menu. Użytkownicy mogą konfigurować wszystkie ustawienia, wykonywać wszystkie zadania i wyświetlać dane w pozycji menu.
- **Wyświetl**: użytkownicy mogą tylko wyświetlać ustawienia, zadania i dane w pozycji menu.
- **Brak dostępu**: powoduje ukrycie pozycji menu z widoku.

Typy pozycji menu

Dostępne są dwa typy pozycji menu, które można skonfigurować dla ról użytkowników programu OfficeScan.

TABELA 14-1. Typy pozycji menu

TYP	ZAKRES
Pozycje menu dla serwerów/agentów	• Ustawienia, zadania i dane serwera • Ustawienia agenta globalnego, zadania i dane Pełną listę dostępnych pozycji menu zawiera sekcja *Pozycje menu dla serwerów i agentów na stronie 14-5*.

Typ	Zakres
Pozycje menu dla domen zarządzanych	Szczegółowe ustawienia, zadania i dane agenta, które są dostępne poza drzewem agentów Pełną listę dostępnych pozycji menu zawiera sekcja *Pozycje menu dla domen zarządzanych na stronie 14-8*.

Pozycje menu dla serwerów i agentów

Poniższa tabela przedstawia dostępne pozycje menu dla serwerów/agentów:

Uwaga

Pozycje menu są wyświetlane dopiero po aktywowaniu odpowiedniego programu dodatku. Jeśli na przykład Moduł zapobiegania utracie danych nie został aktywowany, na liście nie będą wyświetlane żadne pozycje menu Zapobieganie utracie danych. Wszystkie dodatkowe programy dodatków są wyświetlane w pozycji menu Dodatki.

Dostęp do pozycji menu Dodatki mają tylko użytkownicy z przypisaną rolą "Administrator (wbudowana)".

Tabela 14-2. Pozycje menu Agenci

Pozycja menu najwyższego poziomu	Pozycja menu
Agenci	• Zarządzanie agentami • Grupowanie agentów • Ustawienia agenta globalnego • Lokalizacja punktu końcowego • Zapobieganie utracie danych • Sprawdzanie połączenia • Ochrona przed epidemią

TABELA 14-3. Pozycje menu Dzienniki

POZYCJA MENU NAJWYŻSZEGO POZIOMU	POZYCJA MENU

Dzienniki	• Agenci
	  • Zagrożenia bezpieczeństwa
	  • Aktualizacja składnika agenta
	• Aktualizacje serwera
	• Zdarzenia systemowe
	• Obsługa dziennika

TABELA 14-4. Pozycje menu Aktualizacje

POZYCJA MENU NAJWYŻSZEGO POZIOMU	POZYCJA MENU	POZYCJA PODMENU
Aktualizacje	Serwer	• Zaplanowana aktualizacja • Aktualizacja ręczna • Źródło aktualizacji
	Agenci	• Aktualizacja automatyczna • Źródło aktualizacji
	Wycofywanie	nd.

TABELA 14-5. Pozycje menu Administracja

POZYCJA MENU NAJWYŻSZEGO POZIOMU	POZYCJA MENU	POZYCJA PODMENU
Administracja	Zarządzanie kontami	• Konta użytkowników • Role użytkowników

Pozycja menu najwyższego poziomu	Pozycja menu	Pozycja podmenu
		Uwaga Dostęp do opcji Konta użytkowników i Role użytkowników mają wyłącznie użytkownicy korzystający z wbudowanych ról administratorów.
	Smart Protection	• Źródła Smart Protection • Zintegrowany serwer • Smart Feedback
	Active Directory	• Integracja usługi Active Directory • Synchronizacja zaplanowana
	Powiadomienia	• Ogólne ustawienia • Epidemia • Agent
	Ustawienia	• Serwer proxy • Połączenie agenta • Nieaktywni agenci • Menedżer kwarantanny • Licencja produktu • Control Manager • Konsola Web • Kopia zapasowa bazy danych

Pozycja menu najwyższego poziomu	Pozycja menu	Pozycja podmenu
		• Lista podejrzanych obiektów • Przekaźnik Krawędziowy

Pozycje menu dla domen zarządzanych

Poniższa tabela przedstawia dostępne pozycje menu dla domen zarządzanych:

Tabela 14-6. Pozycja menu Pulpit

Pozycja menu głównego	Pozycja menu
Pulpit **Uwaga** Dostęp do tej strony jest możliwy dla każdego użytkownika niezależnie od uprawnień.	nd.

Tabela 14-7. Pozycje menu Ocena

Pozycja menu najwyższego poziomu	Pozycja menu	Pozycja podmenu
Ocena	Zgodność z zabezpieczeniami	• Raport ręczny • Raport zaplanowany
	Niezarządzane punkty końcowe	nd.

TABELA 14-8. Pozycje menu Agenci

POZYCJA MENU NAJWYŻSZEGO POZIOMU	POZYCJA MENU	POZYCJA PODMENU
Agenci	Zapora	• Reguły • Profile
	Instalacja agenta	• W przeglądarce • Zdalny

TABELA 14-9. Pozycje menu Dzienniki

POZYCJA MENU NAJWYŻSZEGO POZIOMU	POZYCJA MENU	POZYCJA PODMENU
Dzienniki	Agenci	• Sprawdzanie połączenia • Centralne przywracanie kwarantanny • Przywracanie spyware/ grayware

TABELA 14-10. Pozycje menu Aktualizacje

POZYCJA MENU NAJWYŻSZEGO POZIOMU	POZYCJA MENU	POZYCJA PODMENU
Aktualizacje	Podsumowanie	nd.
	Agenci	Aktualizacja ręczna

TABELA 14-11. Pozycje menu Administracja

POZYCJA MENU NAJWYŻSZEGO POZIOMU	POZYCJA MENU	POZYCJA PODMENU
Administracja	Powiadomienia	Administrator

Wbudowane role użytkowników

Program OfficeScan zawiera zestaw wbudowanych ról użytkownika, których nie można modyfikować ani usuwać. Wbudowane role są następujące:

TABELA 14-12. Wbudowane role użytkowników

NAZWA ROLI	OPIS
Administrator	Tę rolę należy przydzielić innym administratorom programu OfficeScan lub użytkownikom mającym odpowiednią wiedzę na temat programu OfficeScan. Użytkownicy z tą rolę mają uprawnienie „Konfiguruj” do wszystkich pozycji menu. **Uwaga** Dostęp do pozycji menu Dodatki mają tylko użytkownicy z przypisaną rolą “Administrator (wbudowana)”.

Nazwa roli	Opis

Użytkownik-gość	Tę rolę należy przydzielić użytkownikom, którzy chcą wyświetlać konsolę Web w celach informacyjnych.
	• Użytkownicy z tą rolą nie mają dostępu do następujących pozycji menu:
	  • Dodatki
	  • **Administracja** > **Zarządzanie kontami** > **Role użytkowników**
	  • **Administracja** > **Zarządzanie kontami** > **Konta użytkowników**
	• Użytkownicy mają uprawnienie „Wyświetl” do wszystkich innych pozycji menu.

Użytkownik uprzywilejowany Trend (rola tylko do uaktualniania)	Ta rola jest dostępna tylko w przypadku aktualizacji z programu OfficeScan 10. Ta rola dziedziczy uprawnienia z roli „Użytkownik uprzywilejowany” w programie OfficeScan 10. Użytkownicy z tą rolą mają uprawnienie „Konfiguruj” do wszystkich domen w drzewie agentów, lecz nie będą mieli dostępu do nowych funkcji w tej wersji.

Role niestandardowe

Jeśli żadna z wbudowanych ról nie spełnia wymagań, można dodać role niestandardowe.

Uprawnienia do tworzenia niestandardowych ról użytkowników i przydzielania tych ról do kont użytkowników mają wyłącznie użytkownicy z wbudowaną rolą administratora oraz użytkownicy korzystający z konta głównego utworzonego podczas instalacji programu OfficeScan.

Dodawanie ról niestandardowych

Procedura

1. Przejdź do opcji **Administracja** > **Zarządzanie kontami** > **Role użytkowników**.

2. Kliknij przycisk **Dodaj**. Jeśli rola, którą chcesz utworzyć, ma podobne ustawienia, jak istniejąca rola, zaznacz tę rolę i kliknij opcję **Kopiuj**.

   Zostanie wyświetlony nowy ekran.

3. Wpisz nazwę roli oraz w razie potrzeby wprowadź odpowiedni opis.

4. Kliknij opcję **Pozycje menu dla serwerów/agentów** i określ uprawnienie do poszczególnych pozycji menu, jakie są dostępne. Listę dostępnych pozycji menu zawiera sekcja *Pozycje menu dla serwerów i agentów na stronie 14-5*.

5. Kliknij opcję **Pozycje menu dla domen zarządzanych** i określ uprawnienie do poszczególnych pozycji menu, jakie są dostępne. Listę dostępnych pozycji menu zawiera sekcja *Pozycje menu dla domen zarządzanych na stronie 14-8*.

6. Kliknij przycisk **Zapisz**.

   Nowa rola zostanie wyświetlona na liście Role użytkowników.

Modyfikowanie ról niestandardowych

Procedura

1. Przejdź do opcji **Administracja** > **Zarządzanie kontami** > **Role użytkowników**.

2. Kliknij nazwę roli.

   Zostanie wyświetlony nowy ekran.

3. Zmodyfikuj następujące opcje:

   - Opis
   - Uprawienia roli
     - **Pozycje menu dla serwerów/agentów**
     - **Pozycje menu dla domen zarządzanych**

4. Kliknij przycisk **Zapisz**.

Usuwanie ról niestandardowych

Procedura

1. Przejdź do opcji **Administracja** > **Zarządzanie kontami** > **Role użytkowników**.
2. Zaznacz pole wyboru obok roli.
3. Kliknij przycisk **Usuń**.

Uwaga

Roli nie można usunąć, jeśli została przydzielona do co najmniej jednego konta użytkownika.

Import lub eksport ról niestandardowych

Procedura

1. Przejdź do opcji **Administracja** > **Zarządzanie kontami** > **Role użytkowników**.
2. Aby wyeksportować role niestandardowe do pliku `.dat`:
   a. Wybierz role i kliknij przycisk **Eksportuj**.
   b. Zapisz plik `.dat`. Jeśli zarządzasz innym serwerem OfficeScan, wykorzystaj plik `.dat` w celu zaimportowania niestandardowych ról na ten serwer.

   Uwaga

   Operację eksportowania ról można wykonywać wyłącznie między serwerami w takiej samej wersji.
3. Aby wyeksportować role niestandardowe do pliku `.csv`:
   a. Wybierz role i kliknij przycisk **Eksportuj ustawienia ról**.
   b. Zapisz plik `.csv`. Ten plik można wykorzystać do sprawdzenia informacji i uprawnień dotyczących wybranych ról.

4. Jeśli masz plik z niestandardowymi rolami zapisany za pomocą innego serwera OfficeScan i chcesz go zaimportować na bieżący serwer OfficeScan, kliknij polecenie **Importuj** i wskaż plik `.dat` zawierający role niestandardowe.

   - W przypadku importowania roli o takiej samej nazwie, jak istniejąca rola, rola na ekranie Role użytkowników zostanie zastąpiona.
   - Operację importowania ról można wykonywać wyłącznie między serwerami w takiej samej wersji.
   - Rola zaimportowana z innego serwera OfficeScan:
     - Zachowuje uprawnienia do pozycji menu dla serwerów/agentów oraz do pozycji menu dla domen zarządzanych.
     - Stosuje uprawnienia domyślne do pozycji menu zarządzania agentami. Na innym serwerze należy zapisać uprawnienia ról do pozycji menu zarządzania agentami, a następnie zastosować je ponownie do zaimportowanej roli.

Konta użytkownika

Można konfigurować konta użytkowników i przydzielać określone role poszczególnym użytkownikom. W zależności od przypisanej roli użytkownik może wyświetlać i konfigurować różne elementy menu konsoli Web.

Podczas instalacji serwera OfficeScan program instalacyjny automatycznie tworzy wbudowane konto o nazwie „główne". Użytkownicy logujący się za pomocą tego konta (nazywanego „kontem głównym") mają dostęp do wszystkich elementów menu. Konta głównego nie można usunąć, ale można modyfikować jego parametry, takie jak hasło, pełna nazwa czy opis. W przypadku zapomnienia hasła do konta głównego należy się skontaktować z dostawcą obsługi technicznej w celu uzyskania pomocy dotyczącej ponownego ustawienia hasła.

Można dodawać konta niestandardowe oraz konta usługi Active Directory. Wszystkie konta użytkowników są wyświetlane na liście Konta użytkowników w konsoli Web.

Przypisz uprawnienie kont użytkowników do wyświetlania lub konfigurowania szczegółowych ustawień agenta, zadań i danych dostępnych w drzewie agentów. Pełną

listę dostępnych pozycji menu drzewa agentów zawiera sekcja *Pozycje menu zarządzania agentami na stronie 14-15*.

Uwaga

Po aktualizacji serwera OfficeScan konieczna jest edycja kont niestandardowych i ręczne włączenie wszystkich nowych funkcji w uprzednio dodanych kontach niestandardowych. Można to zrobić na ekranie **Krok 3 Zdefiniuj menu drzewa agentów**. Szczegółowe informacje o uprawnieniach zawiera sekcja *Definiowanie uprawnień domen na stronie 14-20*.

Kont użytkownika programu OfficeScan można użyć w celu dokonania „jednokrotnej rejestracji". Rejestracja jednokrotna zapewnia użytkownikom możliwość dostęp do konsoli Web programu OfficeScan z poziomu konsoli programu Trend Micro Control Manager . Szczegółowe informacje przedstawiono w poniższej procedurze.

Pozycje menu zarządzania agentami

Poniższa tabela przedstawia dostępne pozycje menu zarządzania agentami:

Uwaga

Pozycje menu są wyświetlane dopiero po aktywowaniu odpowiedniego programu dodatku. Jeśli na przykład Moduł zapobiegania utracie danych nie został aktywowany, na liście nie będą wyświetlane żadne pozycje menu Zapobieganie utracie danych.

TABELA 14-13. Pozycje menu zarządzania agentami

POZYCJA MENU GŁÓWNEGO	PODMENU
Stan	nd.
Zadania	• Skanuj teraz • Dezinstalacja agenta • Centralne przywracanie kwarantanny • Przywracanie spyware/grayware

Pozycja menu głównego	Podmenu

Ustawienia	• Ustawienia skanowania
	  • Metody skanowania
	  • Ustawienia skanowania ręcznego
	  • Ustawienia skanowania w czasie rzeczywistym
	  • Ustawienia skanowania zaplanowanego
	  • Ustawienia funkcji Skanuj teraz
	• Ustawienia usługi Web Reputation
	• Ustawienia podejrzanego połączenia
	• Ustawienia monitorowania zachowań
	• Ustawienia kontroli urządzeń
	• Ustawienia DLP
	• Przesyłanie próbek
	• Ustawienia agenta aktualizacji
	• Uprawnienia i inne ustawienia
	• Dodatkowe ustawienia usługi
	• Lista dozwolonych spyware/grayware
	• Lista zaufanych programów
	• Ustawienia przewidującego uczenia maszynowego
	• Ustawienia eksportu
	• Importowanie ustawień

Pozycja menu głównego	Podmenu
Dzienniki	• Dzienniki wirusów/złośliwego oprogramowania • Dzienniki spyware/grayware • Dzienniki zapory • Dzienniki usługi Web Reputation • Dzienniki podejrzanego połączenia • Dzienniki podejrzanych plików • Dzienniki wywołań zwrotnych C&C • Dzienniki monitorowania zachowań • Dzienniki przewidującego uczenia maszynowego • Dzienniki kontroli urządzeń • Dzienniki Zapobieganie utracie danych • Dzienniki operacji skanowania • Usuń dzienniki
Zarządzanie drzewem agentów	• Dodawanie domeny • Zmiana nazwy domeny • Przenieś agenta • Usuń domenę/agenta
Eksportuj	nd.

Dodawanie kont niestandardowych

Procedura

1. Przejdź do opcji **Administracja** > **Zarządzanie kontami** > **Konta użytkowników**.
2. Kliknij przycisk **Dodaj**.

Zostanie wyświetlony ekran **Krok 1 Informacje o użytkowniku**.

3. Wybierz opcję **Włącz to konto**.

4. Z listy rozwijanej **Wybierz rolę** wybierz wcześniej skonfigurowaną rolę.

   Szczegółowe informacje o tworzeniu ról użytkowników zawarto w temacie *Role niestandardowe na stronie 14-11*.

5. Wpisz nazwę użytkownika, opis i hasło, a następnie potwierdź hasło.

   Ważne

   Nazwa użytkownika musi się różnić od hasła do konta. Wpisz inne hasło.

6. Wpisz adres e-mail przypisany do konta.

   Uwaga

   Program OfficeScan wysyła powiadomienia na ten adres e-mail. Powiadomienia informują odbiorcę o wykrytych zagrożeniach bezpieczeństwa i transmisjach zasobów cyfrowych. Szczegółowe informacje na temat powiadomień zawiera sekcja *Powiadamianie administratorów o zagrożeniach bezpieczeństwa na stronie 7-91*.

7. Kliknij przycisk **Dalej**.

   Zostanie wyświetlony ekran **Krok 2 Kontrola domeny agenta**.

8. Zdefiniuj zakres drzewa agentów, wybierając domenę główną albo jedną lub kilka domen w drzewie agentów.

   W tym momencie zostały zdefiniowany tylko domeny. Poziom dostępu do wybranych domen zostanie zdefiniowany w kroku 10.

9. Kliknij przycisk **Dalej**.

   Zostanie wyświetlony ekran **Krok 3 Zdefiniuj menu drzewa agentów**.

10. Kliknij opcję **Dostępne pozycje menu** i określ uprawnienie do poszczególnych pozycji menu. Listę dostępnych pozycji menu zawiera sekcja *Pozycje menu zarządzania agentami na stronie 14-15*.

    Zakres drzewa agentów, który skonfigurowano w kroku 8, określa poziom uprawnienia do pozycji menu i definiuje cele dla uprawnienia. Zakresem drzewa

agentów może być domena główna (wszyscy agenci) lub określone domeny drzewa agentów.

Tabela 14-14. Pozycje menu Zarządzanie agentami i zakres drzewa agentów

<table>
<tr><th rowspan="2">Kryteria</th><th colspan="2">Zakres drzewa agentów</th></tr>
<tr><th>Domena główna</th><th>Określone domeny</th></tr>
<tr><td>Uprawnienie do pozycji menu</td><td>Konfiguruj, Wyświetl lub Brak dostępu</td><td>Konfiguruj, Wyświetl lub Brak dostępu</td></tr>
<tr><td rowspan="2">Cel</td><td>Domena główna (wszyscy agenci) lub określone domeny

Na przykład można przyznać roli uprawnienie „Konfiguruj” do pozycji menu „Zadania” w drzewie agentów. Jeśli celem jest domena główna, użytkownik może inicjować zadania na wszystkich agentach. Jeśli celami są domeny A i B, zadania mogą zostać zainicjowane tylko na agentach w domenach A i B.</td><td>Tylko wybrane domeny

Na przykład można przyznać roli uprawnienie „Konfiguruj” do pozycji menu „Ustawienia” w drzewie agentów. Oznacza to, że użytkownik może stosować ustawienia, ale wyłącznie do agentów w wybranych domenach.</td></tr>
<tr><td colspan="2">Drzewo agentów zostanie wyświetlone tylko w przypadku, gdy uprawnieniem do pozycji menu Zarządzanie agentami w sekcji „Pozycje menu dla serwerów/agentów” jest „Wyświetl”.</td></tr>
</table>

- W przypadku zaznaczenia pola wyboru **Konfiguruj** zostanie automatycznie zaznaczone pole wyboru **Wyświetl**.
- Jeśli nie zostanie zaznaczone żadne pole wyboru, uprawnieniem będzie „Brak dostępu”.
- Jeśli konfigurowane są uprawnienia dla określonej domeny, można skopiować uprawnienia do innych domen, klikając opcję **Skopiuj ustawienia wybranej domeny do innych domen**.

11. Kliknij przycisk **Zakończ**.

12. Wyślij szczegóły konta do użytkownika.

Definiowanie uprawnień domen

W przypadku definiowania uprawnień domen program OfficeScan automatycznie stosuje uprawnienia domeny nadrzędnej w odniesieniu do wszystkich poddomen, którymi zarządza. Poddomena nie może mieć mniejszych uprawnień, niż jej domena nadrzędna. Jeśli przykładowo administrator systemu ma uprawnienia do wyświetlania i konfigurowania wszystkich agentów, którymi zarządzania program OfficeScan (domena "serwera OfficeScan"), uprawnienia poddomen muszą umożliwiać administratorowi systemu dostęp do tych funkcji konfiguracji. Po usunięciu uprawnienia w poddomenie administrator systemu nie będzie miał pełnych uprawnień do konfiguracji na wszystkich agentach.

W przypadku poniższej procedury drzewo domeny wygląda następująco:

Aby przykładowo przyznać kontu użytkownika "Chris" uprawnienia do wyświetlania i konfigurowania określonych opcji menu poddomeny "Pracownicy" oraz tylko uprawnienie do wyświetlania dzienników w domenie nadrzędnej "Menedżerowie", należy wykonać następujące czynności.

TABELA 14-15. Uprawnienia konta użytkownika "Chris"

DOMENA	ŻĄDANE UPRAWIENIA
Serwer OfficeScan	Brak specjalnych uprawnień
Menedżerowie	Wyświetlanie **dzienników**

DOMENA	ŻĄDANE UPRAWIENIA
Pracownicy	Wyświetlanie i konfigurowanie **zadań** Wyświetlanie i konfigurowanie **dzienników** Wyświetlanie **ustawień**
Sprzedaż	Brak specjalnych uprawnień

Procedura

1. Przejdź do ekranu **Konta użytkowników: krok 3 Zdefiniuj menu drzewa agentów**.
2. Kliknij domenę "Serwer OfficeScan".
3. Wyczyść wszystkie pola wyboru **Wyświetlanie** i **Konfiguracja**.

> **Uwaga**
>
> Domenę "Serwer OfficeScan" można konfigurować tylko wtedy, jeśli wybrało się jej wszystkie poddomeny na ekranie **Konta użytkowników: Krok 2 Kontrola domeny agenta**.

4. Kliknij domenę "Sprzedaż".
5. Wyczyść wszystkie pola wyboru **Wyświetlanie** i **Konfiguracja**.

> **Uwaga**
>
> Domena "Sprzedaż" zostanie wyświetlona tylko po jej wybraniu na ekranie **Konta użytkowników: Krok 2 Kontrola domeny agenta**.

6. Kliknij domenę "Menedżerowie".
7. Zaznacz pole wyboru "Wyświetlanie dzienników" i wyczyść wszystkie pozostałe pola wyboru **Wyświetlanie** i **Konfiguracja**.
8. Kliknij ponownie domenę "Pracownicy".
9. Wybierz następujące elementy dla użytkownika Chris:

- **Zadania**: wyświetlanie i konfigurowanie
- **Dzienniki**: wyświetlanie i konfigurowanie
- **Ustawienia**: wyświetlanie

Użytkownik Chris może teraz wyświetlać i konfigurować wybrane opcje menu poddomeny "Pracownicy" oraz tylko wyświetlać **Dzienniki** w domenie "Menedżerowie".

Jeśli użytkownik Chris ma uprawnienia do wyświetlania i konfigurowania domeny "Menedżerowie", program OfficeScan automatycznie przyzna te same uprawnienia w odniesieniu do poddomeny "Pracownicy". Dzieje się tak, ponieważ domena "Menedżerowie" zarządza wszystkimi należącymi do niej poddomenami.

Modyfikowanie kont niestandardowych

Uwaga

Po aktualizacji serwera OfficeScan konieczna jest edycja kont niestandardowych i ręczne włączenie wszystkich nowych funkcji w uprzednio dodanych kontach niestandardowych. Można to zrobić na ekranie **Krok 3 Zdefiniuj menu drzewa agentów**. Szczegółowe informacje o uprawnieniach zawiera sekcja *Definiowanie uprawnień domen na stronie 14-20*.

Procedura

1. Przejdź do opcji **Administracja** > **Zarządzanie kontami** > **Konta użytkowników**.
2. Kliknij konto użytkownika.
3. Włącz lub wyłącz konto, korzystając z pola wyboru.
4. Należy zmodyfikować następujące opcje:
   - Rola
   - Opis
   - Hasło

Uwaga

Podczas edycji konta nie można wpisać hasła, które było już używane. Aby dalej używać starego hasła, nie zmieniaj zawartości pola **Hasło**.

- Adres e-mail

5. Kliknij przycisk **Dalej**.
6. Zdefiniuj zakres drzewa agentów.
7. Kliknij przycisk **Dalej**.
8. Kliknij opcję **Dostępne pozycje menu** i określ uprawnienie do poszczególnych pozycji menu.

   Listę dostępnych pozycji menu zawiera sekcja *Pozycje menu zarządzania agentami na stronie 14-15*.
9. Kliknij przycisk **Zakończ**.
10. Wyślij szczegóły nowego konta do użytkownika.

Dodawanie kont lub grup usług Active Directory

Procedura

1. Przejdź do opcji **Administracja** > **Zarządzanie kontami** > **Konta użytkowników**.
2. Kliknij przycisk **Dodaj**.

   Zostanie wyświetlony ekran **Krok 1 Informacje o użytkowniku**.
3. Wybierz opcję **Włącz to konto**.
4. Z listy rozwijanej **Wybierz rolę** wybierz wcześniej skonfigurowaną rolę.

   Szczegółowe informacje o tworzeniu ról użytkowników zawarto w temacie *Role niestandardowe na stronie 14-11*.

5. Wybierz opcję **Użytkownik lub grupa Active Directory**.

Ważne

Aby możliwe było zarządzanie kontami użytkowników, serwer OfficeScan musi zostać dołączony do domeny Active Directory.

6. Znajdź konto (nazwę użytkownika lub grupę), określając nazwę użytkownika i domenę, do której należy konto.

Uwaga

Do wyszukiwania wielu kont użyj znaku (*). Jeśli symbol wieloznaczny nie zostanie zastosowany, należy wpisać pełną nazwę konta. Program OfficeScan nie zwraca wyników, jeśli nazwa konta jest niekompletna lub jeśli używana jest domyślna grupa „Użytkownicy domeny".

7. Gdy program OfficeScan wyszuka prawidłowe konto, wyświetli jego nazwę w sekcji **Użytkownicy i grupy**. Aby zmienić położenie konta w sekcji **Wybrani użytkownicy i grupy**, kliknij ikonę strzałki (>).

   W przypadku określenia grupy usługi Active Directory wszystkim członkom tej grupy zostanie przypisana taka sama rola. Jeśli określone konto należy do co najmniej dwóch grup, a role wybrane dla poszczególnych grup są inne:

   - Uprawnienia obu grup są łączone. Jeśli użytkownik skonfigurował określone ustawienie i występuje konflikt między uprawnieniami do tego ustawienia, jest stosowane uprawnienie wyższego poziomu.
   - Wszystkie role użytkowników są wyświetlane w dziennikach zdarzeń systemowych. Na przykład „Użytkownik John Doe jest zalogowany z następującymi rolami: administrator, użytkownik uprzywilejowany".

8. Kliknij przycisk **Dalej**.

   Zostanie wyświetlony ekran **Krok 2 Kontrola domeny agenta**.

9. Zdefiniuj zakres drzewa agentów.

10. Kliknij przycisk **Dalej**.

    Zostanie wyświetlony ekran **Krok 3 Zdefiniuj menu drzewa agentów**.

11. Kliknij opcję **Dostępne pozycje menu** i określ uprawnienie do poszczególnych pozycji menu.

    Listę dostępnych pozycji menu zawiera sekcja *Pozycje menu zarządzania agentami na stronie 14-15*.

12. Kliknij przycisk **Zakończ**.

13. Poinformuj użytkownika o możliwości logowania się do konsoli Web za pomocą jego hasła i nazwy domeny.

Trend Micro Control Manager

Narzędzie Trend Micro™ Control Manager™ jest centralną konsolą zarządzania produktami i usługami Trend Micro zabezpieczającymi bramę, serwer poczty, serwer plików oraz komputery w firmie. Konsola Web zarządzania programu Control Manager to pojedynczy punkt monitorowania zarządzanych produktów i usług w całej sieci.

Narzędzie Control Manager umożliwia administratorom systemu monitorowanie i raportowanie takiej aktywności, jak infekcje, naruszenie bezpieczeństwa lub miejsca przenikania wirusów. Administratorzy systemu mogą pobierać i wysyłać elementy w sieci, zapewniając spójność i aktualność zabezpieczeń. Program Control Manager umożliwia zarówno ręczne jak i zaplanowane aktualizacje oraz konfigurowanie i administrowanie produktami w grupach lub indywidualnie, co zapewnia większą elastyczność.

Integracja z programem Control Manager w bieżącej wersji programu OfficeScan

Ta wersja programu OfficeScan zapewnia następujące funkcje umożliwiające zarządzanie serwerami OfficeScan za pomocą programu Control Manager:

- Tworzenie, wdrażanie i obsługiwanie reguł funkcji Antywirus, Zapobieganie utracie danych i Kontrola urządzeń programu OfficeScan oraz przydzielanie uprawnień bezpośrednio do agentów OfficeScan z konsoli programu Control Manager.Agenci OfficeScan

Poniższa tabela zawiera konfiguracje reguł dostępne w programie Control Manager 6.0 z dodatkiem SP3 i poprawką 2.

TABELA 14-16. OfficeScan Rodzaje opcji zarządzania regułami w programie Control Manager

TYP REGUŁY	FUNKCJE
Ustawienia programu antywirusowego i agenta programu OfficeScan	• Dodatkowe ustawienia usługi • Ustawienia monitorowania zachowań • Ustawienia kontroli urządzeń • Ustawienia skanowania ręcznego • Uprawnienia i inne ustawienia • Ustawienia skanowania w czasie rzeczywistym • Lista dozwolonych spyware/ grayware • Metody skanowania • Ustawienia funkcji Skanuj teraz • Ustawienia skanowania zaplanowanego • Ustawienia podejrzanego połączenia • Lista zaufanych programów • Ustawienia agenta aktualizacji • Ustawienia usługi Web Reputation

TYP REGUŁY	FUNKCJE
Ochrona danych	Ustawienia reguł Zapobieganie utracie danych **Uwaga** Zarządzanie uprawnieniami do funkcji Kontrola urządzeń dla Ochrona danych w regułach agenta OfficeScan.

- Za pomocą konsoli programu Control Manager między serwerami OfficeScan można replikować następujące ustawienia:
  - *Typy identyfikatorów danych na stronie 11-5*
  - *Szablony Zapobieganie utracie danych na stronie 11-21*

Uwaga

Jeśli te ustawienia zostaną zreplikowane na serwerach OfficeScan, na których nie aktywowano licencji Ochrona danych, ustawienia zostaną zastosowane dopiero po aktywowaniu tej licencji.

Obsługiwane wersje programu Control Manager

Ta wersja programu OfficeScan obsługuje następujące wersje programu Control Manager:

- Control Manager 6.0 lub nowszy

Szczegółowe informacje o adresach IP, które serwer OfficeScan i Agenci OfficeScan raportują do programu Control Manager, zawiera temat *Ekrany wyświetlające adresy IP na stronie A-7*.

Aby można było za pomocą programu Control Manager zarządzać wersjami programu OfficeScan, należy zastosować najnowsze poprawki i pakiety hot fix o znaczeniu krytycznym przeznaczone do programu Control Manager. W celu uzyskania najnowszych poprawek i pakietów hot fix należy się skontaktować z dostawcą obsługi technicznej lub odwiedzić Centrum aktualizacji firmy Trend Micro pod adresem:

http://www.trendmicro.com/download/emea/?lng=emea

Po zainstalowaniu programu OfficeScan należy go zarejestrować w programie Control Manager, a następnie skonfigurować ustawienia OfficeScan w konsoli zarządzania programu Control Manager. Informacje o zarządzaniu serwerami OfficeScan zawiera *dokumentacja programu Control Manager*.

Rejestrowanie serwera OfficeScan w programie Control Manager

Ważne

Po uaktualnieniu programu OfficeScan 10.6 SP3 lub starszego do programu OfficeScan XG lub nowszego należy wyrejestrować połączenie z serwerem Control Manager i ponownie zarejestrować połączenie w przypadku zamiaru korzystania z autoryzacji certyfikatu.

Procedura

1. Przejdź do opcji **Administracja** > **Ustawienia** > **Control Manager**.
2. Wprowadź nazwę wyświetlaną jednostki. Jest to nazwa serwera OfficeScan, która będzie widoczna w programie Control Manager.

   Domyślnie ta nazwa zawiera nazwę komputera serwera oraz nazwę używanego produktu (na przykład Serwer01_OSCE).

   Uwaga

   W programie Control Manager, serwery OfficeScan i inne produkty zarządzane przez program Control Manager są określane jako „jednostki”.
3. Określ nazwę FQDN lub adres IP serwera Control Manager, a także numer portu, który ma być wykorzystany do połączenia się z tym serwerem. Opcjonalnie skorzystaj z połączenia o podwyższonym bezpieczeństwie przy użyciu protokołu HTTPS.

   - W przypadku serwera OfficeScan z dwoma stosami wpisz nazwę FQDN lub adres IP (IPv4 lub IPv6, jeśli jest dostępna) programu Control Manager.

- W przypadku serwera OfficeScan korzystającego wyłącznie z protokołu IPv4 wpisz nazwę FQDN lub adres IPv4 programu Control Manager.
- W przypadku serwera OfficeScan korzystającego wyłącznie z protokołu IPv6 wpisz nazwę FQDN lub adres IPv6 programu Control Manager.

4. Obok pozycji **Certyfikat serwera Control Manager** kliknij przycisk **Przeglądaj** i wybierz plik certyfikatu pobrany z docelowego serwera Control Manager.

   Aby uzyskać plik certyfikatu serwera Control Manager, przejdź do serwera Control Manager i skopiuj plik certyfikatu na serwer OfficeScan z następującej lokalizacji:

   ```
   <folder instalacji programu Control Manager>\Certificate\CA
   \TMCM_CA_Cert.pem
   ```

   Ważne

   Jeśli firma używa dostosowanego certyfikatu na serwerze Control Manager, należy przesłać certyfikat głównego urzędu certyfikacji podczas rejestracji programu Control Manager.

   Aby uzyskać więcej informacji, patrz *Autoryzacja certyfikatu serwera Control Manager na stronie 14-30*.

5. Jeżeli serwer Web IIS programu Control Manager wymaga uwierzytelnienia, należy wprowadzić nazwę użytkownika i hasło.

6. W przypadku korzystania z serwera proxy w celu połączenia się z serwerem Control Manager określ poniższe ustawienia serwera proxy:

   - Protokół proxy:
   - Nazwa FQDN lub adres IPv4/IPv6 i port serwera
   - Identyfikator użytkownika i hasło uwierzytelniania serwera proxy

7. Określ, czy będzie wykorzystywane przekierowanie portów komunikacji jednokierunkowej lub dwukierunkowej, a następnie określ adres IPv4/IPv6 oraz port.

8. Aby sprawdzić, czy program OfficeScan może być połączony z serwerem Control Manager na podstawie ustawień określonych przez użytkownika, należy kliknąć opcję **Połączenie testowe**.

   Jeśli udało się nawiązać połączenie, kliknij polecenie **Zarejestruj**.

9. Jeśli jest używany serwer programu Control Manager w wersji 6.0 SP1 lub nowszej, zostanie wyświetlony komunikat z monitem o użycie serwera programu Control Manager jako źródła aktualizacji dla zintegrowanego serwera Smart Protection programu OfficeScan. Kliknij przycisk **OK**, aby użyć serwera programu Control Manager jako źródła aktualizacji zintegrowanego serwera Smart Protection, lub przycisk **Anuluj**, aby kontynuować użycie bieżącego źródła aktualizacji (domyślnie jest to serwer ActiveUpdate).

10. Jeśli po rejestracji na tym ekranie zostaną wprowadzone zmiany, po wprowadzaniu zmian kliknij opcję **Zaktualizuj ustawienia** w celu powiadomienia serwera Control Manager o wprowadzonych zmianach.

Uwaga

Jeśli serwer Control Manager jest połączony z serwerem Deep Discovery, proces automatycznej subskrypcji rozpocznie się po ukończeniu rejestracji. Aby uzyskać więcej informacji, patrz *Ustawienia listy podejrzanych obiektów na stronie 14-33*.

11. Jeżeli nie ma potrzeby dalszego zarządzania programem OfficeScan przez program Control Manager, kliknij przycisk **Wyrejestruj**.

Autoryzacja certyfikatu serwera Control Manager

Przed zarejestrowaniem programu OfficeScan na serwerze Control Manager należy najpierw uzyskać plik certyfikatu programu Control Manager z serwera Control Manager, który znajduje się w następującym miejscu:

```
<folder instalacji programu Control Manager>\Certificate\CA
\TMCM_CA_Cert.pem
```

Programy OfficeScan i Control Manager używają certyfikatu i szyfrowania kluczem publicznym w celu zapewnienia, że między serwerami odbywa się tylko autoryzowana komunikacja na potrzeby rejestracji i zarządzania regułami. Jeśli dowolny serwer wykryje nieautoryzowaną komunikację, odrzuci rejestrację lub otrzymane ustawienia reguł.

Ważne

Jeśli firma używa dostosowanego certyfikatu na serwerze Control Manager, należy przesłać certyfikat głównego urzędu certyfikacji podczas rejestracji programu Control Manager.

Sprawdzanie stan programu OfficeScanna konsoli zarządzania Control Manager

Procedura

1. Otwórz konsolę zarządzania Control Manager.

   Aby otworzyć konsolę programu Control Manager na dowolnym punkcie końcowym w sieci, otwórz przeglądarkę internetową i wprowadź poniższy adres:

   `https://<Nazwa serwera programu Control Manager>/Webapp/login.aspx`

   Gdzie `<Nazwa serwera programu Control Manager>` jest adresem IP lub nazwą hosta serwera programu Control Manager

2. W menu głównym kliknij kolejno opcje **Katalogi** > **Produkty**.

3. W wyświetlonym drzewie przejdź do folderu **[Serwer programu Control Manager]** > **Folder lokalny** > **Nowy obiekt**.

4. Sprawdź, czy jest wyświetlana ikona serwera OfficeScan.

Narzędzie do eksportowania wytycznych

Narzędzie do eksportowania wytycznych w programie Trend Micro OfficeScan Server umożliwia administratorom eksportowanie ustawień reguł programu OfficeScan, które są obsługiwane przez program Control Manager 6.0 lub nowszy. Administratorzy potrzebują także narzędzia do importowania programu Control Manager w celu importowania reguł. Narzędzie do eksportowania wytycznych obsługuje program OfficeScan 10.6 z dodatkiem Service Pack 1 lub nowszy.

- Ustawienia skanowania w czasie rzeczywistym
- Ustawienia skanowania zaplanowanego
- Ustawienia skanowania ręcznego
- Ustawienia funkcji Skanuj teraz
- Ustawienia agenta aktualizacji
- Ustawienia usługi Web Reputation
- Metoda skanowania
- Ustawienia monitorowania zachowań
- Ustawienia kontroli urządzeń
- Ustawienia Zapobieganie utracie danych
- Uprawnienia i inne ustawienia
- Dodatkowe ustawienia usługi
- Lista dozwolonych spyware/grayware
- Ustawienia podejrzanego połączenia

Używanie narzędzie do eksportowania wytycznych

Procedura

1. Na komputerze serwera OfficeScan przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\PolicyExportTool`.

2. Dwukrotnie kliknij plik `PolicyExportTool.exe`, aby uruchomić narzędzie do eksportowania wytycznych.

   Zostanie otwarty ekran interfejsu wiersza polecenia, a narzędzie do eksportowania wytycznych rozpocznie eksportowanie ustawień. Narzędzie tworzy dwa foldery (`PolicyClient` i `PolicyDLP`) w folderze `PolicyExportTool`, które zawierają wyeksportowane ustawienia.

3. Skopiuj dwa foldery do folderu instalacji programu Control Manager.

4. Wykonaj narzędzie do importowania reguł na serwerze Control Manager.

   Szczegółowe informacje dotyczące narzędzia do importowania reguł zawiera *plik Readme narzędzia do importowania reguł* na serwerze Control Manager (`folder_instalacji_TMCM\WebUI\WebApp\widget\common\tool\PolicyImport\`).

Uwaga

Narzędzie do eksportowania wytycznych nie eksportuje dostosowanych identyfikatorów danych ani dostosowanych szablonów DLP. Jeśli administrator musi wyeksportować dostosowane identyfikatory danych i szablony DLP, należy wykonać ręczne eksportowanie z konsoli programu OfficeScan, a następnie ręcznie zaimportować plik przy użyciu konsoli programu Control Manager.

Ustawienia listy podejrzanych obiektów

Podejrzane obiekty to cyfrowe artefakty wynikające z analizy realizowanej przez produkty Trend Micro Deep Discovery lub pochodzącej z innych źródeł. Program OfficeScan pozwala na synchronizację podejrzanych obiektów i realizację działań pobranych z serwera Control Manager 6.0 SP3 lub nowszego (połączonego z serwerem Deep Discovery).

Po zasubskrybowaniu programu Control Manager wybierz typy podejrzanych obiektów, aby monitorować wywołania zwrotne C&C lub potencjalne ataki ukierunkowane zidentyfikowane przez program agenci w sieci. Podejrzane obiekty to między innymi:

- Lista podejrzanych adresów URL
- Lista podejrzanych adresów IP
- Lista podejrzanych plików

Uwaga

W programie OfficeScan w wersjach od 10.6 do 11.0 głównym źródłem podejrzanych obiektów jest usługa Deep Discovery Analyzer. Od wersji OfficeScan 11.0 SP1 głównym źródłem jest program Control Manager 6.0 SP3, który zapewnia lepsze funkcje zarządzania podejrzanymi obiektami i sprawniejszy proces ich obsługi.

Jeśli program OfficeScan jest subskrybowany w usłudze Deep Discovery Analyzer, dostępna jest tylko lista podejrzanych adresów URL. Po anulowaniu subskrypcji programu OfficeScan z usługi Deep Discovery Analyzer nie ma możliwości ponownego subskrybowania. Aby synchronizować podejrzane obiekty, program OfficeScan musi być subskrybowany w programie Control Manager połączonym z usługą Deep Discovery.

By uzyskać więcej informacji o tym, jak program Control Manager zarządza podejrzanymi obiektami, zapoznaj się z *Podręcznikiem administratora programu Control Manager*.

Konfigurowanie ustawień listy podejrzanych obiektów

Podczas rejestracji programu OfficeScan program Control Manager wdraża klucz API w programie OfficeScan, aby rozpocząć proces subskrypcji. Aby włączyć automatyczny proces subskrypcji, należy skontaktować się z administratorem serwera Control Manager i upewnić się, że ma on połączenie z funkcją Control Manager, a wymagane ustawienia zostały skonfigurowane.

Szczegółowe informacje na temat rejestrowania serwera Control Manager zawiera sekcja *Rejestrowanie serwera OfficeScan w programie Control Manager na stronie 14-28*.

Procedura

1. Przejdź do opcji **Administracja** > **Ustawienia** > **Lista podejrzanych obiektów**.
2. Wybierz listę, która ma być włączona na agentach.
   - Lista podejrzanych adresów URL
   - Lista podejrzanych adresów IP (dostępna tylko po dokonaniu subskrypcji serwera Control Manager)
   - Lista podejrzanych plików (dostępna tylko po dokonaniu subskrypcji serwera Control Manager)

Administratorzy mogą w dowolnym momencie wykonać ręczną synchronizację list podejrzanych obiektów, klikając przycisk **Synchronizuj teraz**.

3. W sekcji **Aktualizuj listę podejrzanych obiektów w agentach OfficeScan** określ, kiedy agenci mają aktualizować listy podejrzanych obiektów.

   - **Na podstawie harmonogramu aktualizacji składników agentów OfficeScan**: Agenci OfficeScan aktualizują listy podejrzanych obiektów na podstawie bieżącego harmonogramu aktualizacji.
   - **Automatycznie po aktualizacji list podejrzanych obiektów na serwerze**: Agenci OfficeScan automatycznie aktualizują listy podejrzanych obiektów po otrzymaniu przez serwer OfficeScan zaktualizowanych list.

   Uwaga

   Agenci OfficeScan, którzy nie są skonfigurowani do odbierania aktualizacji z agentów aktualizacji, wykonują aktualizacje przyrostowe zasubskrybowanych list podejrzanych obiektów podczas synchronizacji.

4. Kliknij przycisk **Zapisz**.

Serwery odniesienia

Jednym ze sposobów określenia przez agenta Agent OfficeScan używanych reguł lub profili jest sprawdzenie stanu połączenia z serwerem OfficeScan. Jeśli wewnętrzny Agent OfficeScan (lub dowolny agent w sieci korporacyjnej) nie może się połączyć z serwerem, jego stan zmienia się na offline. Agent stosuje wtedy regułę lub profil przeznaczone dla agentów zewnętrznych. Rozwiązaniem tego problemu może być użycie serwerów odniesienia.

Agent OfficeScan, który utraci połączenie z serwerem OfficeScan, próbuje nawiązać połączenie z serwerami odniesienia. W przypadku pomyślnego nawiązania połączenia agenta z serwerem odniesienia zostaną zastosowane reguły lub profile odpowiednie dla agentów wewnętrznych.

Reguły i profile zarządzane przez serwery referencyjne obejmują:

- Profile zapory
- Reguły Web Reputation
- Reguły Ochrona danych
- Reguły kontroli urządzeń

Należy wziąć pod uwagę następujące kwestie:

- Jako serwer odniesienia należy przypisać komputer o odpowiednich możliwościach, taki jak serwer sieci Web, serwer SQL lub serwer FTP. Można określić do 320 serwerów odniesienia.
- Agenci OfficeScan łączą się najpierw z pierwszym serwerem na liście serwerów odniesienia. W przypadku niepowodzenia agent usiłują nawiązać połączenie z kolejnymi serwerami na liście.
- Agenci OfficeScan używają serwerów odniesienia podczas określania ustawień antywirusowych (Monitorowanie zachowań, Kontrola urządzeń, profile zapory, reguły Web Reputation) oraz ustawień Ochrona danych, które zostaną użyte. Serwery odniesienia nie umożliwiają zarządzania agentami, instalowania aktualizacji ani zmiany ustawień agentów. Tego typu zadania są przeprowadzane przez serwer OfficeScan.
- Agent OfficeScan nie ma możliwości wysyłania dzienników do serwerów odniesienia ani używania tych serwerów jako źródeł aktualizacji.

Zarządzanie listą serwerów odniesienia

Procedura

1. Przejdź do opcji **Agenci** > **Zapora** > **Profile** lub **Agenci** > **Lokalizacja punktu końcowego**.
2. W zależności od wyświetlonego ekranu wykonaj następujące czynności:
   - Jeśli wyświetlany jest ekran **Profile zapory dla agentów**, kliknij polecenie **Edytuj listę serwerów odniesienia**.

- Jeśli wyświetlany jest ekran **Lokalizacja punktu końcowego**, kliknij **listę serwerów odniesienia**.

3. Wybierz polecenie **Włącz listę serwerów odniesienia**.
4. Aby dodać punkt końcowy do listy, kliknij przycisk **Dodaj**.
   a. Określ adres IPv4/IPv6 punktu końcowego, jego nazwę lub w pełni kwalifikowaną nazwę domeny (FQDN), na przykład:
      - `computer.networkname`
      - `12.10.10.10`
      - `mycomputer.domain.com`
   b. Wpisz port, za pośrednictwem którego agenci komunikują się z tym punktem końcowym. Można wybrać dowolny port otwarty na serwerze odniesienia (np. 20, 23 lub 80).

      Uwaga

      Aby określić inny port na tym samym serwerze odniesienia, należy powtórzyć czynności opisane w punktach 2a i 2b. Agent OfficeScan korzysta najpierw z pierwszego portu na liście. Gdy nie można nawiązać połączenia, wybiera kolejny port.

   c. Kliknij przycisk **Zapisz**.
5. Aby edytować ustawienia punktu końcowego na liście, kliknij jego nazwę. Zmień nazwę punktu końcowego lub port, a następnie kliknij przycisk **Zapisz**.
6. Aby usunąć punkt końcowy z listy, zaznacz jego nazwę i kliknij przycisk **Usuń**.
7. Aby punkty końcowe działały jako serwery odniesienia, kliknij przycisk **Przypisz do agentów**.

Ustawienia powiadamiania administratorów

Aby zapewnić prawidłowe działanie funkcji wysyłania przez program OfficeScan powiadomień za pomocą poczty elektronicznej i pułapki SNMP, należy skonfigurować

ustawienia powiadamiania administratorów. Program OfficeScan może także wysyłać powiadomienia za pomocą dziennika zdarzeń systemu Windows NT, ale dla tego kanału powiadomień nie są konfigurowane żadne ustawienia.

Program OfficeScan może wysyłać do administratorów OfficeScan powiadomienia po wykryciu następujących zdarzeń:

TABELA 14-17. Przypadki wykrycia powodujące wysłanie powiadomień do administratorów

PRZYPADKI WYKRYCIA	KANAŁY POWIADOMIEŃ		
	POCZTA ELEKTRONICZNA	PUŁAPKA SNMP	DZIENNIKI ZDARZEŃ SYSTEMU WINDOWS NT
Wirusy i złośliwe oprogramowanie	Tak	Tak	Tak
Spyware i grayware	Tak	Tak	Tak
Transmisje zasobów cyfrowych	Tak	Tak	Tak
Wywołania zwrotne C&C	Tak	Tak	Tak
Epidemie wirusów i złośliwego oprogramowania	Tak	Tak	Tak
Epidemie spyware i grayware	Tak	Tak	Tak
Epidemie naruszeń zapory	Tak	Nie	Nie
Epidemie sesji folderów udostępnionych	Tak	Nie	Nie
Epidemie wywołań zwrotnych C&C	Tak	Tak	Tak

Konfigurowanie ogólnych ustawień powiadomień

Procedura

1. Przejdź do opcji **Administracja** > **Powiadomienia** > **Ogólne ustawienia**.
2. Skonfiguruj ustawienia powiadomień e-mail.
   a. Określ adres IPv4/IPv6 lub nazwę punktu końcowego w polu **Serwer SMTP**.
   b. Określ numer portu z zakresu od 1 do 65535.
   c. Podaj adres e-mail.

      Jeśli chcesz włączyć protokół ESMTP w następnym kroku, podaj prawidłowy adres e-mail.
   d. Włącz protokół **ESMTP** (opcjonalnie).
   e. Podaj nazwę użytkownika i hasło dla adresu e-mail wprowadzonego w polu **Od**.
   f. Wybierz metodę uwierzytelniania agenta na serwerze:
      - **Logowanie**: logowanie to starsza wersja agenta użytkownika poczty. Zarówno serwer, jak i agent używają kodowania BASE64 do uwierzytelniania nazwy użytkownika i hasła.
      - **Zwykły tekst**: zwykłego tekstu używa się najłatwiej, ale ta metoda może być niebezpieczna, ponieważ nazwa użytkownika i hasło są wysyłane jako jeden ciąg zakodowany przy użyciu metody BASE64 przed przesłaniem przez Internet.
      - **CRAM-MD5**: CRAM-MD5 korzysta z połączenia mechanizmu uwierzytelniania typu wezwanie/odpowiedź i algorytmu kryptograficznego Message Digest 5 w celu wymiany i uwierzytelniania informacji.
3. Skonfiguruj ustawienia powiadomień przez pułapkę SNMP.
   a. Określ adres IPv4/IPv6 lub nazwę punktu końcowego w polu **Adres IP serwera**.

b. Określ trudną do odgadnięcia nazwę społeczności.

Uwaga

Ze względu na kwestie bezpieczeństwa nazwa społeczności jest wyświetlana jako zamaskowana wartość z użyciem znaku (*). Domyślna przypisana wartość to: "publiczna".

4. Kliknij przycisk **Zapisz**.

Dzienniki zdarzeń systemowych

Program OfficeScan zapisuje w dziennikach informacje o zdarzeniach związanych z działaniem programu serwera, takich jak wyłączenie i uruchomienie. Dzienniki te służą do sprawdzania, czy serwer OfficeScan i usługi działają prawidłowo.

Aby dzienniki nie zajmowały zbyt dużo miejsca na dysku twardym, można je ręcznie usunąć lub skonfigurować harmonogram ich usuwania. Dodatkowe informacje dotyczące dzienników zarządzania zawiera sekcja *Zarządzanie dziennikiem na stronie 14-41*.

Przeglądanie dzienników zdarzeń systemu

Procedura

1. Przejdź do opcji **Dzienniki** > **Zdarzenia systemowe**.
2. W obszarze **Zdarzenie** sprawdź dzienniki, które wymagają działania. Program OfficeScan rejestruje następujące zdarzenia:

TABELA 14-18. Dzienniki zdarzeń systemowych

TYP DZIENNIKA	ZDARZENIA
OfficeScan Master Service i serwer bazy danych:	• Uruchomiono usługę Master • Pomyślnie zatrzymano usługę główną • Zatrzymanie usługi głównej nie powiodło się
Ochrona przed epidemią	• Włączono ochronę przed epidemią • Wyłączono ochronę przed epidemią • Liczba sesji folderów udostępnionych w ciągu ostatnich <ilość minut>
Kopia zapasowa bazy danych	• Tworzenie kopii zapasowej bazy danych powiodło się • Pomyślnie wykonano kopię zapasową bazy danych
Oparty na rolach dostęp do konsoli Web	• logowanie w konsoli, • modyfikacja hasła, • wylogowywanie z konsoli, • Przekroczenie czasu trwania sesji (użytkownik jest automatycznie wylogowywany).
Uwierzytelnianie serwera	• Agent OfficeScan otrzymał nieprawidłowe polecenia z serwera • Certyfikat uwierzytelniający jest nieprawidłowy lub wygasł

3. Aby zapisać dzienniki w formacie CSV (plik z tekstem oddzielanym przecinkami), kliknij opcję **Eksportuj do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Zarządzanie dziennikiem

Program OfficeScan obszerne dzienniki, w których odnotowywane są informacje o wykrytych zagrożeniach bezpieczeństwa, zdarzeniach oraz aktualizacjach. Dzienników

tych można użyć do oceny reguł ochrony, a także do identyfikacji agentów OfficeScan, którzy są bardziej narażeni na zarażenie wirusami i ataki. Ponadto za pomocą dzienników można sprawdzić połączenie między agentem a serwerem i ustalić, czy aktualizacje składników zostały prawidłowo zainstalowane.

Program OfficeScan korzysta również z centralnego mechanizmu weryfikacji czasu do zapewnienia zgodności czasu serwera OfficeScan i agentów. Zapobiega to niespójności danych dziennika powodowanych przez strefy czasowe, czas letni oraz różnice czasu, która może prowadzić do trudności podczas analizy danych zapisanych w dziennikach.

Uwaga

Program OfficeScan przeprowadza weryfikację czasu w odniesieniu do wszystkich dzienników z wyjątkiem serwera aktualizacji i dzienników zdarzeń systemowych.

Serwer OfficeScan otrzymuje następujące dzienniki od agentów Agenci OfficeScan:

- *Wyświetlanie dzienników wirusów/złośliwego oprogramowania na stronie 7-102*
- *Wyświetlanie dzienników oprogramowania spyware/grayware na stronie 7-111*
- *Wyświetlanie dzienników przywracania po usunięciu oprogramowania spyware/grayware na stronie 7-115*
- *Wyświetlanie dzienników zapory na stronie 13-30*
- *Wyświetlanie dzienników usługi Web Reputation na stronie 12-23*
- *Przeglądanie dzienników podejrzanego połączenia na stronie 8-15*
- *Wyświetlanie dzienników podejrzanych plików na stronie 7-115*
- *Wyświetlanie dzienników wywołań zwrotnych C&C na stronie 12-24*
- *Wyświetlanie dzienników monitorowania zachowań na stronie 9-19*
- *Wyświetlanie dzienników kontroli urządzeń na stronie 10-19*
- *Wyświetlanie dzienników operacji skanowania: na stronie 7-116*
- *Wyświetlanie dzienników Zapobieganie utracie danych na stronie 11-61*

- *Wyświetlanie dzienników aktualizacji agenta OfficeScan na stronie 6-54*
- *Wyświetlanie dzienników sprawdzania połączenia na stronie 15-47*

Serwer OfficeScan tworzy następujące dzienniki:

- *Dzienniki aktualizacji serwera OfficeScan na stronie 6-28*
- *Dzienniki zdarzeń systemowych na stronie 14-40*

Na serwerze OfficeScan i agentach OfficeScan dostępne są również następujące dzienniki:

- *Dziennik zdarzeń systemu Windows na stronie 18-26*
- *Dzienniki serwera OfficeScan na stronie 18-3*
- *Dzienniki agenta OfficeScan na stronie 18-14*

Obsługa dziennika

Aby dzienniki nie zajmowały zbyt dużo miejsca na dysku twardym, można je ręcznie usunąć lub skonfigurować harmonogram ich usuwania za pomocą konsoli Web.

Usuwanie dzienników na podstawie harmonogramu

Procedura

1. Przejdź do opcji **Dzienniki** > **Obsługa dziennika**.
2. Zaznacz pole **Włącz planowe usuwanie dzienników**.
3. Wybierz typy dzienników do usunięcia. Wszystkie dzienniki wygenerowane przez program OfficeScan z wyjątkiem dzienników diagnostycznych mogą być usuwane zgodnie z harmonogramem. W przypadku dzienników diagnostycznych należy wyłączyć funkcję rejestracji danych, aby zatrzymać pobieranie informacji do dzienników.

Uwaga

W przypadku dzienników wirusów/złośliwego oprogramowania można usuwać dzienniki utworzone przez określone typy skanowania i Usługi Usuwania Szkód Services. W przypadku dzienników programowania spyware/grayware można usuwać dzienniki dotyczące określonych typów skanowania. Szczegółowe informacje o typach skanowania zawiera temat *Rodzaje skanowania na stronie 7-15*.

4. Ustal, czy mają być usuwane dzienniki wszystkich wybranych typów, czy tylko starsze niż określona liczba dni.
5. Określ czas i częstotliwość usuwania dzienników.
6. Kliknij przycisk **Zapisz**.

Ręczne usuwanie dzienników

Procedura

1. Przejdź do opcji **Dzienniki** > **Agenci** > **Zagrożenia bezpieczeństwa** lub **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Wykonaj jedną z następujących czynności:
   - W przypadku dostępu do ekranu **Dzienniki zagrożeń bezpieczeństwa** kliknij opcję **Usuń dzienniki**.
   - W przypadku dostępu do ekranu **Zarządzanie agentami** kliknij kolejno opcje **Dzienniki** > **Usuń dzienniki**.
4. Wybierz typy dzienników do usunięcia. Tylko następujące typy dzienników mogą być usuwane ręcznie:
   - Dzienniki monitorowania zachowań
   - Dzienniki wywołań zwrotnych C&C

- Dzienniki Zapobieganie utracie danych
- Dzienniki kontroli urządzeń
- Dzienniki zapory
- Dzienniki przewidującego uczenia maszynowego
- Dzienniki spyware/grayware
- Dzienniki operacji skanowania
- Dzienniki podejrzanego połączenia
- Dzienniki podejrzanych plików
- Dzienniki wirusów/złośliwego oprogramowania
- Dzienniki usługi Web Reputation

Uwaga

W przypadku dzienników wirusów/złośliwego oprogramowania można usuwać dzienniki utworzone przez określone typy skanowania i Usługi Usuwania Szkód Services. W przypadku dzienników programowania spyware/grayware można usuwać dzienniki dotyczące określonych typów skanowania.

Szczegółowe informacje o typach skanowania zawiera temat *Rodzaje skanowania na stronie 7-15*.

5. Ustal, czy mają być usuwane dzienniki wszystkich wybranych typów, czy tylko starsze niż określona liczba dni.
6. Kliknij przycisk **Usuń**.

Licencje

W konsoli Web można przeglądać, uaktywniać i odnawiać usługi licencji OfficeScan, a także włączać i wyłączać zaporę programu OfficeScan. Zapora programu OfficeScan to element usługi Antywirus, która obsługuje również ochronę przed epidemią.

Uwaga

Niektóre natywne funkcje programu OfficeScan, takie jak Ochrona danych i Virtual Desktop Support, mają własne licencje. Do aktywowania licencji tych funkcji i zarządzania nimi służy program Plug-in Manager. Szczegółowe informacje na temat licencjonowania tych funkcji zawierają sekcje *Licencja Ochrona danych na stronie 3-4* i *Licencja Virtual Desktop Support na stronie 15-82*.

Serwer OfficeScan wykorzystujący wyłącznie protokół IPv6 nie może połączyć się z serwerem Trend Micro Online Registration Server w celu aktywacji/odnowienia licencji. Aby umożliwić serwerowi OfficeScan nawiązanie połączenia z serwerem rejestracji, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate.

Wyświetlanie informacji o licencji produktu

Procedura

1. Przejdź do opcji **Administracja** > **Ustawienia** > **Licencja produktu**.
2. Sprawdź podsumowanie stanu licencji widoczne w górnej części ekranu. Przypomnienia dotyczące licencji są wyświetlane w następujących przypadkach:

TABELA 14-19. Przypomnienia o licencji

TYP LICENCJI	PRZYPOMNIENIE
Pełna wersja	• Podczas okresu próbnego korzystania z produktu. Czas trwania okresu próbnego różni się w zależności od regionu. Informacje na ten temat można uzyskać u przedstawiciela firmy Trend Micro. • Po wygaśnięciu licencji i upływie okresu próbnego. W tym okresie nie ma możliwości korzystania z pomocy technicznej ani dokonywania aktualizacji składników. Silniki skanowana będą jednak skanować punkty końcowe, używając nieaktualnych składników. Te nieaktualne składniki mogą nie zapewniać pełnej ochrony przed najnowszymi zagrożeniami bezpieczeństwa.

Typ licencji	Przypomnienie
Wersja próbna	Po wygaśnięciu licencji. W tym okresie program OfficeScan wyłącza aktualizację składników. Silniki skanowana będą jednak skanować punkty końcowe, używając nieaktualnych składników. Te nieaktualne składniki mogą nie zapewniać pełnej ochrony przed najnowszymi zagrożeniami bezpieczeństwa.

3. Wyświetl informacje o licencji. W sekcji **Informacje o licencji** znajdują się następujące informacje:

   - **Usługi**: dotyczy wszystkich usług licencji OfficeScan.
   - **Stan**: wyświetlana jest wartość „Aktywowane”, „Nieaktywowane”, „Wygasłe” lub „W okresie próbnym”. Jeśli dla usługi jest wiele licencji, a co najmniej jedna z nich jest nadal aktywna, wyświetlany jest stan „Aktywowane”.
   - **Wersja**: wyświetlana jest wartość „Pełna” lub „Próbna”. Jeśli używane są obie wersje, wyświetlana jest wersja „Pełna”.
   - **Data wygaśnięcia**: jeśli dla usługi jest wiele licencji, wyświetlana jest najpóźniejsza data wygaśnięcia. Na przykład, jeśli licencje wygasają w dniach 31-12-2007 i 30-06-2008, wyświetlana jest data 30-06-2008.

   Uwaga

   Nieaktywowane usługi licencji mają wersję i datę wygaśnięcia o wartości „nd”.

4. Program OfficeScan umożliwia aktywację wielu licencji usług. Aby wyświetlić wszystkie licencje przypisane do wybranej usługi (aktywne i wygasłe), należy kliknąć jej nazwę.

Aktywacja lub odnowienie licencji

Procedura

1. Przejdź do opcji **Administracja** > **Ustawienia** > **Licencja produktu**.

2. Kliknij nazwę usługi licencji.
3. Na ekranie **Szczegóły dotyczące licencji produktu** kliknij polecenie **Nowy kod aktywacyjny**.
4. Na wyświetlonym ekranie wpisz Kod aktywacyjny i kliknij przycisk **Zapisz**.

Uwaga

Przed aktywowaniem usługi należy ją zarejestrować. Aby uzyskać więcej informacji na temat klucza rejestracyjnego i kodu aktywacyjnego, należy się skontaktować z przedstawicielem firmy Trend Micro.

5. Na ekranie **Szczegóły dotyczące licencji produktu** kliknij opcję **Informacja o aktualizacji**, aby odświeżyć ekran ze szczegółami nowej licencji i stanem usługi. Ekran ten zawiera także łącze do witryny internetowej firmy Trend Micro, na której znajdują się szczegółowe informacje o licencji.

Kopia zapasowa bazy danych OfficeScan

Baza danych serwera OfficeScan zawiera wszystkie ustawienia programu OfficeScan, w tym także ustawienia i uprawnienia skanowania. Jeżeli baza danych serwera zostanie uszkodzona, można ją odtworzyć na podstawie wcześniej utworzonej kopii zapasowej. Kopię zapasową bazy danych można utworzyć ręcznie w dowolnym momencie lub skonfigurować harmonogram jej tworzenia.

Podczas wykonywania kopii zapasowej bazy danych program OfficeScan automatycznie wykonuje defragmentację bazy danych i naprawia potencjalne uszkodzenia w pliku indeksu.

Stan kopii zapasowej można sprawdzić w dzienniku zdarzeń systemowych. Aby uzyskać więcej informacji, patrz *Dzienniki zdarzeń systemowych na stronie 14-40*.

Porada

Firma Trend Micro zaleca skonfigurowanie harmonogramu automatycznego tworzenia kopii zapasowej. Kopię zapasową bazy danych należy wykonywać poza godzinami szczytu, kiedy ruch w obszarze serwera jest niewielki.

OSTRZEŻENIE!

Do tworzenia kopii zapasowych nie należy używać innych typów narzędzi ani aplikacji. Konfigurowanie kopii zapasowej bazy danych należy przeprowadzać wyłącznie z konsoli Web programu OfficeScan.

Tworzenie kopii zapasowych bazy danych OfficeScan

Procedura

1. Przejdź do opcji **Administracja** > **Ustawienia** > **Kopia zapasowa bazy danych**.
2. Wpisz lokalizację, w której chcesz zapisać bazę danych. Jeśli ten folder jeszcze nie istnieje, wybierz polecenie **Utwórz folder, jeśli nie istnieje**. W ścieżce uwzględnij dysk i pełną ścieżkę do katalogu, np. `c:\OfficeScan\DatabaseBackup`.

   Domyślnie program OfficeScan zapisuje kopię zapasową w następującym katalogu: <*Folder instalacji serwera*>`\DBBackup`

   Uwaga

   Program OfficeScan utworzy podfolder w ścieżce kopii zapasowej. Nazwa folderu zawiera informację o czasie wykonania kopii zapasowej i ma następujący format: RRRRMMDD_HHMMSS. Program OfficeScan zachowuje 7 ostatnich folderów kopii zapasowej, automatycznie usuwając starsze foldery.

3. Jeżeli ścieżka kopii zapasowej znajduje się na komputerze zdalnym (jest to ścieżka UNC), wprowadź odpowiednią nazwę konta i hasło. Upewnij się, że konto ma przypisane uprawnienia do zapisu na komputerze.
4. Aby skonfigurować harmonogram tworzenia kopii zapasowej:
   a. Wybierz polecenie **Włącz zaplanowane tworzenie kopii zapasowej bazy danych**.
   b. Określ częstotliwość i godzinę wykonywania kopii zapasowej.

c. Aby wykonać kopię zapasową bazy danych i zapisać wprowadzone zmiany, kliknij polecenie **Twórz kopię zapasową teraz**. Aby zapisać bez tworzenia kopii zapasowej bazy danych, kliknij przycisk **Zapisz**.

Przywracanie plików kopii zapasowej bazy danych

Procedura

1. Zatrzymaj OfficeScan Master Service.
2. Zastąp pliki bazy danych w lokalizacji <*Folder instalacji serwera*>\PCCSRV\HTTPDB plikami kopii zapasowej.
3. Ponownie uruchom OfficeScan Master Service.

Narzędzie SQL Server Migration Tool

Administratorzy mogą dokonać migracji istniejącej bazy danych OfficeScan z natywnego stylu CodeBase do bazy danych SQL Server przy użyciu narzędzia SQL Server Migration Tool. Narzędzie SQL Server Migration Tool obsługuje następujące rodzaje migracji bazy danych:

- baza danych CodeBase programu OfficeScan do nowej bazy danych SQL Server Express,
- baza danych CodeBase programu OfficeScan do istniejącej bazy danych SQL Server,
- baza danych SQL programu OfficeScan (wcześniej poddana migracji), która została przeniesiona do innej lokalizacji.

Użycie narzędzia SQL Server Migration Tool

Narzędzie SQL Server Migration Tool umożliwia migrację istniejącej bazy danych CodeBase do bazy danych SQL przy użyciu programu SQL Server 2014 SP2 Express.

Porada

Po ukończeniu migracji bazy danych OfficeScan można przenieść nowo migrowaną bazę danych SQL na inny serwer SQL Server. Uruchom ponownie narzędzie SQL Server Migration Tool i wybierz opcję **Przełącz na istniejącą bazę danych SQL programu OfficeScan**, aby użyć innego serwera SQL Server.

Procedura

1. Na serwerze OfficeScan przejdź do folderu <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\SQL`.

2. Kliknij dwukrotnie plik `SQLTxfr.exe`, aby uruchomić narzędzie.

   Zostanie otwarta konsola narzędzia **SQL Server Migration Tool**.

3. Wybierz typ migracji:

Opcja	Opis
Zainstaluj nowy program SQL Server 2014 SP2 Express i przeprowadź migrację bazy danych OfficeScan	Automatycznie instaluje program SQL Server 2014 SP2 Express i migruje istniejącą bazę danych OfficeScan do nowej bazy danych SQL **Uwaga** Program OfficeScan automatycznie przydziela port 1433 serwerowi SQL Server.
Przeprowadź migrację bazy danych OfficeScan na istniejący serwer SQL Server	Migruje istniejącą bazę danych OfficeScan do nowej bazy danych SQL na istniejącym serwerze SQL Server
Przełącz na istniejącą bazę danych SQL programu OfficeScan	Zmienia ustawienia konfiguracji programu OfficeScan w celu wskazania istniejącej bazy danych SQL programu OfficeScan na istniejącym serwerze SQL Server

4. Podaj **Nazwę serwera** w następujący sposób:

   - W przypadku nowych instalacji SQL: nazwa hosta lub adres IP serwera SQL> \<nazwa wystąpienia

- W przypadku migracji serwera SQL Server: nazwa hosta lub adres IP serwera SQL>,<numer portu>\<nazwa wystąpienia
- Przy przełączaniu na istniejącą bazę danych SQL programu OfficeScan: nazwa hosta lub adres IP serwera SQL>,<numer portu>\<nazwa wystąpienia

Ważne

Program OfficeScan automatycznie tworzy wystąpienie dla bazy danych OfficeScan podczas instalacji serwera SQL Server. W czasie migracji istniejącego serwera SQL Server lub bazy danych wpisz nazwę istniejącego wystąpienia dla wystąpienia programu OfficeScan na serwerze SQL Server.

5. Określ poświadczenia uwierzytelniania dla bazy danych SQL Server.
   - Gdy do zalogowania na serwerze używa się **Konta Windows, nazwa użytkownika** musi mieć następujący format:

     nazwa_domeny\nazwa_użytkownika lub nazwa_użytkownika

     Ważne

     Konto użytkownika musi należeć do grupy administratorów lokalnych lub wbudowanego administratora Active Directory (AD), a ponadto konieczne jest skonfigurowanie następujących zasad przypisywania uprawnień użytkownika za pomocą **Zasad zabezpieczeń lokalnych** systemu Windows lub konsoli **Zarządzanie zasadami grupy**:

     - Logowanie w trybie usługi
     - Logowanie w trybie wsadowym
     - Logowanie lokalne

     Konto użytkownika musi również mieć następujące role bazy danych:

     - dbcreator
     - bulkadmin
     - db_owner
6. W przypadku nowej instalacji serwera SQL Server wpisz nowe hasło i potwierdź.

Uwaga

Hasła muszą spełniać następujące wymagania minimalne dotyczące siły:

a. Minimalna długość: 8 znaków.

b. Musi zawierać przynajmniej 3 z następujących typów znaków:

- Wielkie litery: A–Z
- Małe litery: a–z
- Cyfry: 0–9
- Znaki specjalne: !@#$^*?_~-();.+: !@#$^*?_~-();.+:

7. Określ wartość **Nazwa bazy danych**OfficeScan na serwerze SQL Server.

   Podczas migrowania bazy danych CodeBase programu OfficeScan do nowej bazy danych SQL program OfficeScan automatycznie tworzy nową bazę danych o podanej nazwie.

8. Opcjonalnie wykonaj następujące czynności:

   - Kliknij przycisk **Sprawdź połączenie**, aby potwierdzić poświadczenia uwierzytelniania dla istniejącego serwera SQL Server lub bazy danych.
   - Kliknij opcję **Ostrzeżenie dotyczące niedostępnej bazy danych SQL…**, aby skonfigurować ustawienia powiadomienia bazy danych SQL.

     Szczegółowe informacje zawiera sekcja *Konfigurowanie ostrzeżenia dotyczące niedostępnej bazy danych SQL na stronie 14-53*.

9. Aby zastosować zmiany w konfiguracji, kliknij przycisk **Początek**.

Konfigurowanie ostrzeżenia dotyczące niedostępnej bazy danych SQL

Program OfficeScan automatycznie wysyła to ostrzeżenie, gdy baza danych SQL staje się niedostępna.

OSTRZEŻENIE!

W takim przypadku program OfficeScan automatycznie zatrzymuje wszystkie usługi. Program OfficeScan nie może rejestrować informacji o agentach i zdarzeniach, wykonywać aktualizacji ani konfigurować agentów, gdy baza danych jest niedostępna.

Procedura

1. Na serwerze OfficeScan przejdź do folderu <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\SQL`.
2. Kliknij dwukrotnie plik `SQLTxfr.exe`, aby uruchomić narzędzie.

   Zostanie otwarta konsola narzędzia **SQL Server Migration Tool**.
3. Kliknij opcję **Ostrzeżenie dotyczące niedostępnej bazy danych SQL…**.

   Zostanie wyświetlony ekran **Ostrzeżenie dotyczące niedostępnego serwera SQL Server**.
4. Wpisz adres e-mail odbiorców ostrzeżenia.

   Poszczególne wpisy należy oddzielać średnikami (;).
5. W razie potrzeby zmodyfikuj pola **Temat** i **Wiadomość**.

   Program OfficeScan udostępnia następujące zmienne znaczników:

   TABELA 14-20. Zmienne znaczników ostrzeżenia dotyczącego niedostępnej bazy danych SQL

ZMIENNA	OPIS
%x	Nazwa wystąpienia serwera SQL programu OfficeScan
%s	Nazwa serwera OfficeScan, którego dotyczy problem

6. Kliknij przycisk **OK**.

Ustawienia połączenia serwera Web/agenta programu OfficeScan

Podczas instalacji serwera OfficeScan program instalacyjny automatycznie konfiguruje serwer sieci Web, który umożliwia działającym w sieci komputerom łączenie się z serwerem OfficeScan. Można skonfigurować serwer Web, z którym będą się łączyć agenci punktów końcowych w sieci.

Jeżeli ustawienia serwera sieci Web są modyfikowane z zewnątrz (na przykład z konsoli zarządzania programu IIS), należy zastosować takie same zmiany w programie OfficeScan. Jeżeli na przykład numer IP serwera dla komputerów w sieci jest zmieniany ręcznie lub gdy do serwera został przypisany dynamiczny adres IP, należy ponownie skonfigurować ustawienia serwera OfficeScan.

OSTRZEŻENIE!

Zmiana ustawień połączenia może spowodować trwałą utratę połączenia między serwerem a agentami, przez co konieczne będzie ponowne zainstalowanie Agenci OfficeScan.

Konfigurowanie ustawień połączenia

Procedura

1. Przejdź do opcji **Administracja** > **Ustawienia** > **Połączenie agenta**.
2. Wpisz nazwę domeny lub adres IPv4/IPv6 i numer portu serwera sieci Web.

   Uwaga

   Port ten jest portem zaufanym, używanym przez serwer OfficeScan do komunikacji z agentami OfficeScan.

3. Kliknij przycisk **Zapisz**.

Komunikacja serwer-agent

Program OfficeScan można tak skonfigurować, aby dawał gwarancję poprawności komunikacji między serwerem i agentami. Program OfficeScan oferuje funkcje szyfrowania kluczem publicznym w celu ochrony całej komunikacji między serwerem i agentami.

Szczegółowe informacji na temat funkcji ochrony komunikacji zawierają następujące tematy:

- *Uwierzytelnianie komunikacji inicjowanej przez serwer na stronie 14-56*
- *Rozszerzone szyfrowanie komunikacji serwer-agent na stronie 14-61*

Uwierzytelnianie komunikacji inicjowanej przez serwer

Program OfficeScan używa szyfrowania klucza publicznego w celu uwierzytelniania komunikacji inicjowanej przez serwer OfficeScan na agentach. W przypadku szyfrowania kluczem publicznym serwer zachowuje klucz prywatny i instaluje klucz publiczny na wszystkich agentach. Agenci używają klucza publicznego w celu weryfikacji, czy przychodząca komunikacja została zainicjowana przez serwer i jest prawidłowa. Agenci odpowiadają w przypadku powodzenia weryfikacji.

Uwaga

Program OfficeScan nie uwierzytelnia komunikacji inicjowanej przez agentów na serwerze.

Klucze publiczny i prywatny są powiązane z certyfikatem firmy Trend Micro. Podczas instalacji serwera OfficeScan program instalacyjny zapisuje certyfikat w magazynie certyfikatów hosta. Narzędzie Menedżer certyfikatów uwierzytelniających umożliwia zarządzanie certyfikatami i kluczami firmy Trend Micro.

W chwili podejmowania decyzji o używaniu pojedynczego klucza uwierzytelniania na wszystkich serwerach OfficeScan należy pamiętać o poniższych aspektach:

- Wdrożenie pojedynczego klucza certyfikatu jest częstą praktyką w przypadku standardowego poziomu bezpieczeństwa. W takim rozwiązaniu równoważy się poziom zabezpieczeń organizacji i zmniejsza nakład pracy związany z zarządzaniem wieloma kluczami.

- Wdrożenie wielu kluczy certyfikatów na serwerach OfficeScan zapewnia maksymalny poziom bezpieczeństwa. Takie podejście powoduje zwiększenie nakładów związanych z obsługą przeterminowanych kluczy i koniecznością ich ponownej dystrybucji na serwerach.

Ważne

Przed ponownym zainstalowaniem serwera OfficeScan należ utworzyć kopię zapasową istniejącego certyfikatu. Po zakończeniu nowej instalacji należy zaimportować certyfikat z kopii zapasowej, aby uwierzytelnianie komunikacji między serwerem OfficeScan a agentami OfficeScan było kontynuowane bez zakłóceń. Jeśli w czasie instalacji serwera zostanie utworzony nowy certyfikat, Agenci OfficeScan nie będą mogli uwierzytelniać komunikacji serwera, ponieważ ciągle będą używać starego certyfikatu (który już nie istnieje).

Szczegółowe informacje dotyczące tworzenia kopii zapasowych, przywracania, eksportowania i importowania certyfikatów zawiera temat *Korzystanie z Menedżera certyfikatów uwierzytelniających serwera na stronie 14-58*.

Konfigurowanie uwierzytelniania komunikacji inicjowanej przez serwer

Procedura

1. Na serwerze OfficeScan przejdź do lokalizacji `<Folder_instalacji_serwera>\PCCSRV` i otwórz plik `ofcscan.ini` w edytorze tekstu.

2. Dodaj lub zmodyfikuj ciąg tekstowy `SGNF` w sekcji `[Global Settings]`.

   Aby włączyć uwierzytelnianie: `SGNF=1`

   Aby wyłączyć uwierzytelnianie: `SGNF=0`

Uwaga

Program OfficeScan domyślnie włącza uwierzytelnianie. Dodaj klucz `SGNF` do pliku `ofcscan.ini` tylko w przypadku, gdy chcesz wyłączyć tę funkcję.

3. W konsoli Web przejdź do pozycji **Agenci** > **Ustawienia agenta globalnego** i kliknij przycisk **Zapisz**, aby zainstalować ustawienia w agentach.

Korzystanie z Menedżera certyfikatów uwierzytelniających serwera

Serwer OfficeScan zachowuje wygasłe certyfikaty dla agentów z kluczami publicznymi, które wygasły. Dla przykładu, agenci, którzy nie łączyli się z serwerem przez dłuższy czas, mają wygasłe klucze publiczne. Po ponownym nawiązaniu połączenia agenci tworzą powiązanie wygasłego klucza publicznego z wygasłym certyfikatem, co umożliwia im rozpoznanie komunikacji inicjowanej przez serwer. Następnie serwer instaluje na agentach najnowszy klucz publiczny.

Podczas konfigurowania certyfikatów należy pamiętać o następujących kwestiach:

- W ścieżce certyfikatu akceptowane są zmapowane dyski i ścieżki UNC.
- Należy wybrać silne hasło, a następnie zapisać je do wykorzystania w przyszłości.

Ważne

Podczas używania narzędzia Menedżer certyfikatów uwierzytelniających należy pamiętać o następujących wymaganiach:

- Użytkownik musi mieć uprawnienia administratora
- Narzędzie umożliwia zarządzanie certyfikatami znajdującymi się wyłącznie na lokalnym punkcie końcowym

Procedura

1. Na serwerze OfficeScan otwórz wiersz polecenia i przejdź do katalogu <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\CertificateManager`.
2. Wykonaj jedno z poniższych poleceń:

POLECENIE	PRZYKŁAD	OPIS
CertificateManager.exe -c [hasło_do_kopii_zapasowej]	`CertificateManager.exe -c silnehasło`	Wygenerowanie nowego certyfikatu firmy Trend Micro i zastąpienie istniejącego certyfikatu Wykonaj tę czynność, jeśli istniejący certyfikat wygasł lub dostał się w ręce nieautoryzowanych osób.
CertificateManager.exe -b [Hasło] [Ścieżka certyfikatu] **Uwaga** Certyfikat ma format ZIP.	`CertificateManager.exe -b strongpassword D:\Test\TrendMicro.zip`	Umożliwia przywrócenie wszystkich certyfikatów firmy Trend Micro wystawionych przez bieżący serwer OfficeScan Wykonaj tę czynność, aby utworzyć kopię zapasową certyfikatu na serwerze OfficeScan. **Uwaga** Utworzenie kopii zapasowych certyfikatów serwera OfficeScan umożliwia ich użycie przy ponownej instalacji serwera OfficeScan.
CertificateManager.exe -r [Hasło] [Ścieżka certyfikatu] **Uwaga** Certyfikat ma format ZIP.	`CertificateManager.exe -r strongpassword D:\Test\TrendMicro.zip`	Umożliwia przywrócenie wszystkich certyfikatów firmy Trend Micro na serwerze Wykonaj tę czynność, aby przywrócić certyfikat na ponownie zainstalowanym serwerze OfficeScan.

POLECENIE	PRZYKŁAD	OPIS
CertificateManager.exe -e [Ścieżka certyfikatu]	`CertificateManager.exe -e <Folder_instalacji_agenta>\OfcNTCer.dat`	Umożliwia wyeksportowanie klucza publicznego agenta OfficeScan powiązanego z aktualnie używanym certyfikatem Wykonaj tę czynność w przypadku uszkodzenia klucza publicznego używanego przez agentów. Skopiuj plik `.dat` do folderu głównego agenta, zastępując istniejący plik. **Ważne** Ścieżka pliku certyfikatu agenta OfficeScan musi mieć następujący format: `<Folder_instalacji_agenta>\OfcNTCer.dat`
CertificateManager.exe -i [Hasło] [Ścieżka certyfikatu] **Uwaga** Domyślną nazwą certyfikatu jest: `OfcNTCer.pfx`	`CertificateManager.exe -i strongpassword D:\Test\OfcNTCer.pfx`	Importuj certyfikat firmy Trend Micro do magazynu certyfikatów

POLECENIE	PRZYKŁAD	OPIS
`CertificateManager.exe -l [ścieżka do pliku CSV]`	`CertificateManager.exe -l D:\Test\MismatchedAgentList.csv`	Umożliwia wyświetlenie listy agentów (w formacie CSV) używających aktualnie niezgodnego certyfikatu

Rozszerzone szyfrowanie komunikacji serwer-agent

Program OfficeScan oferuje rozszerzone szyfrowanie komunikacji między serwerem i agentami z użyciem standardu AES (Advanced Encryption Standard) 256 w celu dotrzymania rządowych standardów zgodności.

Ważne

Program OfficeScan obsługuje szyfrowanie AES-256 tylko na agentach z uruchomionym programem OfficeScan w wersji 11.0 SP1 lub nowszej i Plug-in Manager w wersji 2.2 lub nowszej.

OSTRZEŻENIE!

Przed włączeniem szyfrowania AES-256 należy uaktualnić wszystkich agentów OfficeScan zarządzanych przez serwer do wersji 11.0 SP1. Starsze wersje agenta OfficeScan Agent OfficeScan mogą nie być w stanie deszyfrować komunikacji zaszyfrowanej w standardzie AES-256. Włączenie szyfrowania AES-256 na starszych wersjach agenta OfficeScan może skutkować całkowitą utratą komunikacji z serwerem OfficeScan przy korzystaniu z serwera proxy.

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Kliknij kartę **Sieć**.
3. Przejdź do sekcji **Komunikacja serwer-agent**.
4. Kliknij dostępny obok polecenia **Szyfrowanie AES-256 komunikacji między serwerem OfficeScan a agentami OfficeScan** przycisk **Zmień**.

Zostanie wyświetlony komunikat.

5. Kliknij przycisk **Kontrola wersji**, aby potwierdzić zaktualizowanie wszystkich agentów do wersji OfficeScan 11.0 SP1 lub nowszej.

6. Kliknij przycisk **OK**.

Hasło konsoli Web

Ekran zarządzania hasłem dostępu do konsoli Web (lub hasłem konta główna utworzonego podczas instalacji serwera OfficeScan) jest dostępny, tylko jeśli komputer serwera nie dysponuje zasobami wymaganymi do korzystania z funkcji Role-based Administration. Ten ekran jest dostępny, jeśli na komputerze serwera jest na przykład uruchomiony system operacyjny Windows Server 2003, a usługa Menedżera autoryzacji nie jest zainstalowana. Jeśli wymagane zasoby są dostępne, ten ekran nie jest wyświetlany, a hasłem można zarządzać, modyfikując ustawienia konta głównego na ekranie **Konta użytkowników**.

Jeśli program OfficeScan nie jest zarejestrowany w programie Control Manager, instrukcje dotyczące sposobu uzyskania dostępu do konsoli Web można uzyskać, kontaktując się z dostawcą obsługi technicznej.

Ustawienia konsoli Web

Na ekranie **Ustawienia konsoli Web** można wykonać następujące czynności:

- Skonfiguruj serwer OfficeScan do okresowego odświeżania pulpitu Podsumowanie. Domyślnie serwer odświeża pulpit co 30 sekund. Można wprowadzić liczbę sekund z zakresu od 10 do 300.

- Określ ustawienia limitu czasu konsoli Web. Domyślnie użytkownik jest automatycznie wylogowywany z konsoli Web po 30 minutach bezczynności. Można wprowadzić liczbę minut z zakresu od 10 do 60.

Konfigurowanie ustawień konsoli Web

Procedura

1. Przejdź do opcji **Administracja** > **Ustawienia** > **Konsola Web**.
2. Wybierz opcję **Włącz automatyczne odświeżanie**, a następnie wskaż przedział czasu odświeżania.
3. Wybierz opcję **Włącz automatyczne wylogowywanie z konsoli Web**, a następnie wskaż limit czasu.
4. Kliknij przycisk **Zapisz**.

Menedżer kwarantanny

Jeśli Agent OfficeScan wykryje zagrożenie bezpieczeństwa i operacją skanowania jest kwarantanna, zarażony plik jest szyfrowany, a następnie umieszczany w lokalnym folderze kwarantanny znajdującym się w lokalizacji <*folder instalacji agenta*>\SUSPECT\Backup.

Po przeniesieniu pliku do lokalnego katalogu kwarantanny Agent OfficeScan wysyła go do wyznaczonego katalogu kwarantanny. Określ katalog na karcie **Agenci** > **Zarządzanie agentami** > **Ustawienia** > **Ustawienia {typ skanowania}** > **Operacja**. Pliki w wyznaczonym katalogu kwarantanny również są szyfrowane, aby zapobiec zarażeniu innych plików. Patrz *Katalog kwarantanny na stronie 7-45* Aby uzyskać więcej informacji.

Jeśli wyznaczony katalog kwarantanny znajduje się na komputerze serwera OfficeScan, ustawienia tego katalogu można modyfikować w konsoli Web. Serwer przechowuje pliki poddane kwarantannie w lokalizacji <*folder instalacji serwera*>\PCCSRV\Virus.

Uwaga

Jeżeli Agent OfficeScan nie może z jakiegoś powodu wysłać zaszyfrowanego pliku na serwer OfficeScan (np. ze względu na problem z siecią), zaszyfrowany plik pozostaje w folderze kwarantanny agenta OfficeScan. Agent OfficeScan ponowi próbę wysłania pliku po połączeniu się z serwerem OfficeScan.

Konfigurowanie ustawień katalogu kwarantanny

Procedura

1. Przejdź do opcji **Administracja** > **Ustawienia** > **Menedżer kwarantanny**.
2. Zaakceptuj lub zmień domyślną pojemność folderu kwarantanny i maksymalny rozmiar zainfekowanego pliku, który program OfficeScan może zapisać w folderze kwarantanny.

   Na ekranie wyświetlone są wartości domyślne.
3. Kliknij przycisk **Zapisz ustawienia kwarantanny**.
4. Aby usunąć wszystkie pliki z folderu kwarantanny, kliknij polecenie **Usuń wszystkie pliki poddane kwarantannie**.

Server Tuner

Narzędzie Server Tuner służy do optymalizacji wydajności serwera OfficeScan z wykorzystaniem parametrów następujących elementów wydajności serwera:

- **Pobieranie**

  Jeżeli liczba agentów OfficeScan (w tym agentów aktualizacji) żądających aktualizacji z serwera OfficeScan przekroczy dostępne zasoby, serwer przenosi żądanie aktualizacji agenta do kolejki i przetwarza je po zwolnieniu zasobów. Kiedy pobranie przez agenta składników aktualizacji z serwera OfficeScan powiedzie się, do serwera jest wysyłane powiadomienie o zakończeniu aktualizacji. Należy ustawić maksymalną liczbę minut oczekiwania serwera OfficeScan na otrzymanie od agenta

powiadomienia o aktualizacji. Należy też ustawić maksymalną liczbę prób wysyłania przez serwer do agenta powiadomienia o konieczności przeprowadzenia aktualizacji i zastosowania nowych ustawień konfiguracji. Serwer kontynuuje próby tylko wówczas, gdy nie otrzyma powiadomienia od agenta.

- **Buffer**

  Gdy serwer OfficeScan otrzymuje od agentów OfficeScan wiele żądań, na przykład wykonania aktualizacji, obsługuje maksymalną możliwą liczbę żądań, a pozostałe umieszcza w buforze. Zachowane w buforze żądania są obsługiwane po zwolnieniu zasobów serwera. Należy określić rozmiar bufora dla zdarzeń takich jak żądania aktualizacji ze strony agenta i raportowanie dziennika agenta.

- **Ruch sieciowy**

  Wielkość ruchu sieciowego zmienia się w ciągu dnia. Przepływ ruchu sieciowego do serwera OfficeScan i innych źródeł aktualizacji można kontrolować, określając liczbę agentów OfficeScan, którzy mogą jednocześnie o wybranej porze dnia aktualizować składniki.

Narzędzie Server Tuner wymaga następującego pliku: `SvrTune.exe`

Uruchamianie narzędzia Server Tuner

Procedura

1. Na komputerze serwera OfficeScan przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\SvrTune`.
2. Dwukrotnie kliknij plik `SvrTune.exe`, aby uruchomić narzędzie Server Tuner.

   Zostanie otwarta konsola narzędzia Server Tuner.
3. W **Download**, zmodyfikuj następujące ustawienia:

   - **Limit czasu klienta**: wpisz liczbę minut, jaką serwer OfficeScan ma czekać na odpowiedź agenta dotyczącą aktualizacji. Jeżeli agent nie odpowie w tym czasie, na serwerze OfficeScan przyjmowane jest założenie, że agent nie ma bieżących składników. Kiedy upływa limit czasu powiadomionego agent, serwer przechodzi do przetwarzania danych kolejnego oczekującego na powiadomienie agenta.

- **Limit czasu agenta aktualizacji**: wpisz liczbę minut, jaką serwer OfficeScan ma czekać na odpowiedź agenta aktualizacji dotyczącą aktualizacji. Kiedy upływa limit czasu powiadomionego agent, serwer przechodzi do przetwarzania danych kolejnego oczekującego na powiadomienie agenta.
- **Liczba prób**: wpisz maksymalną liczbę prób powiadamiania agenta przez serwer OfficeScan o konieczności przeprowadzenia aktualizacji lub zastosowania nowych ustawień konfiguracji.
- **Interwał ponownych prób**: w tym polu należy wpisać, ile minut serwer OfficeScan powinien odczekać przed kolejną próbą powiadomienia.

4. W obszarze **Network Traffic** zmień następujące ustawienia:
   - **Godziny normalne**: kliknij przyciski opcji odpowiadających godzinom, w których ruch sieciowy jest normalny.
   - **Godziny poza szczytem**: kliknij przyciski opcji odpowiadających godzinom, w których ruch sieciowy jest najmniejszy.
   - **Godziny szczytu**: kliknij przyciski opcji odpowiadających godzinom, w których ruch sieciowy jest największy.
   - **Maksymalna liczba połączeń klientów**: wpisz maksymalną ilość klientów, którzy mogą równocześnie aktualizować składniki zarówno z „innych źródeł aktualizacji", jak i z serwera OfficeScan. Wpisz maksymalną liczbę klientów dla każdego z powyższych przedziałów czasu. Jeżeli została osiągnięta maksymalna liczba połączeń, Agenci OfficeScan mogą aktualizować składniki dopiero po zamknięciu bieżącego połączenia agenta (zarówno jeżeli aktualizacja została zakończona, jak i gdy odpowiedź agenta przekroczyła limit czasu określony w polu **Limit czasu klienta** lub **Limit czasu agenta aktualizacji**.
5. Kliknij przycisk **OK**. Zostanie wyświetlony monit o ponowne uruchomienie OfficeScan Master Service.

Uwaga

Ponowne uruchomienie dotyczy tylko usługi, a nie komputera.

6. Wybierz odpowiednie opcje ponownego uruchamiania:

- Kliknij opcję **Tak**, aby zapisać ustawienia narzędzia Server Tuner i ponownie uruchomić usługę. Ustawienia zostaną uwzględnione natychmiast po ponownym uruchomieniu usługi.
- Kliknij opcję **Nie**, aby zapisać ustawienia narzędzia Server Tuner bez ponownego uruchamiania usługi. Uruchom ponownie OfficeScan Master Service lub serwer OfficeScan, aby zastosować ustawienia.

Smart Feedback

Funkcja Trend Micro Smart Feedback udostępnia sieci Smart Protection Network anonimowe dane o zagrożeniach, umożliwiając firmie Trend Micro natychmiastowe identyfikowanie i eliminowanie nowych zagrożeń. Funkcję Smart Feedback można wyłączyć w dowolnej chwili, korzystając z tej konsoli.

Uczestnictwo w programie Smart Feedback

Procedura

1. Przejdź do opcji **Administracja** > **Smart Protection** > **Smart Feedback**.
2. Kliknij polecenie **Włącz funkcję Trend Micro Smart Feedback**.
3. Aby poinformować firmę Trend Micro o charakterze prowadzonej działalności, wybierz wartość opcji **Branża**.
4. Aby wysyłać informacje o potencjalnych zagrożeniach bezpieczeństwa występujących w plikach na agentach OfficeScan, zaznacz pole wyboru **Włącz informowanie o podejrzanych plikach programów**.

   Uwaga

   Pliki przesyłane za pomocą funkcji Smart Feedback nie zawierają danych użytkownika i są wysyłane wyłącznie na potrzeby analizy zagrożeń.

5. Aby skonfigurować kryteria dotyczące wysyłania danych, ustal, jaka liczba wykryć określonego zagrożenia w wybranej jednostce czasu ma aktywować zgłoszenie.

6. W celu zminimalizowania zakłóceń ruchu sieciowego określ maksymalną przepustowość, jaką program OfficeScan może wykorzystywać podczas wysyłania zgłoszeń.

7. Kliknij przycisk **Zapisz**.

Rozdział 15

Zarządzanie agentem OfficeScan

W tym rozdziale przedstawiono zarządzanie agentami OfficeScan i konfiguracje.

Rozdział składa się z następujących tematów:

Lokalizacja punktu końcowego

Program OfficeScan zawiera funkcję rozpoznawania lokalizacji, która określa, czy Agent OfficeScan ma lokalizację wewnętrzną, czy zewnętrzną. Rozpoznawanie lokalizacji jest wykorzystywane przez następujące funkcje i usługi programu OfficeScan:

TABELA 15-1. Funkcje i usługi wykorzystujące rozpoznawanie lokalizacji

FUNKCJA/ USŁUGA	OPIS
Usługi Web Reputation Services	Lokalizacja agenta OfficeScan decyduje o regułach Web Reputation, które będą stosowane przez agenta OfficeScan. Administratorzy z reguły stosują ściślejsze reguły dla agentów zewnętrznych. Szczegółowe informacje o regułach usługi Web Reputation zawiera temat *Reguły Web Reputation na stronie 12-5*.
Usługi File Reputation Services	W przypadku agentów używających usługi Smart Scan lokalizacja agenta OfficeScan decyduje o źródle programu Smart Protection, do którego agenci wysyłają żądania skanowania. Agenci zewnętrzni OfficeScan wysyłają żądania skanowania do sieci Smart Protection Network, podczas gdy agenci wewnętrzni wysyłają żądania do źródeł zdefiniowanych na liście źródeł programu Smart Protection. Szczegółowe informacje o źródłach Smart Protection zawiera temat *Źródła Smart Protection na stronie 4-6*.
Zapobieganie utracie danych	Lokalizacja agenta OfficeScan decyduje o regułach Zapobieganie utracie danych, które będą stosowane przez agenta. Administratorzy z reguły stosują ściślejsze reguły dla agentów zewnętrznych. Szczegółowe informacje o regułach Zapobieganie utracie danych zawiera temat *Reguły Zapobieganie utracie danych na stronie 11-3*.
Kontrola urządzeń	Lokalizacja agenta OfficeScan decyduje o regułach kontroli urządzeń, które będą stosowane przez agenta. Administratorzy z reguły stosują ściślejsze reguły dla agentów zewnętrznych. Szczegółowe informacje o regułach kontroli urządzeń zawiera temat *Kontrola urządzeń na stronie 10-2*.

Kryteria lokalizacji

Należy ustalić, czy lokalizacja jest określana na podstawie adresu IP bramy punktu końcowego agenta OfficeScan czy stanu połączenia agenta OfficeScan z serwerem OfficeScan lub dowolnym serwerem odniesienia.

- **Stan połączenia agenta**: Jeśli agent OfficeScan może się połączyć z serwerem OfficeScan lub dowolnym przypisanym serwerem odniesienia w sieci intranet, lokalizacja punktu końcowego ma charakter wewnętrzny. Dodatkowo, jeśli punkt końcowy spoza sieci korporacyjnej może nawiązać połączenie z serwerem OfficeScan lub serwerem odniesienia, jego lokalizacja również ma charakter wewnętrzny. Jeśli żaden z tych warunków nie ma zastosowania, to lokalizacja punktu końcowego na charakter zewnętrzny.
- **Adres IP i adres MAC bramy**: Jeśli adres IP bramy punktu końcowego agenta OfficeScan odpowiada dowolnemu adresowi IP bramy wprowadzonemu na ekranie **Lokalizacja punktu końcowego**, lokalizacja punktu końcowego ma charakter wewnętrzny. W przeciwnym razie punkt końcowy jest traktowany jako zewnętrzny.

Konfiguracja ustawień lokalizacji

Procedura

1. Przejdź do opcji **Agenci** > **Lokalizacja punktu końcowego**.
2. Wybierz, czy lokalizacja jest określana na podstawie **stanu połączenia agenta** lub **adresów MAC i IP bramy**.
3. W przypadku wybrania opcji **Stan połączenia agenta** ustal, czy chcesz korzystać z serwera odniesienia.

   Szczegółowe informacje można znaleźć w części *Serwery odniesienia na stronie 14-35*.

   a. W przypadku wystąpienia poniższych zdarzeń, jeśli nie został określony serwer odniesienia, Agent OfficeScan sprawdza stan połączenia względem serwera OfficeScan:

      - Agent OfficeScan przechodzi z trybu niezależnego do zwykłego (online/offline).

- Agent OfficeScan przechodzi z jednej metody skanowania na inną.

  Szczegółowe informacje można znaleźć w części *Typy metod skanowania na stronie 7-9*.

- Agent OfficeScan wykrywa zmianę adresu IP punktu końcowego.
- Agent OfficeScan uruchamia się ponownie.
- Klient inicjuje weryfikację połączenia.

  Szczegółowe informacje można znaleźć w części *Ikony agenta OfficeScan na stronie 15-27*.

- Kryteria lokalizacji usługi Web Reputation ulegają zmianie podczas stosowania ustawień globalnych.
- Reguła ochrony przed epidemią nie jest wymuszana i zostają przywrócone ustawienia sprzed epidemii.

b. Jeśli został określony serwer odniesienia, a połączenie z serwerem OfficeScan zakończyło się niepowodzeniem, Agent OfficeScan najpierw sprawdza stan połączenia względem serwera OfficeScan, a następnie względem serwera odniesienia. Agent OfficeScan sprawdza stan połączenia co godzinę oraz gdy wystąpi dowolne powyższe zdarzenie.

4. W przypadku wybrania opcji **Adres IP i MAC bramy**:

   a. Wpisz adres IPv4/IPv6 bramy w wyświetlonym polu tekstowym.

   b. Wpisz adres MAC.

   c. Kliknij przycisk **Dodaj**.

      Jeśli adres MAC nie zostanie wpisany, program OfficeScan włączy wszystkie adresy MAC należące do podanego adresu IP.

   d. Powtórz kroki od a do c, aż zostaną dodane wszystkie adresy IP bram.

   e. Aby zaimportować listę ustawień bramy, należy skorzystać z narzędzia do importowania ustawień bramy.

      Szczegółowe informacje można znaleźć w części *Narzędzie do importowania ustawień bramy na stronie 15-5*.

5. Kliknij przycisk **Zapisz**.

Narzędzie do importowania ustawień bramy

Program OfficeScan sprawdza lokalizację punktu końcowego, aby ustalić, z jakiej reguły Web Reputation należy korzystać, oraz z którym źródłem programu Smart Protection należy się łączyć. Jednym ze sposobów określenia przez program OfficeScan lokalizacji punktu końcowego jest sprawdzenie adresu IP bramy i adresu MAC punktu końcowego.

Ustawienia bramy można skonfigurować na ekranie **Lokalizacja punktu końcowego** lub za pomocą narzędzia do importowania ustawień bramy zaimportować listę ustawień bramy do ekranu **Lokalizacja punktu końcowego**.

Używanie narzędzia do importowania ustawień bramy

Procedura

1. Przygotuj plik tekstowy (`.txt`) zawierający listę ustawień bramy. W każdym wierszu wprowadź adres IPv4 lub IPv6 oraz opcjonalnie adres MAC.

   Oddziel adresy IP i adresy MAC przecinkami. Maksymalna liczba wpisów wynosi 4096.

   Na przykład:

   ```
   10.1.111.222,00:17:31:06:e6:e7

   2001:0db7:85a3:0000:0000:8a2e:0370:7334

   10.1.111.224,00:17:31:06:e6:e7
   ```

2. Na komputerze serwera przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\GatewaySettingsImporter`.

3. Prawym przyciskiem myszy kliknij plik `GSImporter.exe` i wybierz opcję **Uruchom jako administrator**.

Uwaga

Narzędzia do importowania ustawień bramy nie można uruchamiać z poziomu usług terminalowych.

4. Na ekranie **Narzędzie do importowania ustawień bramy** przejdź do pliku utworzonego w punkcie 1 i kliknij polecenie **Importuj**.

5. Kliknij przycisk **OK**.

   Ustawienia bramy wyświetlają się na ekranie **Lokalizacja punktu końcowego**, a serwer OfficeScan wdraża je na agentach Agenci OfficeScan.

6. Aby usunąć wszystkie wpisy, kliknij przycisk **Wyczyść wszystkie**.

   Jeśli zamierzasz usunąć konkretny wpis, usuń go na ekranie **Lokalizacja punktu końcowego**.

7. Aby wyeksportować ustawienia do pliku, kliknij przycisk **Eksportuj wszystkie**, a następnie określ nazwę i typ pliku.

Zarządzanie programem agenta OfficeScan

Następujące tematy przedstawiają sposoby zarządzania programem agenta OfficeScan i jego ochrony:

Usługi agenta OfficeScan

Agent OfficeScan uruchamia usługi wymienione w tabeli. Stan tych usług można przeglądać za pośrednictwem konsoli Microsoft Management Console.

TABELA 15-2. Usługi agenta OfficeScan

USŁUGA	KONTROLOWANE FUNKCJE
Usługa zapobiegania nieautoryzowanym zmianom firmy Trend Micro (`TMBMSRV.exe`)	• Monitorowanie zachowań • Kontrola urządzeń • Usługa Certified Safe Software Service
Zapora OfficeScan NT (`TmPfw.exe`)	Zapora programu OfficeScan
Usługa Ochrona danych OfficeScan (`dsagent.exe`)	• Zapobieganie utracie danych • Kontrola urządzeń
OfficeScan NT Listener (`TmListen.exe`)	Komunikacja między agentem OfficeScan a serwerem OfficeScan
Usługa proxy OfficeScan NT (`TmProxy.exe`)	• Usługa Web Reputation • Skanowanie poczty POP3
OfficeScan NT RealTime Scan (`NTRtScan.exe`)	• Skanowanie w czasie rzeczywistym • Skanowanie zaplanowane • Skanowanie ręczne/Skanuj teraz
OfficeScan Common Client Solution Framework (`TmCCSF.exe`)	Usługa zaawansowanej ochrony • Zapobieganie wykorzystaniu luki w zabezpieczeniach przeglądarki • Skanowanie pamięci

Następujące usługi zapewniają zaawansowaną ochronę, ale ich mechanizmy monitorowania mogą obciążać zasoby systemowe, szczególnie w przypadku serwerów, na których działają aplikacje obciążające system:

- Usługa zapobiegania nieautoryzowanym zmianom firmy Trend Micro (`TMBMSRV.exe`)

- Zapora OfficeScan NT (`TmPfw.exe`)
- Usługa Ochrona danych OfficeScan (`dsagent.exe`)

Z tego powodu usługi te są domyślnie wyłączone na platformach serwerowych (Windows Server 2003, Windows Server 2008 i Windows Server 2012). Jeśli te usługi mają zostać włączone:

- Należy stale monitorować wydajność systemu i podjąć odpowiednie działanie w przypadku spadku wydajności.
- Usługę `TMBMSRV.exe` można włączyć, jeśli z reguł monitorowania zachowań zostaną wykluczone aplikacje obciążające system. W celu zidentyfikowania takich aplikacji można użyć narzędzia do optymalizacji wydajności. Szczegółowe informacje zawiera sekcja *Używanie narzędzia optymalizacji wydajności firmy Trend Micro na stronie 15-10*.

W przypadku platform komputerów stacjonarnych należy wyłączyć te usługi tylko w przypadku zaobserwowania poważnego spadku wydajności.

Włączanie lub wyłączanie usług agenta za pośrednictwem konsoli Web

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. Agenci OfficeScan działający w systemie Windows XP, Vista, 7, 8, 8.1 lub 10:
   a. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.

> **Uwaga**
>
> W przypadku wybrania domeny głównej lub konkretnych domen ustawienie zostanie zastosowane tylko do agentów działających w systemie Windows. Ustawienie nie zostanie zastosowane do agentów działających na dowolnej platformie Windows Server, nawet jeśli stanowią część domeny.

b. Kliknij polecenie **Ustawienia** > **Dodatkowe ustawienia usługi**.

c. Zaznacz lub usuń zaznaczenie pól wyboru w następujących sekcjach:

- **Usługa zapobiegania nieautoryzowanym zmianom**
- **Usługa zapory**
- **Usługa podejrzanego połączenia**
- **Usługa Ochrona danych**
- **Usługa zaawansowanej ochrony**

d. Kliknij przycisk **Zapisz**, aby zastosować ustawienia do domen(y). Jeśli wybrano ikonę domeny głównej, należy wybrać spośród następujących opcji:

- **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów w systemie Windows oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów w systemie Windows dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

3. W przypadku Agenci OfficeScan z systemem Windows Server:

a. Wybierz jednego agenta w drzewie agentów.

b. Kliknij polecenie **Ustawienia** > **Dodatkowe ustawienia usługi**.

c. Zaznacz lub usuń zaznaczenie pól wyboru w następujących sekcjach:

- **Usługa zapobiegania nieautoryzowanym zmianom**
- **Usługa zapory**
- **Usługa podejrzanego połączenia**
- **Usługa Ochrona danych**

- **Usługa zaawansowanej ochrony**

d. Kliknij przycisk **Zapisz**.

Używanie narzędzia optymalizacji wydajności firmy Trend Micro

Procedura

1. Pobierz Narzędzie optymalizacji wydajności firmy Trend Micro spod następującego adresu:

   http://esupport.trendmicro.com/solution/en-us/1056425.aspx

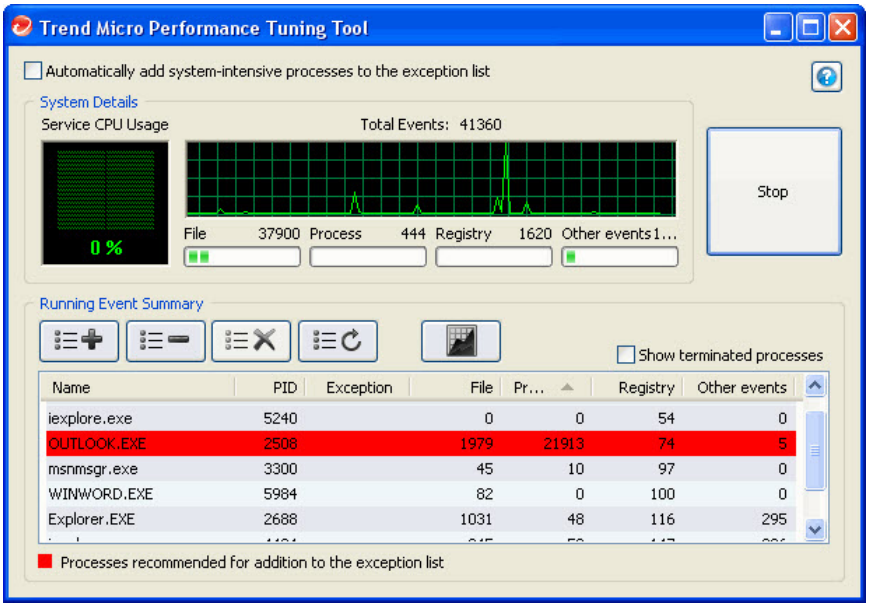
2. Rozpakuj plik `TMPerfTool.zip`, aby wyodrębnić plik `TMPerfTool.exe`.

3. Umieść plik `TMPerfTool.exe` w <*folderze instalacyjnym agenta*> lub w tym samym folderze co plik `TMBMCLI.dll`.

4. Kliknij prawym przyciskiem myszy plik `TMPerfTool.exe` i wybierz polecenie **Uruchom jako administrator**.

5. Przeczytaj i zaakceptuj umowę użytkownika, a następnie kliknij przycisk **OK**.

6. Kliknij **Analizuj**.



ILUSTRACJA 15-1. Wyróżniony proces obciążający system

Narzędzie rozpocznie analizowanie wykorzystania procesora i ładowania zdarzeń. Proces obciążający system zostanie wyróżniony kolorem czerwonym.

7. Wybierz proces obciążający system i kliknij przycisk **Dodaj do listy wyjątków (zezwól)** ( ).

8. Sprawdź, czy podniesie się wydajność systemu lub aplikacji.

9. Jeśli wydajność podniesie się, wybierz ponownie proces i kliknij przycisk **Usuń z listy wyjątków** ( ).

10. Jeśli wydajność ponownie spadnie, wykonaj następujące czynności:

    a. Zapisz nazwę aplikacji.

    b. Kliknij **Stop**.

    c. Kliknij przycisk **Wygeneruj raport** ( ) i zapisz plik `.xml`.

d. Przejrzyj aplikacje, które zostały zidentyfikowane jako powodujące konflikty, a następnie dodaj je do listy wyjątków monitorowania zachowań.

Szczegółowe informacje zawiera sekcja *Lista wyjątków monitorowania zachowań na stronie 9-10*.

Ponowne uruchomienie usługi Agent OfficeScan Service

Program OfficeScan ponownie uruchamia usługi agenta OfficeScan, które nieoczekiwanie przestały odpowiadać i nie zostały zatrzymane przez zwykły proces systemowy. Szczegółowe informacje na temat usług agenta zawiera sekcja *Usługi agenta OfficeScan na stronie 15-7*.

Aby umożliwić ponowne uruchamianie usług agenta OfficeScan, należy skonfigurować wymagane ustawienia.

Konfiguracja ponownego uruchamiania usługi

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Kliknij kartę **System**.
3. Przejdź do sekcji **Ponowne uruchamianie usług**.
4. Wybierz opcję **Automatycznie ponownie uruchamiaj usługę agenta OfficeScan, jeśli nastąpi niespodziewane przerwanie jej działania**.
5. Skonfiguruj następujące elementy:
   - **Ponownie uruchom usługę po __ min**. Określ czas (w minutach), jaki musi upłynąć, zanim program OfficeScan ponownie uruchomi usługę.
   - **Jeśli pierwsza próba ponownego uruchomienia usługi nie powiedzie się, spróbuj ponownie __ razy**: Należy określić maksymalną liczbę prób ponownego uruchomienia usługi. Jeśli po przeprowadzeniu maksymalnej liczby prób usługa nadal nie jest uruchomiona, należy ją uruchomić ręcznie.

- **Zresetuj licznik nieudanych prób ponownego uruchomienia po _ godz.**: Jeśli usługa jest nadal zatrzymana po wykonaniu maksymalnej liczby prób, przed zresetowaniem licznika nieudanych prób program OfficeScan czeka ustaloną liczbę godzin. Jeśli usługa jest nadal zatrzymana po upływie ustalonej liczby godzin, program OfficeScan ponownie ją uruchamia.

Własna ochrona agenta OfficeScan

Własna ochrona agenta OfficeScan to funkcja agenta OfficeScan, która zapewnia możliwość ochrony procesów i innych zasobów, względem których jest wymagane prawidłowe działanie. Własna ochrona agenta OfficeScan ułatwia zapobieganie próbom wyłączania funkcji ochrony przed złośliwym oprogramowaniem, które są podejmowane przez programy lub osoby.

Własna ochrona agenta OfficeScan oferuje następujące opcje:

- *Ochrona usług agenta OfficeScan na stronie 15-14*
- *Ochrona plików w folderze instalacyjnym agenta OfficeScan na stronie 15-15*
- *Ochrona kluczy rejestru agenta OfficeScan na stronie 15-16*
- *Ochrona procesów agenta OfficeScan na stronie 15-16*

Konfigurowanie ustawień własnej ochrony agenta OfficeScan

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Kliknij kartę **Inne ustawienia** i przejdź do sekcji **Własna ochrona agenta OfficeScan**.

5. Włącz następujące opcje:

   - *Ochrona usług agenta OfficeScan na stronie 15-14*
   - *Ochrona plików w folderze instalacyjnym agenta OfficeScan na stronie 15-15*
   - *Ochrona kluczy rejestru agenta OfficeScan na stronie 15-16*
   - *Ochrona procesów agenta OfficeScan na stronie 15-16*

6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Ochrona usług agenta OfficeScan

Program OfficeScan blokuje wszystkie próby przerwania działania następujących usług agenta OfficeScan:

- OfficeScan NT Listener (`TmListen.exe`)
- OfficeScan NT RealTime Scan (`NTRtScan.exe`)
- OfficeScan NT Proxy Service (`TmProxy.exe`)
- OfficeScan NT Firewall (`TmPfw.exe`)
- Ochrona danych OfficeScan Service (`dsagent.exe`)
- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)

Uwaga

Jeśli ta opcja jest włączona, program OfficeScan może uniemożliwić instalację produktów innych firm na punktach końcowych. W przypadku wystąpienia tego problemu można tymczasowo wyłączyć tę opcję i włączyć ją ponownie po zainstalowaniu produktu innej firmy.

- Ogólne środowisko rozwiązania klienta Trend Micro (`TmCCSF.exe`)

Ochrona plików w folderze instalacyjnym agenta OfficeScan

Aby zapobiegać modyfikowaniu lub usuwaniu plików agenta OfficeScan przez inne programy lub osoby, program OfficeScan oferuje kilka rozszerzonych funkcji ochrony.

Po włączeniu opcji **Chroń pliki w folderze instalacji agenta OfficeScan** program OfficeScan blokuje następujące pliki w głównym folderze <*Folder instalacji agenta*>:

- Wszystkie podpisane cyfrowo pliki z rozszerzeniami `.exe`, `.dll`, oraz `.sys`
- niektóre pliki bez cyfrowych podpisów, w tym:
  - `bspatch.exe`
  - `bzip2.exe`
  - `INETWH32.dll`
  - `libcurl.dll`
  - `libeay32.dll`
  - `libMsgUtilExt.mt.dll`
  - `msvcm80.dll`
  - `MSVCP60.DLL`
  - `msvcp80.dll`
  - `msvcr80.dll`
  - `OfceSCV.dll`
  - `OFCESCVPack.exe`
  - `patchbld.dll`
  - `patchw32.dll`
  - `patchw64.dll`
  - `PiReg.exe`
  - `ssleay32.dll`
  - `Tmeng.dll`
  - `TMNotify.dll`
  - `zlibwapi.dll`

Po włączeniu opcji **Chroń pliki w folderze instalacji agenta OfficeScan** i skanowania w czasie rzeczywistym pod kątem wirusów/złośliwego oprogramowania program OfficeScan wykonuje następujące operacje:

- Sprawdzanie integralności plików przed uruchomieniem plików `.exe` w folderze instalacyjnym

  W trakcie aktualizacji ActiveUpdate program OfficeScan sprawdza, czy wydawcą pliku wyzwalającego aktualizację jest firma Trend Micro. Jeśli wydawca nie zostanie rozpoznany jako Trend Micro i funkcja ActiveUpdate nie może zastąpić nieprawidłowego pliku, program OfficeScan rejestruje taki przypadek w dzienniku zdarzeń systemu Windows oraz blokuje aktualizację.

- Zapobieganie przejęciu kontroli nad plikami DLL

  Niektórzy twórcy złośliwego oprogramowania kopiują pliki bibliotek dołączanych dynamicznie do folderu instalacji agenta OfficeScan lub folderu funkcji Monitorowanie zachowań w celu wczytania tych plików przed wczytaniem agenta. Pliki takie usiłują zakłócić ochronę zapewnianą przez program OfficeScan. Aby zapobiec kopiowaniu plików, nad którymi przejęto kontrolę, do folderów agenta OfficeScan, program OfficeScan uniemożliwia kopiowanie plików do folderu instalacji lub folderu funkcji Monitorowanie zachowań.

- Zapobieganie blokowaniu plików za pomocą ustawienia "SHARE:NONE" w systemie Windows

Ochrona kluczy rejestru agenta OfficeScan

Program OfficeScan blokuje wszystkie próby modyfikacji, usuwania i dodawania nowych wpisów do następujących kluczy i podkluczy rejestru:

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP`

Ochrona procesów agenta OfficeScan

Program OfficeScan blokuje wszystkie próby przerwania działania procesów wskazanych w poniższej tabeli.

Proces	Opis
TmListen.exe	Odbiera polecenia i powiadomienia z serwera OfficeScan i zapewnia komunikację agenta OfficeScan z serwerem
NTRtScan.exe	Przeprowadza na agentach OfficeScan skanowanie w czasie rzeczywistym, zaplanowane i ręczne
TmProxy.exe	skanuje ruch w sieci przed przesłaniem go do aplikacji docelowej
TmPfw.exe	udostępnia zaporę na poziomie pakietów, skanowanie wirusów sieciowych i możliwości wykrywania ingerencji
TMBMSRV.exe	kontroluje dostęp do zewnętrznych urządzeń pamięci masowej i zapobiega wprowadzaniu nieautoryzowanych zmian do kluczy rejestrów i procesów
DSAgent.exe	monitoruje transmisję ważnych danych i kontroluje dostęp do urządzeń
PccNTMon.exe	Ten proces jest odpowiedzialny za uruchamianie konsoli agenta OfficeScan
TmCCSF.exe	wykonuje funkcję zapobiegania wykorzystaniu luki w zabezpieczeniach przeglądarki i skanowanie pamięci

Program OfficeScan może także chronić przed dodawaniem procesów do listy zasad ograniczeń oprogramowania (SRP) firmy Microsoft. Zasady ograniczeń oprogramowania uniemożliwiają uruchamianie wskazanych na liście aplikacji na punkcie końcowym. Aby zapobiegać dodawaniu procesów programu OfficeScan do listy zasad ograniczeń oprogramowania:

1. Włącz opcję **Chroń procesy agenta OfficeScan**.
2. Włącz opcję **Usługa zapobiegania nieautoryzowanym zmianom**.

   Szczegółowe informacje zawiera sekcja *Włączanie lub wyłączanie usług agenta za pośrednictwem konsoli Web na stronie 15-8*.

Ograniczenie dostępu do konsoli agenta OfficeScan

To ustawienie powoduje wyłączenie dostępu do konsoli agenta OfficeScan z paska zadań i z menu Start systemu Windows. Jedynym sposobem uzyskania dostępu do

konsoli agenta OfficeScan jest dwukrotne kliknięcie pliku `PccNTMon.exe` w lokalizacji <*Folder instalacji agenta*>. Aby zastosować to ustawienie, po jego skonfigurowaniu należy ponownie załadować agenta OfficeScan.

To ustawienie nie powoduje wyłączenia agenta OfficeScan. Agent OfficeScan pracuje w tle i zapewnia ciągłą ochronę przed zagrożeniami bezpieczeństwa.

Ograniczanie dostępu do konsoli agenta OfficeScan

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Kliknij kartę **Inne ustawienia** i przejdź do sekcji **Ograniczenia dostępu do agenta OfficeScan**.
5. Wybierz opcję **Nie zezwalaj użytkownikom na dostęp do konsoli agenta OfficeScan z paska zadań lub z menu Start systemu Windows**.
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Zamykanie i odblokowywanie agenta OfficeScan

Uprawnienie do zamykania i odblokowywania agenta OfficeScan zapewnia użytkownikom możliwość tymczasowego zatrzymania pracy agenta OfficeScan lub

uzyskania dostępu do zaawansowanych funkcji konsoli Web przy użyciu hasła lub bez użycia hasła.

Przyznawanie uprawnienia do zamykania i odblokowywania agenta

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Na karcie **Uprawnienia** przejdź do sekcji **Zamknij i odblokuj**.
5. Aby umożliwić zamknięcie agenta OfficeScan bez podawania hasła, wybierz opcję **Nie wymaga hasła**.
   - Jeśli hasło jest wymagane, wybierz opcję **Wymagaj hasła**, wpisz hasło, a następnie potwierdź je.
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Uprawnienie trybu niezależnego Agent OfficeScan

Określonym użytkownikom można przyznać uprawnienie trybu niezależnego Agent OfficeScan, jeśli zdarzenia agent-serwer zakłócają zadania użytkownika. Na przykład

użytkownik, który często prowadzi prezentacje, może włączyć tryb niezależny przed rozpoczęciem prezentacji, aby uniemożliwić serwerowi OfficeScan instalowanie ustawień Agent OfficeScan i uruchamianie skanowania na Agent OfficeScan.

Kiedy Agenci OfficeScan są w trybie niezależnym:

- Agenci OfficeScan nie wysyłają dzienników do serwera OfficeScan, nawet jeśli istnieje działające połączenie między serwerem a agentami.
- Serwer OfficeScan nie inicjuje zadań i instalowania ustawień na agentach Agent OfficeScan, nawet jeśli istnieje działające połączenie między serwerem a agentami.
- Agenci OfficeScan aktualizują składniki, jeśli mogą nawiązać połączenie z dowolnym źródłem aktualizacji. Źródła obejmują serwer OfficeScan, agenty aktualizacji oraz niestandardowe źródło aktualizacji.

  Następujące zdarzenia uruchamiają aktualizację na agentach w trybie niezależnym:

  - Użytkownik wykonuje aktualizację ręczną.
  - Uruchomiona zostaje automatyczna aktualizacja agenta. Można wyłączyć automatyczną aktualizację agenta na agentach w trybie niezależnym.

    Szczegółowe informacje zawiera sekcja *Wyłączanie automatycznej aktualizacji agenta na agentach w trybie niezależnym na stronie 15-21*.
  - Uruchomiona zostaje aktualizacja zaplanowana. Tylko agenci z wymaganymi uprawnieniami mogą wykonywać aktualizacje zaplanowane. Uprawnienie to można odwołać w dowolnym momencie.

    Szczegółowe informacje zawiera sekcja *Odwołanie uprawnienia do zaplanowanej aktualizacji na agentach w trybie niezależnym na stronie 15-22*.

Przyznawanie Agent uprawnienia trybu niezależnego

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.

3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Na karcie **Uprawnienia** przejdź do sekcji **Tryb niezależny**.
5. Wybierz opcję **Włącz tryb niezależny**.
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Wyłączanie automatycznej aktualizacji agenta na agentach w trybie niezależnym

Procedura

1. Przejdź do opcji **Aktualizacje** > **Agenci** > **Aktualizacja automatyczna**.
2. Przejdź do sekcji **Aktualizacja wywołana zdarzeniem**.
3. Wyłącz opcję **Uwzględnij agentów w trybie niezależnym i offline**.

> **Uwaga**
>
> Opcja ta zostaje automatycznie wyłączona, jeśli wyłączono opcję **Rozpocznij natychmiastową aktualizację składnika na agentach po jego pobraniu przez serwer OfficeScan**.

Odwołanie uprawnienia do zaplanowanej aktualizacji na agentach w trybie niezależnym

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej () albo wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Na karcie **Uprawnienia** przejdź do sekcji **Aktualizacje składników**.
5. Usuń zaznaczenie opcji **Włącz/wyłącz aktualizacje w oparciu o harmonogram**.
6. Kliknij przycisk **Zapisz**.

Konfiguracja języka agenta OfficeScan

Wszystkich agentów OfficeScan można skonfigurować do wyświetlania z użyciem ustawień języka serwera OfficeScan lub lokalnie zalogowanego użytkownika. Po zainstalowaniu lub uaktualnieniu programu agenta OfficeScan agent stosuje ustawienia języka skonfigurowane na ekranie **Ustawienia globalne**.

Domyślnie, jeśli Agent OfficeScan nie obsługuje ustawień języka zalogowanego użytkownika, przyjmowane są ustawienia języka serwera OfficeScan, a następnie języka angielskiego.

Konfigurowanie ustawień języka agenta OfficeScan

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Kliknij kartę **Kontrola agentów**.

3. Przejdź do sekcji **Konfiguracja języka agenta**.

4. Określ, w jaki sposób Agent OfficeScan stosuje ustawienia języka:

   - **Lokalne ustawienia języka w punkcie końcowym**: Agent OfficeScan wyświetla treści z użyciem ustawień języka zalogowanego użytkownika.

     Uwaga

     Jeśli Agent OfficeScan nie obsługuje ustawień języka zalogowanego użytkownika, agent stosuje język serwera OfficeScan. Jeśli punkt końcowy nie obsługuje języka serwera OfficeScan, wyświetla treści w języku angielskim.

   - **Język serwera OfficeScan**: Agent OfficeScan wyświetla treści w języku serwera OfficeScan.

     Uwaga

     Jeśli punkt końcowy nie obsługuje języka serwera OfficeScan, wyświetla treści w języku angielskim.

5. Kliknij przycisk **Zapisz**.

Agent Mover

Jeżeli w sieci występuje więcej niż jeden serwer OfficeScan, za pomocą narzędzia Agent Mover można przenieść agentów OfficeScan z jednego serwera OfficeScan na inny. Jest to szczególnie przydatne po dodaniu nowego serwera OfficeScan do sieci w przypadku przenoszenia istniejących agentów OfficeScan na nowy serwer.

Uwaga

Oba serwery muszą być tej samej wersji językowej. W przypadku użycia narzędzia Agent Mover w celu przeniesienia agenta OfficeScan z wcześniejszą wersją na serwer z bieżącą wersją programu, agent OfficeScan zostanie uaktualniony automatycznie.

Przed rozpoczęciem używania narzędzia upewnij się, czy konto, którego używasz ma uprawnienia administratora.

Uruchamianie programu Agent Mover

Procedura

1. Na serwerze OfficeScan przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\IpXfer`.
2. Skopiuj plik `IpXfer.exe` na punkt końcowy Agent OfficeScan. Jeśli punkt końcowy Agent OfficeScan to platforma typu x64, zamiast powyższego pliku skopiuj plik `IpXfer_x64.exe`.
3. Otwórz na punkcie końcowym Agent OfficeScan wiersz polecenia, a następnie przejdź do folderu zawierającego skopiowany plik wykonywalny.
4. Uruchom narzędzie Agent Mover, używając następującej składni:

```
<nazwa pliku wykonywalnego> -s <nazwa serwera> -p <port
nasłuchiwania serwera> -c <port nasłuchiwania agenta> -d
<domena lub hierarchia domeny> -e <lokalizacja i nazwa
pliku certyfikatu> -pwd <hasło uprawnienia do zamykania
i odblokowywania agenta>
```

TABELA 15-3. Parametry narzędzia Agent Mover

PARAMETR	WYJAŚNIENIE
`<nazwa pliku wykonywalnego>`	`IpXfer.exe` lub `IpXfer_x64.exe`
`-s <nazwa serwera>`	Nazwa docelowego serwera OfficeScan (na który zostanie przeniesiony agent Agent OfficeScan).
`-p <port nasłuchiwania serwera>`	Port nasłuchiwania (lub zaufany port) docelowego serwera OfficeScan Aby wyświetlić port nasłuchiwania na konsoli Web programu OfficeScan, kliknij polecenie **Administracja** > **Ustawienia** > **Połączenie agenta** w menu głównym.
`-c <port nasłuchiwania agenta>`	Numer portu używany przez punkt końcowy Agent OfficeScan do komunikowania się z serwerem

PARAMETR	WYJAŚNIENIE
`-d <domena lub hierarchia domeny>`	Domena lub poddomena drzewa agentów, z którą zostanie zgrupowany agent Hierarchia domeny powinna wskazywać poddomenę.
`-e <lokalizacja i nazwa pliku certyfikatu>`	Umożliwia zaimportowanie nowego certyfikatu uwierzytelniającego Agent OfficeScan w trakcie procesu przenoszenia Jeśli ten parametr nie jest używany, Agent OfficeScan automatycznie odczyta bieżący certyfikat uwierzytelniający z nowego serwera, który nim zarządza. **Uwaga** Domyślna lokalizacja certyfikatu na serwerze OfficeScan to: <*Folder instalacji serwera*>`\PCCSRV\Pccnt\Common\OfcNTCer.dat`. Gdy używa się certyfikatu ze źródła innego niż OfficeScan, należy upewnić się, że certyfikat ma format DER (Distinguished Encoding Rules).
`-pwd <hasło uprawnienia do zamykania i odblokowywania agenta>`	Hasło uprawnienia do zamykania i odblokowywania, które skonfigurowano na ekranie Uprawnienia i inne ustawienia **Uwaga** Jeśli hasło do zamykania i odblokowywania jest wymagane, ale nie zostało podane, narzędzie Agent Mover wyświetli monit przed podjęciem próby przeniesienia agentów.

Przykłady:

```
ipXfer.exe -s Server01 -p 8080 -c 21112 -d Workgroup -pwd
unlock
```

```
ipXfer_x64.exe -s Server02 -p 8080 -c 21112 -d Workgroup
\Group01 -pwd unlock
```

5. Aby sprawdzić, czy Agent OfficeScan zgłasza się teraz do innego serwera, wykonaj następujące czynności:

   a. Na punkcie końcowym Agent OfficeScan kliknij prawym przyciskiem myszy ikonę programu Agent OfficeScan na pasku zadań.

   b. Wybierz opcję **Wersje składników**.

   c. W polu **Nazwa/port serwera** sprawdź, któremu serwerowi OfficeScan podlega Agent OfficeScan.

   Uwaga

   Jeżeli Agent OfficeScan nie jest widoczny w drzewie agentów nowego serwera OfficeScan, który nim zarządza, należy ponownie uruchomić główną usługę nowego serwera (`ofservice.exe`).

Nieaktywni Agenci OfficeScan

W przypadku usuwania programu agenta OfficeScan z punktów końcowych za pomocą jego programu dezinstalacyjnego, program agenta OfficeScan powiadamia serwer automatycznie. Kiedy serwer otrzymuje powiadomienie, usuwa ikonę agenta OfficeScan z drzewa agentów w celu wskazania, że agent już nie istnieje.

Jeżeli jednak agent Agent OfficeScan zostanie usunięty za pomocą innych metod, takich jak formatowanie dysku twardego punktu końcowego lub ręczne usunięcie plików agenta OfficeScan, do programu OfficeScan nie dotrą informacje o usunięciu i Agent OfficeScan będzie przedstawiany jako nieaktywny. Jeżeli użytkownik zamknie lub wyłączy agenta OfficeScan na dłuższy czas, serwer również będzie przedstawiać agenta OfficeScan jako nieaktywnego.

Aby w drzewie agentów byli widoczni wyłącznie aktywni agenci, program OfficeScan można skonfigurować tak, aby automatycznie usuwał nieaktywnych agentów z drzewa agentów.

Automatyczne usuwanie nieaktywnych Agenci

Procedura

1. Przejdź do opcji **Administracja** > **Ustawienia** > **Nieaktywni agenci**.
2. Wybierz opcję **Włącz automatyczne usuwanie nieaktywnych agentów**.
3. Określ, po ilu dniach program OfficeScan będzie uważał Agent OfficeScan za nieaktywnego.
4. Kliknij przycisk **Zapisz**.

Połączenie agent-serwer

Agent OfficeScan musi utrzymywać stałe połączenie z serwerem macierzystym, aby mógł aktualizować składniki, odbierać powiadomienia i stosować zmiany konfiguracji we właściwym czasie. Następujące tematy przedstawiają sposób sprawdzania stanu połączenia agenta OfficeScan oraz rozwiązywania problemów z połączeniem:

- *Adresy IP agentów na stronie 5-11*
- *Ikony agenta OfficeScan na stronie 15-27*
- *Sprawdzanie połączenia Agent-serwer na stronie 15-46*
- *Dzienniki sprawdzania połączenia na stronie 15-47*
- *Nieosiągalni agenci na stronie 15-48*

Ikony agenta OfficeScan

Ikona agenta OfficeScan w zasobniku systemowym oferuje wizualne informacje o bieżącym stanie agenta OfficeScan oraz wyświetla monity o wykonanie określonych czynności. Ikona jest zawsze budowana z poniższych podstawowych wskazówek wizualnych.

TABELA 15-4. Stan agenta OfficeScan wskazywany przez ikonę agenta OfficeScan

STAN AGENTA	OPIS	WSKAZÓWKA WIZUALNA
Połączenie agenta z serwerem OfficeScan	Agenci online są połączeni z serwerem OfficeScan. Serwer może inicjować zadania i instalować ustawienia na agentach.	Ikona z symbolem przypominającym uderzenie serca.  Tło ma kolor niebieski lub czerwony, zależnie od stanu usługi skanowania w czasie rzeczywistym.
	Agenci offline są odłączeni od serwera OfficeScan. Serwer nie może zarządzać tymi agentami.	Ikona z symbolem przypominającym brak uderzenia serca.  Tło ma kolor niebieski lub czerwony, zależnie od stanu usługi skanowania w czasie rzeczywistym. Agent może przejść w tryb offline nawet, gdy jest podłączony do sieci. Aby uzyskać szczegółowe informacje na temat tego problemu, patrz *Rozwiązywanie problemów wskazywanych przez ikony agentów OfficeScan na stronie 15-42*.
	Agenci mobilni mogą lub nie mogą komunikować się z serwerem OfficeScan.	Ikona z symbolem biurka i sygnału.  Tło ma kolor niebieski lub czerwony, zależnie od stanu usługi skanowania w czasie rzeczywistym. Aby uzyskać szczegółowe informacje na temat agenci w trybie niezależnym, patrz *Uprawnienie trybu niezależnego Agent OfficeScan na stronie 15-19*.

STAN AGENTA	OPIS	WSKAZÓWKA WIZUALNA
Dostępność źródeł Smart Protection	Źródła Smart Protection to serwery Smart Protection oraz sieć Trend Micro Smart Protection Network. Agenci skanowania standardowego łączą się ze źródłami Smart Protection, aby wysłać zapytania do usługi Web Reputation. Agenci Smart Scan łączą się ze źródłami Smart Protection, aby wysłać zapytania o skanowanie i do usługi Web Reputation.	Ikona ma symbol zaznaczenia, jeśli źródło Smart Protection jest dostępne. 
		Ikona zawiera pasek postępu, jeśli nie jest dostępne żadne źródło Smart Protection, a agent próbuje nawiązać połączenie ze źródłami.  Aby uzyskać szczegółowe informacje na temat tego problemu, patrz *Rozwiązywanie problemów wskazywanych przez ikony agentów OfficeScan na stronie 15-42*.
		W przypadku agentów skanowania standardowego nie jest wyświetlany znacznik wyboru ani pasek postępu, jeśli usługi Web Reputation zostały wyłączone na agencie.

Stan agenta	Opis	Wskazówka wizualna
Status usługi skanowania w czasie rzeczywistym	Program OfficeScan korzysta z usługi skanowania w czasie rzeczywistym zarówno w trakcie skanowania w czasie rzeczywistym, jak i w czasie skanowania ręcznego i zaplanowanego. Gdy usługa nie działa prawidłowo, agenci są narażeni na zagrożenia bezpieczeństwa.	Gdy usługa skanowania w czasie rzeczywistym działa prawidłowo, cała ikona ma niebieski odcień. Do wskazania metody skanowania agenta używane są dwa odcienie koloru niebieskiego. • Skanowanie standardowe:  • Skanowanie Smart Scan: 
		Gdy usługa skanowania w czasie rzeczywistym została wyłączona lub nie działa prawidłowo, cała ikona ma czerwony odcień. Do wskazania metody skanowania agenta używane są dwa odcienie koloru czerwonego. • Skanowanie standardowe:  • Skanowanie Smart Scan:  Aby uzyskać szczegółowe informacje na temat tego problemu, patrz *Rozwiązywanie problemów wskazywanych przez ikony agentów OfficeScan na stronie 15-42*.

Stan agenta	Opis	Wskazówka wizualna
Stan skanowania w czasie rzeczywistym	Skanowanie w czasie rzeczywistym zapewnia ochronę prewencyjną, ponieważ skanuje pliki pod kątem zagrożeń bezpieczeństwa wtedy, gdy są tworzone, modyfikowane lub pobierane.	Nie są dostępne wizualne informacje o tym, czy skanowanie w czasie rzeczywistym jest włączone.
		Jeśli skanowanie w czasie rzeczywistym jest wyłączone, cała ikona jest otoczona czerwonym, przekreślonym okręgiem.  Aby uzyskać szczegółowe informacje na temat tego problemu, patrz *Rozwiązywanie problemów wskazywanych przez ikony agentów OfficeScan na stronie 15-42*.
Stan aktualizacji sygnatur	Aby zapewnić ochronę przed najnowszymi zagrożeniami, agenci muszą regularnie aktualizować sygnatury.	Gdy sygnatura jest aktualna lub od niedawna nieaktualizowana, nie są wyświetlane żadne wskazówki wizualne.
		Gdy sygnatura jest od dawna nieaktualizowana, ikona ma znak wykrzyknika. Oznacza to, że od dłuższego czasu sygnatura nie była aktualizowana.  Szczegółowe informacje o sposobie aktualizowania agentów zawiera temat *Aktualizacje agenta OfficeScan na stronie 6-29*.
Stan licencji wersji próbnej serwera OfficeScan	Agenci online są połączeni z serwerem OfficeScan z wygasłą licencją próbną.	Ta ikona wskazuje, że licencja wersji próbnej na serwerze OfficeScan wygasła. 

Ikony skanowania Smart Scan

Gdy Agenci OfficeScan wykonują skanowanie Smart Scan, może być wyświetlana jedna z poniższych ikon.

TABELA 15-5. Ikony skanowania Smart Scan

IKONA	POŁĄCZENIE Z SERWEREM OFFICESCAN	DOSTĘPNOŚĆ ŹRÓDEŁ SMART PROTECTION	USŁUGA SKANOWANIA W CZASIE RZECZYWISTYM	SKANOWANIE W CZASIE RZECZYWISTYM
	Online	Dostępne	Działa	Włączone
	Online	Dostępne	Działa	Wyłączone
	Online	Dostępne	Wyłączony lub niedziałający	Wyłączony lub niedziałający
	Online	Niedostępny; ponowne łączenie ze źródłem	Działa	Włączone
	Online	Niedostępny; ponowne łączenie ze źródłem	Działa	Wyłączone
	Online	Niedostępny; ponowne łączenie ze źródłem	Wyłączony lub niedziałający	Wyłączony lub niedziałający
	Offline	Dostępne	Działa	Włączone
	Offline	Dostępne	Działa	Wyłączone
	Offline	Dostępne	Wyłączony lub niedziałający	Wyłączony lub niedziałający

Ikona	Połączenie z serwerem OfficeScan	Dostępność źródeł Smart Protection	Usługa skanowania w czasie rzeczywistym	Skanowanie w czasie rzeczywistym
	Offline	Niedostępny; ponowne łączenie ze źródłem	Działa	Włączone
	Offline	Niedostępny; ponowne łączenie ze źródłem	Działa	Wyłączone
	Offline	Niedostępny; ponowne łączenie ze źródłem	Wyłączony lub niedziałający	Wyłączony lub niedziałający
	Tryb niezależny	Dostępne	Działa	Włączone
	Tryb niezależny	Dostępne	Działa	Wyłączone
	Tryb niezależny	Dostępne	Wyłączony lub niedziałający	Wyłączony lub niedziałający
	Tryb niezależny	Niedostępny; ponowne łączenie ze źródłem	Działa	Włączone
	Tryb niezależny	Niedostępny; ponowne łączenie ze źródłem	Działa	Wyłączone
	Tryb niezależny	Niedostępny; ponowne łączenie ze źródłem	Wyłączony lub niedziałający	Wyłączony lub niedziałający

Ikony skanowania standardowego

Gdy Agenci OfficeScan wykonują skanowanie standardowe, może być wyświetlona dowolna z poniższych ikon.

TABELA 15-6. Ikony skanowania standardowego

IKONA	POŁĄCZENIE Z SERWEREM OFFICESCAN	USŁUGI WEB REPUTATION SERVICES DOSTARCZANE PRZEZ ŹRÓDŁA SMART PROTECTION	USŁUGA SKANOWANIA W CZASIE RZECZYWISTYM	SKANOWANIE W CZASIE RZECZYWISTYM	SYGNATURA WIRUSA
	Online	Dostępne	Działa	Włączone	Aktualna lub nieaktualizowana od niedawna
	Online	Niedostępny; ponowne łączenie ze źródłem	Działa	Włączone	Aktualna lub nieaktualizowana od niedawna
	Online	Dostępne	Działa	Włączone	Od dawna nieaktualizowana
	Online	Niedostępny; ponowne łączenie ze źródłem	Działa	Włączone	Od dawna nieaktualizowana
	Online	Dostępne	Działa	Wyłączone	Aktualna lub nieaktualizowana od niedawna
	Online	Niedostępny; ponowne łączenie ze źródłem	Działa	Wyłączone	Aktualna lub nieaktualizowana od niedawna

Ikona	Połączenie z serwerem OfficeScan	Usługi Web Reputation Services dostarczane przez źródła Smart Protection	Usługa skanowania w czasie rzeczywistym	Skanowanie w czasie rzeczywistym	Sygnatura wirusa
	Online	Dostępne	Działa	Wyłączone	Od dawna nieaktualizowana
	Online	Niedostępny; ponowne łączenie ze źródłem	Działa	Wyłączone	Od dawna nieaktualizowana
	Online	Dostępne	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Aktualna lub nieaktualizowana od niedawna
	Online	Niedostępny; ponowne łączenie ze źródłem	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Aktualna lub nieaktualizowana od niedawna
	Online	Dostępne	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Od dawna nieaktualizowana
	Online	Niedostępny; ponowne łączenie ze źródłem	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Od dawna nieaktualizowana
	Offline	Dostępne	Działa	Włączone	Aktualna lub nieaktualizowana od niedawna

Ikona	Połączenie z serwerem OfficeScan	Usługi Web Reputation Services dostarczane przez źródła Smart Protection	Usługa skanowania w czasie rzeczywistym	Skanowanie w czasie rzeczywistym	Sygnatura wirusa
	Offline	Niedostępny; ponowne łączenie ze źródłem	Działa	Włączone	Aktualna lub nieaktualizowana od niedawna
	Offline	Dostępne	Działa	Włączone	Od dawna nieaktualizowana
	Offline	Niedostępny; ponowne łączenie ze źródłem	Działa	Włączone	Od dawna nieaktualizowana
	Offline	Dostępne	Działa	Wyłączone	Aktualna lub nieaktualizowana od niedawna
	Offline	Niedostępny; ponowne łączenie ze źródłem	Działa	Wyłączone	Aktualna lub nieaktualizowana od niedawna
	Offline	Dostępne	Działa	Wyłączone	Od dawna nieaktualizowana
	Offline	Niedostępny; ponowne łączenie ze źródłem	Działa	Wyłączone	Od dawna nieaktualizowana

Ikona	Połączenie z serwerem OfficeScan	Usługi Web Reputation Services dostarczane przez źródła Smart Protection	Usługa skanowania w czasie rzeczywistym	Skanowanie w czasie rzeczywistym	Sygnatura wirusa
	Offline	Dostępne	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Aktualna lub nieaktualizowana od niedawna
	Offline	Niedostępny; ponowne łączenie ze źródłem	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Aktualna lub nieaktualizowana od niedawna
	Offline	Dostępne	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Od dawna nieaktualizowana
	Offline	Niedostępny; ponowne łączenie ze źródłem	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Od dawna nieaktualizowana
	Tryb niezależny	Dostępne	Działa	Włączone	Aktualna lub nieaktualizowana od niedawna
	Tryb niezależny	Niedostępny; ponowne łączenie ze źródłem	Działa	Włączone	Aktualna lub nieaktualizowana od niedawna
	Tryb niezależny	Dostępne	Działa	Włączone	Od dawna nieaktualizowana

Ikona	Połączenie z serwerem OfficeScan	Usługi Web Reputation Services dostarczane przez źródła Smart Protection	Usługa skanowania w czasie rzeczywistym	Skanowanie w czasie rzeczywistym	Sygnatura wirusa
	Tryb niezależny	Niedostępny; ponowne łączenie ze źródłem	Działa	Włączone	Od dawna nieaktualizowana
	Tryb niezależny	Dostępne	Działa	Wyłączone	Aktualna lub nieaktualizowana od niedawna
	Tryb niezależny	Niedostępny; ponowne łączenie ze źródłem	Działa	Wyłączone	Aktualna lub nieaktualizowana od niedawna
	Tryb niezależny	Dostępne	Działa	Wyłączone	Od dawna nieaktualizowana
	Tryb niezależny	Niedostępny; ponowne łączenie ze źródłem	Działa	Wyłączone	Od dawna nieaktualizowana
	Tryb niezależny	Dostępne	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Aktualna lub nieaktualizowana od niedawna
	Tryb niezależny	Niedostępny; ponowne łączenie ze źródłem	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Aktualna lub nieaktualizowana od niedawna

Ikona	Połączenie z serwerem OfficeScan	Usługi Web Reputation Services dostarczane przez źródła Smart Protection	Usługa skanowania w czasie rzeczywistym	Skanowanie w czasie rzeczywistym	Sygnatura wirusa
	Tryb niezależny	Dostępne	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Od dawna nieaktualizowana
	Tryb niezależny	Niedostępny; ponowne łączenie ze źródłem	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Od dawna nieaktualizowana
	Online	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Działa	Włączone	Aktualna lub nieaktualizowana od niedawna
	Online	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Działa	Włączone	Od dawna nieaktualizowana
	Online	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Działa	Wyłączone	Aktualna lub nieaktualizowana od niedawna
	Online	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Działa	Wyłączone	Od dawna nieaktualizowana

Ikona	Połączenie z serwerem OfficeScan	Usługi Web Reputation Services dostarczane przez źródła Smart Protection	Usługa skanowania w czasie rzeczywistym	Skanowanie w czasie rzeczywistym	Sygnatura wirusa
	Online	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Aktualna lub nieaktualizowana od niedawna
	Online	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Od dawna nieaktualizowana
	Offline	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Działa	Włączone	Aktualna lub nieaktualizowana od niedawna
	Offline	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Działa	Włączone	Od dawna nieaktualizowana
	Offline	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Działa	Wyłączone	Aktualna lub nieaktualizowana od niedawna
	Offline	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Działa	Wyłączone	Od dawna nieaktualizowana

Ikona	Połączenie z serwerem OfficeScan	Usługi Web Reputation Services dostarczane przez źródła Smart Protection	Usługa skanowania w czasie rzeczywistym	Skanowanie w czasie rzeczywistym	Sygnatura wirusa
	Offline	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Aktualna lub nieaktualizowana od niedawna
	Offline	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Od dawna nieaktualizowana
	Tryb niezależny	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Działa	Włączone	Aktualna lub nieaktualizowana od niedawna
	Tryb niezależny	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Działa	Włączone	Od dawna nieaktualizowana
	Tryb niezależny	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Działa	Wyłączone	Aktualna lub nieaktualizowana od niedawna
	Tryb niezależny	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Działa	Wyłączone	Od dawna nieaktualizowana

Ikona	Połączenie z serwerem OfficeScan	Usługi Web Reputation Services dostarczane przez źródła Smart Protection	Usługa skanowania w czasie rzeczywistym	Skanowanie w czasie rzeczywistym	Sygnatura wirusa
	Tryb niezależny	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Aktualna lub nieaktualizowana od niedawna
	Tryb niezależny	Nie dotyczy (funkcja Web Reputation wyłączona na agencie)	Wyłączony lub niedziałający	Wyłączony lub niedziałający	Od dawna nieaktualizowana

Rozwiązywanie problemów wskazywanych przez ikony agentów OfficeScan

Jeśli ikona agenta OfficeScan wskazuje dowolny z następujących stanów, należy wykonać niezbędne działania:

Warunek	Opis
Plik sygnatur dawno nie był aktualizowany	Użytkownicy agentów OfficeScan muszą zaktualizować składniki. Za pomocą konsoli Web skonfiguruj ustawienia aktualizacji składników w opcji **Aktualizacje** > **Agenci** > **Aktualizacja automatyczna** lub przyznaj użytkownikom uprawnienie do aktualizacji w opcji **Agenci** > **Zarządzanie agentami>Ustawienia** > **Uprawnienia i inne ustawienia** > **Uprawnienia (karta)** > **Aktualizacje składników**.
Usługa skanowania w czasie rzeczywistym została zatrzymana lub nie działa	Jeśli usługa skanowania w czasie rzeczywistym (OfficeScan NT RealTime Scan) została wyłączona lub nie działa, użytkownicy muszą ręcznie uruchomić usługę z poziomu konsoli Microsoft Management Console.

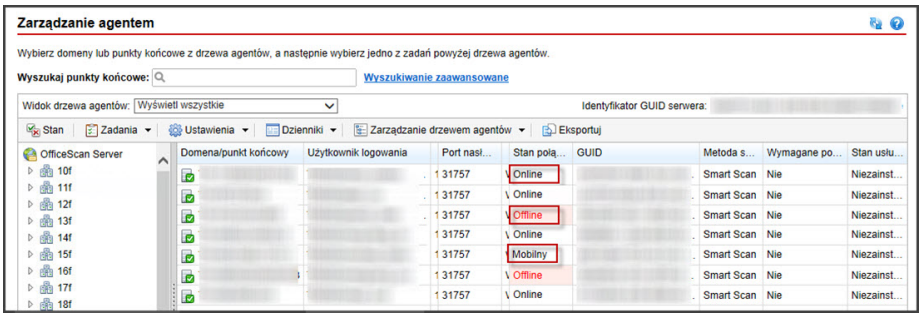
Warunek	Opis
Wyłączono funkcję skanowania w czasie rzeczywistym	Należy włączyć skanowanie w czasie rzeczywistym za pomocą konsoli Web (**Agenci** > **Zarządzanie agentami > Ustawienia** > **Ustawienia skanowania** > **Ustawienia skanowania w czasie rzeczywistym**).
Wyłączono skanowanie w czasie rzeczywistym, a Agent OfficeScan działa w trybie niezależnym	Użytkownik musi najpierw wyłączyć tryb niezależny. Po wyłączeniu trybu niezależnego należy włączyć skanowanie w czasie rzeczywistym z poziomu konsoli Web.
Agent OfficeScan jest podłączony do sieci, ale jest pokazany jako znajdujący się w trybie offline	Sprawdź połączenie za pomocą konsoli Web (**Agenci** > **Sprawdzanie połączenia**), a następnie sprawdź dzienniki sprawdzania połączenia (**Dzienniki** > **Agenci** > **Dzienniki sprawdzania połączenia**). Jeśli po sprawdzeniu Agent OfficeScan nadal pozostaje w stanie offline: 1. Jeśli stan połączenia zarówno agenta OfficeScan, jak i serwera to offline, należy sprawdzić połączenie sieciowe. 2. Jeśli stan połączenia Agent OfficeScan to offline, ale serwer znajduje się w trybie online, mogła ulec zmianie nazwa domeny serwera, a Agent OfficeScan łączy się z serwerem, korzystając z nazwy domeny (w przypadku wybrania nazwy domeny podczas instalacji serwera). Zarejestruj nazwę domeny serwera OfficeScan na serwerze DNS lub WINS bądź dodaj nazwę domeny i informacje o adresie IP do pliku „hosts” na punkcie końcowym agenta w następującym folderze: `<Folder systemu Windows>\system32\drivers\etc` 3. Jeśli stan połączenia agenta OfficeScan to online, a stan serwera to offline, należy sprawdzić ustawienia zapory programu OfficeScan. Zapora może blokować komunikację serwer-agent, ale zezwalać na komunikację agent-serwer. 4. Jeśli stan połączenia agenta OfficeScan to online, a stan serwera to offline, zmiana adresu IP agenta OfficeScan mogła nie zostać zaktualizowana na serwerze (na przykład

Warunek	Opis
	w przypadku ponownego załadowania agenta). Należy spróbować ponownie zainstalować agenta OfficeScan.
Źródła programu Smart Protection są niedostępne	Jeśli agent utraci połączenie ze źródłami programu Smart Protection, należy wykonać następujące czynności: 1. W konsoli Web przejdź do ekranu **Lokalizacja punktu końcowego** (**Agenci** > **Lokalizacja punktu końcowego**) i sprawdź, czy następujące ustawienia lokalizacji punktu końcowego zostały prawidłowo skonfigurowane: • serwery odniesienia i numery portów, • adresy IP bramy. 2. W konsoli Web przejdź do ekranu Źródło programu Smart Protection (**Administracja** > **Smart Protection** > **Źródła programu Smart Protection**), a następnie wykonaj następujące czynności: a. Sprawdź, czy ustawienia serwera Smart Protection na standardowej lub niestandardowej liście źródeł są prawidłowe. b. Sprawdź, czy można nawiązać połączenie z serwerami. c. Kliknij opcję **Powiadom wszystkich agentów** po skonfigurowaniu listy źródeł. 3. Sprawdź, czy na serwerze Smart Protection i na agencie OfficeScan są zsynchronizowane następujące pliki: • `sscfg.ini` • `ssnotify.ini` 4. Otwórz Edytor rejestru i sprawdź, czy agent jest połączony z siecią korporacyjną. Klucz: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\iCRC Scan\Scan Server` • Jeśli wartość `LocationProfile=1`, Agent OfficeScan jest połączony z siecią i powinien mieć możliwość nawiązania połączenia z serwerem Smart Protection.

Warunek	Opis
	• Jeśli wartość `LocationProfile=2`, Agent OfficeScan nie jest połączony z siecią i powinien połączyć się z siecią Smart Protection Network. Sprawdź za pomocą programu Internet Explorer, czy punkt końcowy Agent OfficeScan ma dostęp do stron internetowych. 5. Sprawdź ustawienia wewnętrznego i zewnętrznego serwera proxy używane do połączenia z siecią Smart Protection Network i serwerami Smart Protection. Szczegółowe informacje zawiera sekcja *Wewnętrzny serwer proxy dla agentów OfficeScan na stronie 15-52* i *Zewnętrzny serwer proxy dla agentów OfficeScan na stronie 15-53*. 6. W przypadku agentów skanowania standardowego z systemami Windows XP, Vista, Server 2003 lub Server 2008 należy sprawdzić, czy uruchomiono usługę proxy OfficeScan NT (`TmProxy.exe`). Jeśli usługa zostanie zatrzymana, agenci nie mogą połączyć się ze źródłami Smart Protection w celu wysłania zapytania do usługi Web Reputation. W przypadku agentów skanowania standardowego z systemami operacyjnymi Windows 7, Server 2012 i nowszymi wersjami należy sprawdzić, czy uruchomiono sterownik tmusa. Jeśli sterownik zostanie zatrzymany, agenci nie mogą połączyć się ze źródłami programu Smart Protection w celu wysłania zapytania do usługi Web Reputation.

Sprawdzanie połączenia Agent-serwer

Stan połączenia agenta z serwerem OfficeScan jest wyświetlany w drzewie agentów konsoli Web programu OfficeScan.



ILUSTRACJA 15-2. Drzewo agentów wyświetlające stan połączenia agenta z serwerem OfficeScan

W niektórych przypadkach wyświetlenie prawidłowego stanu połączenia agenta w drzewie agentów. Przykładowo przypadkowe wyjęcie kabla sieciowego agenta może uniemożliwić powiadomienie serwera, że agent działa w trybie offline. W drzewie agentów stan tego agenta będzie wciąż wyświetlany jako online.

Należy ręcznie sprawdzić połączenie agent-serwer lub umożliwić programowi OfficeScan przeprowadzenie sprawdzania zaplanowanego. Nie można wybrać określonych domen lub agentów, a następnie zweryfikować ich stanu połączenia. Program OfficeScan sprawdza stan połączenia ze wszystkimi zarejestrowanymi agentami.

Sprawdzanie połączenia agent-serwer

Procedura

1. Przejdź do opcji **Agenci** > **Sprawdzanie połączenia**.
2. Aby ręcznie sprawdzić połączenie agent-serwer, przejdź do karty **Sprawdzanie ręczne** i kliknij polecenie **Sprawdź teraz**.

3. Aby automatycznie sprawdzić połączenie agent-serwer, przejdź do karty **Sprawdzanie zaplanowane**.

   a. Wybierz polecenie **Włącz sprawdzanie zaplanowane**.

   b. Określ częstotliwość weryfikacji i godzinę rozpoczęcia.

   c. Kliknij przycisk **Zapisz**, aby zapisać harmonogram sprawdzania.

4. Sprawdź drzewo agentów, aby zweryfikować stan lub wyświetlić dzienniki sprawdzania połączenia.

Dzienniki sprawdzania połączenia

Program OfficeScan przechowuje dzienniki sprawdzania połączenia, dzięki czemu można określić, czy serwer OfficeScan może komunikować się ze wszystkimi zarejestrowanymi agentami. Program OfficeScan tworzy wpis w dzienniku za każdym razem, gdy z poziomu konsoli Web sprawdzane jest połączenie agent-serwer.

Aby dzienniki nie zajmowały zbyt dużo miejsca na dysku twardym, można je ręcznie usunąć lub skonfigurować harmonogram ich usuwania. Dodatkowe informacje dotyczące dzienników zarządzania zawiera sekcja *Zarządzanie dziennikiem na stronie 14-41*.

Wyświetlanie dzienników sprawdzania połączenia

Procedura

1. Przejdź do opcji **Dzienniki** > **Agenci** > **Dzienniki sprawdzania połączenia**.

2. Wyświetl wyniki sprawdzania połączenia, zaznaczając kolumnę **Stan**.

3. Aby zapisać dzienniki w formacie `CSV` (plik z tekstem oddzielanym przecinkami), kliknij opcję **Eksportuj do pliku CSV**. Otwórz plik lub zapisz go w określonym miejscu.

Nieosiągalni agenci

Agenci OfficeScan w nieosiągalnych sieciach, np. w segmentach sieci za bramą NAT, są niemal zawsze offline, ponieważ serwer nie może ustanowić bezpośredniego połączenia z agentami. W rezultacie serwer nie może powiadomić agentów, aby:

- Pobrać najnowsze składniki.
- Zastosować ustawienia agenta skonfigurowane przy użyciu konsoli Web. Na przykład po zmianie częstotliwości skanowania zaplanowanego przy użyciu konsoli Web serwer automatycznie powiadomi agentów w celu zastosowania nowego ustawienia.

W związku z powyższym nieosiągalni agenci nie mogą wykonać tych zadań we właściwym czasie. Wykonują zadania tylko wtedy, gdy inicjują połączenie z serwerem, co ma miejsce, gdy:

- Rejestrują się do serwera po instalacji.
- Ponownie uruchamiają się lub ładują. To zdarzenie nie występuje często i zwykle wymaga interwencji użytkownika.
- Aktualizacja ręczna lub zaplanowana jest wyzwalana na agencie. Również to zdarzenie nie występuje często.

Tylko podczas rejestracji, ponownego uruchomienia lub ładowania serwer staje się „świadomy" łączności z agentami i traktuje je tak, jakby były online. Serwer nadal nie może jednak nawiązać połączenia z agentami, więc natychmiast zmienia stan na offline.

Program OfficeScan zapewnia funkcje „pulsu" i sondowania serwera umożliwiające rozwiązanie problemów związanych z nieosiągalnymi agentami. Dzięki tym funkcjom serwer przestaje powiadamiać agentów o aktualizacjach składników i zmianach ustawień. Zamiast tego przyjmuje pasywną rolę i zawsze czeka, aż agenci wyślą puls lub zainicjują sondowanie. Kiedy serwer wykryje dowolne z tych zdarzeń, traktuje agentów jak dostępnych online.

Uwaga

Zdarzenia inicjowane przez agenta i niepowiązane z pulsami czy sondowaniem serwera, takie jak ręczna aktualizacja agenta i wysyłanie dziennika, nie wyzwalają aktualizacji stanu nieosiągalnych agentów przez serwer.

Puls

Agenci OfficeScan wysyłają komunikaty pulsu, aby powiadomić serwer, że połączenie od agenta nadal działa. Po otrzymaniu komunikatu pulsu serwer traktuje agenta jako agenta online. Agent w drzewie agentów może mieć stan:

- **Online**: zwykli agenci online
- **Niedostępne/Online**: agenci online w nieosiągalnej sieci

Uwaga

Agenci OfficeScan nie aktualizują składników ani nie stosują nowych ustawień podczas wysyłania komunikatów pulsu. Zwykli agenci wykonują te zadania podczas rutynowych aktualizacji (patrz *Aktualizacje agenta OfficeScan na stronie 6-29*). Agenci w nieosiągalnej sieci wykonują te zadania podczas sondowania serwera.

Funkcja pulsu rozwiązuje problem polegający na tym, że Agenci OfficeScan w nieosiągalnych sieciach zawsze pojawiają się jako agenci offline nawet wtedy, gdy mogą połączyć się z serwerem.

Ustawienie w konsoli Web steruje częstotliwością wysyłania komunikatów pulsu przez agentów. Jeśli serwer nie otrzyma pulsu, nie potraktuje natychmiast agentów jako agentów offline. Inne ustawienie steruje ilością czasu bez pulsu, jaki musi upłynąć przed zmianą stanu agenta na:

- **Offline**: zwykli Agenci OfficeScan offline
- **Niedostępne/Offline**: Agenci OfficeScan offline w nieosiągalnej sieci

Wybierając ustawienie pulsu, należy osiągnąć równowagę między potrzebą wyświetlania najbardziej aktualnych informacji o stanie agenta a koniecznością zarządzania zasobami systemowymi. W większości przypadków domyślne ustawienie jest zadowalające. Dostosowując ustawienia pulsu, należy wziąć pod uwagę następujące zagadnienia:

TABELA 15-7. Zalecenia dotyczące pulsu

CZĘSTOTLIWOŚĆ PULSU	ZALECENIE
Długie interwały między pulsami (powyżej 60 minut)	Im dłuższy interwał między pulsami, tym więcej zdarzeń może wystąpić, zanim serwer odzwierciedli stan agenta w konsoli Web.
Krótkie interwały miedzy pulsami (poniżej 60 minut)	Dzięki krótkim interwałom prezentowany stan agenta jest bardziej aktualny, ale mogą one powodować większe wykorzystanie przepustowości.

Sondowanie serwera

Funkcja sondowania serwera rozwiązuje problem nieosiągalnych agentów OfficeScan nieotrzymujących na czas powiadomień o aktualizacjach składników i zmianach ustawień agenta. Działa niezależnie od funkcji pulsu.

Przy użyciu funkcji sondowania serwera:

- Agenci OfficeScan automatycznie inicjują połączenie z serwerem OfficeScan w regularnych interwałach. Kiedy serwer wykryje wykonane sondowanie, potraktuje agenta jako „Nieosiągalnego/Online".
- Agenci OfficeScan nawiązują połączenia z jednym lub kilkoma źródłami aktualizacji, aby pobrać dowolne aktualizowane składniki zastosować nowe ustawienia agenta. Jeśli podstawowym źródłem aktualizacji jest serwer OfficeScan lub agent aktualizacji, agenci pozyskują zarówno składniki, jak i nowe ustawienia. Jeśli źródłem nie jest serwer OfficeScan lub agent aktualizacji, agenci pozyskują tylko zaktualizowane składniki, a następnie łączą się z serwerem OfficeScan lub agentem aktualizacji w celu uzyskania nowych ustawień.

Konfigurowanie pulsu i sondowania serwera

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.

2. Kliknij kartę **Sieć**.
3. Przejdź do sekcji **Sieć nieosiągalna**.
4. Skonfiguruj ustawienia sondowania serwera.

   Szczegółowe informacje o sondowaniu serwera zawiera sekcja *Sondowanie serwera na stronie 15-50*.

   a. Jeśli serwer OfficeScan ma zarówno adres IPv4, jak i adres IPv6, można wpisać zakres adresów IPv4 oraz prefiks IPv6 i długość.

      Wpisz zakres adresów IPv4, jeśli serwer korzysta wyłącznie z protokołu IPv4, lub prefiks IPv6 i długość, jeśli serwer korzysta wyłącznie z protokołu IPv6.

      Jeśli adres IP agenta będzie zgodny z adresem IP w zakresie, agent zastosuje ustawienia pulsu i sondowania serwera, a serwer będzie traktował agenta jak część nieosiągalnej sieci.

      Uwaga

      Agenci z adresem IPv4 mogą nawiązać połączenie z serwerem OfficeScan korzystającym wyłącznie z protokołu IPv4 lub z dwoma stosami.

      Agenci z adresem IPv6 mogą nawiązać połączenie z serwerem OfficeScan korzystającym wyłącznie z protokołu IPv6 lub z dwoma stosami.

      agenci z dwoma stosami mogą nawiązać połączenie z serwerem OfficeScan z dwoma stosami, korzystającym wyłącznie z protokołu IPv4 lub korzystającym wyłącznie z protokołu IPv6.

   b. W polu **Agenci sondują serwer pod względem zaktualizowanych składników i ustawień co __ min** określ częstotliwość sondowania serwera. Wpisz wartość z zakresu od 1 do 129 600 minut.

      Porada

      Firma Trend Micro zaleca, aby częstotliwość sondowania serwera była co najmniej trzykrotnością częstotliwości wysyłania pulsu.

5. Skonfiguruj ustawienia pulsu.

   Szczegółowe informacje o funkcji pulsu zawiera sekcja *Puls na stronie 15-49*.

a. Wybierz opcję **Zezwalaj agentom na wysyłanie pulsów na serwer**.

b. Wybierz opcję **Wszyscy agenci** lub **Tylko agenci w nieosiągalnej sieci**.

c. W polu **Agenci wysyłają puls co __ min** określ częstotliwość, z jaką agenci wysyłają puls. Wpisz wartość z zakresu od 1 do 129 600 minut.

d. W polu **Agent jest offline, jeśli brak pulsu po upływie __ min** określ czas bez pulsu, jaki musi upłynąć, zanim serwer OfficeScan będzie traktować agent jako offline. Wpisz wartość z zakresu od 1 do 129 600 minut.

6. Kliknij przycisk **Zapisz**.

Ustawienia serwera proxy agenta OfficeScan

Agentów OfficeScan można skonfigurować tak, aby podczas łączenia się z wewnętrznymi i zewnętrznymi serwerami wykorzystywali ustawienia serwera proxy.

Wewnętrzny serwer proxy dla agentów OfficeScan

Agenci OfficeScan mogą korzystać z ustawień wewnętrznego serwera proxy, łącząc się z następującymi serwerami w sieci:

- Serwer OfficeScan

  Na komputerze serwera jest zainstalowany serwer OfficeScan i zintegrowany Serwer Smart Protection. Agenci OfficeScan łączą się z serwerem OfficeScan w celu aktualizacji składników, pobierania ustawień konfiguracji i wysyłania dzienników. Agenci OfficeScan łączą się ze zintegrowanym serwerem Smart Protection, aby wysyłać żądania skanowania.

- serwery Smart Protection

  serwery Smart Protection obejmują wszystkie samodzielne i zintegrowane serwery Smart Protection innych serwerów OfficeScan. Agenci OfficeScan łączą się z tymi serwerami, aby wysyłać żądania skanowania i zapytania usługi Web Reputation.

Konfigurowanie ustawień wewnętrznego proxy

Procedura

1. Przejdź do opcji **Administracja** > **Ustawienia** > **Serwer proxy**.
2. Kliknij kartę **Wewnętrzny serwer proxy**.
3. Przejdź do sekcji **Połączenie agenta z serwerem OfficeScan**.
   a. Wybierz opcję **Używaj następujących ustawień serwera proxy, gdy agenci nawiązują połączenie z serwerem OfficeScan**.
   b. Wpisz nazwę serwera proxy lub jego adres IPv4/IPv6 i numer portu.

   Uwaga

   Jeśli istnieją agenci IPv4 i IPv6, określ serwer proxy z dwoma stosami, który jest identyfikowany przez jego nazwę hosta. Jest to spowodowane tym, że ustawienia wewnętrznego serwera proxy są ustawieniami globalnymi. Jeśli zostanie określony adres IPv4, agenci IPv6 nie będą mogli połączyć się z serwerem proxy. Analogiczna zasada odnosi się do agentów IPv4.

   c. Jeżeli serwer proxy wymaga uwierzytelniania, wpisz nazwę użytkownika i hasło, a następnie potwierdź hasło.
4. Przejdź do sekcji **Połączenie agenta z oddzielnymi Serwer Smart Protection**.
   a. Wybierz opcję **Używaj następujących ustawień serwera proxy, gdy agenci nawiązują połączenie z oddzielnymi Serwer Smart Protection**.
   b. Wpisz nazwę serwera proxy lub jego adres IPv4/IPv6 i numer portu.
   c. Jeżeli serwer proxy wymaga uwierzytelniania, wpisz nazwę użytkownika i hasło, a następnie potwierdź hasło.
5. Kliknij przycisk **Zapisz**.

Zewnętrzny serwer proxy dla agentów OfficeScan

Serwer OfficeScan i Agent OfficeScan, łącząc się z serwerami obsługiwanymi przez firmę Trend Micro, mogą korzystać z ustawień zewnętrznego serwera proxy. W tym

temacie omówiono ustawienia zewnętrznego serwera proxy dotyczące agentów. Więcej informacji na temat zewnętrznych ustawień proxy serwera zawiera sekcja *Serwer proxy do aktualizacji serwera OfficeScan na stronie 6-21*.

Agenci OfficeScan mogą korzystać z ustawień proxy skonfigurowanych w przeglądarce Internet Explorer lub Chrome do łączenia się z siecią Trend Micro Smart Protection Network. Jeśli jest wymagane uwierzytelnienie serwera proxy, agenci stosują poświadczenia uwierzytelniania serwera proxy (identyfikator i hasło użytkownika).

Konfiguracja poświadczeń uwierzytelniania serwera proxy

Procedura

1. Przejdź do opcji **Administracja** > **Ustawienia** > **Serwer proxy**.
2. Kliknij kartę **Zewnętrzny serwer proxy**.
3. Przejdź do sekcji **Połączenie agenta z serwerami Trend Micro**.
4. Wpisz identyfikator użytkownika oraz hasło wymagane do uwierzytelniania na serwerze proxy. Są obsługiwane następujące protokoły uwierzytelniania serwera proxy:
   - podstawowe uwierzytelnianie dostępu,
   - skrócone uwierzytelnianie dostępu,
   - zintegrowane uwierzytelnianie systemu Windows.
5. Kliknij przycisk **Zapisz**.

Konfigurowanie ustawień serwera proxy usługi Global Smart Protection

Agenci OfficeScan używają skonfigurowanych ustawień usługa proxy Smart Protection podczas zapytania źródeł programu Smart Protection o następujące funkcje:

- Predykcyjne uczenie maszynowe

- Monitorowanie zachowania

Uwaga

Jeśli zintegrowany Serwer Smart Protection jest niedostępny, Agenci OfficeScan łączą się z siecią Trend Micro Smart Protection Network podczas wykonywania zapytań.

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Kliknij kartę **System**.
3. Przejdź do sekcji **Usługa proxy Smart Protection**.
4. Włącz ustawienie **Używaj skonfigurowanych źródeł usługi Smart Protection do obsługi zapytań**.

Ważne

Usługa proxy Smart Protection obsługuje protokół HTTPS wyłącznie dla zapytań usługi File Reputation. Należy upewnić się, że wszystkie skonfigurowane serwery Smart Protection świadczące usługi File Reputation używają protokołu HTTPS.

Domyślnie zintegrowany Serwer Smart Protection nie używa komunikacji HTTPS. Sposób zmiany metody komunikacji opisano w temacie *Konfigurowanie ustawień zintegrowanego serwera Smart Protection na stronie 4-22*.

Sposób weryfikacji metody komunikacji używanej przez autonomiczne serwery Smart Protection opisano w temacie *Konfigurowanie list niestandardowych źródeł Smart Protection na stronie 4-28*.

5. Kliknij przycisk **Zapisz**.

Uprawnienia do konfiguracji proxy dla agentów

Można przydzielać użytkownikom agenta uprawnienie do konfigurowania ustawień serwera proxy. Agenci OfficeScan wykorzystują konfigurowane przez użytkownika ustawienia proxy tylko w następujących przypadkach:

- Gdy Agenci OfficeScan wykonują funkcję „Aktualizuj teraz”.
- Gdy użytkownicy wyłączą automatyczne ustawienia proxy lub gdy Agent OfficeScan nie może ich wykryć.

  Patrz *Automatyczne ustawienia proxy dla agenta OfficeScan na stronie 15-57* Aby uzyskać więcej informacji.

OSTRZEŻENIE!

Niepoprawnie skonfigurowane przez użytkownika ustawienia proxy mogą spowodować problemy z aktualizacją. Należy zachować ostrożność przy przyznawaniu użytkownikom możliwości konfiguracji własnych ustawień serwera proxy.

Przyznawanie uprawnień do konfiguracji proxy

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Na karcie **Uprawnienia** przejdź do sekcji **Ustawienia serwera proxy**.
5. Wybierz opcję **Zezwalaj użytkownikom na konfigurowanie ustawień proxy**.
6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:
   - **Zastosuj do wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.

- **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Automatyczne ustawienia proxy dla agenta OfficeScan

Ręczne konfigurowanie ustawień serwera proxy może być dla wielu użytkowników końcowych skomplikowanym zadaniem. Użyj automatycznych ustawień serwera proxy, aby zapewnić stosowanie właściwych ustawień serwera proxy bez ingerencji użytkownika.

Po włączeniu tej opcji automatyczne ustawienia proxy są głównymi ustawieniami proxy, gdy Agenci OfficeScan aktualizują składniki poprzez aktualizację automatyczną albo w ramach funkcji Aktualizuj teraz. Informacje dotyczące automatycznej aktualizacji i funkcji Aktualizuj teraz zawiera rozdział *Metody aktualizacji agenta OfficeScan na stronie 6-39*.

Jeśli Agenci OfficeScan nie mogą łączyć się za pomocą automatycznych ustawień serwera proxy, użytkownicy agenta z uprawnieniem do konfigurowania ustawień serwera proxy mogą użyć skonfigurowanych przez siebie ustawień proxy. W przeciwnym razie nawiązanie połączenia przy użyciu automatycznych ustawień serwera proxy nie powiedzie się.

Uwaga

Autoryzacja serwera proxy nie jest obsługiwana.

Konfigurowanie ustawień automatycznego proxy

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Kliknij kartę **Sieć**.
3. Przejdź do sekcji **Konfiguracja serwera proxy**.

4. Wybierz opcję **Automatyczne wykrywanie ustawień**, aby program OfficeScan automatycznie wykrywał ustawienia serwera proxy skonfigurowane przez administratora za pomocą protokołu DHCP lub DNS.

5. Aby program OfficeScan korzystał z ustawionego przez administratora sieci skryptu automatycznej konfiguracji serwera proxy (PAC) w celu wykrycia odpowiedniego serwera proxy:

   a. Wybierz opcję **Użyj skryptu automatycznej konfiguracji**.

   b. Wpisz adres skryptu PAC.

6. Kliknij przycisk **Zapisz**.

Wyświetlanie informacji o agencie OfficeScan

Na ekranie Wyświetlanie stanu wyświetlane są istotne informacje o agentach OfficeScan, z uwzględnieniem uprawnień, szczegółów oprogramowania agenta i zdarzeń systemowych.

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.

2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, albo wybierz określone domeny lub agentów.

3. Kliknij opcję **Stan**.

4. Wyświetl informacje o stanie, rozwijając nazwę punktu końcowego agenta. Jeśli wybrano wielu agentów OfficeScan, kliknij przycisk **Rozwiń wszystkie**, aby wyświetlić informacje o stanie wszystkich wybranych agentów.

5. (Opcjonalnie) Użyj przycisków **Resetuj**, aby wyzerować licznik zagrożeń bezpieczeństwa.

Importowanie i eksportowanie ustawień

Program OfficeScan umożliwia wyeksportowanie do pliku ustawień drzewa agentów zastosowanych przez określonego agenta OfficeScan lub domenę. Następnie można zaimportować ten plik w celu zastosowania ustawień dla innych agentów i domen lub innego serwera OfficeScan o tej samej wersji.

Eksportowane są wszystkie ustawienia drzewa agentów z wyjątkiem ustawień agenta aktualizacji.

Eksportowanie ustawień agenta

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, albo wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Ustawienia eksportu**.
4. Kliknij dowolne łącze, aby przeglądać ustawienia wybranego agenta OfficeScan lub domeny.
5. Kliknij opcję **Eksportuj**, aby zapisać ustawienia.

   Ustawienia zostaną zapisane w pliku z rozszerzeniem `.dat`.
6. Kliknij przycisk **Zapisz**, a następnie określ miejsce zapisu pliku `.dat`.
7. Kliknij przycisk **Zapisz**.

Importowanie ustawień agenta

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.

2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, albo wybierz określone domeny lub agentów.
3. Kliknij opcje **Ustawienia** > **Importuj ustawienia**.
4. Kliknij przycisk **Przeglądaj**, aby zlokalizować plik `.dat` na punkcie końcowym, a następnie kliknij polecenie **Importuj**.

   Zostanie wyświetlony ekran **Importowanie ustawień** zawierający podsumowanie ustawień.
5. Kliknij dowolne łącze, aby wyświetlić szczegółowe informacje o ustawieniach skanowania lub uprawnieniach do zaimportowania.
6. Zaimportuj ustawienia.
   - Jeśli kliknięto ikonę domeny głównej, wybierz opcję **Zastosuj dla wszystkich domen**, a następnie kliknij opcję **Zastosuj do obiektu docelowego**.
   - Jeśli wybrano domeny, wybierz opcję **Zastosuj do wszystkich komputerów należących do wybranych domen**, a następnie kliknij opcję **Zastosuj do obiektu docelowego**.
   - Jeśli wybrano kilku agentów, kliknij opcję **Zastosuj do obiektu docelowego**.

Zgodność z zabezpieczeniami

Za pomocą funkcji Zgodność z zabezpieczeniami można wykryć błędy, wdrożyć rozwiązania i przeprowadzać konserwację infrastruktury sieciowej. Dzięki tej funkcji można skrócić czas wymagany do zabezpieczenia środowiska sieciowego oraz dopasować potrzeby organizacji dotyczące bezpieczeństwa i funkcjonalności.

Są dostępne dwa typy zgodności punktów końcowych z zabezpieczeniami:

- **Zarządzane**: Punkty końcowe z agentami OfficeScan zarządzanymi przez serwer OfficeScan. Szczegółowe informacje zawiera sekcja *Zgodność z zabezpieczeniami dla agentów zarządzanych na stronie 15-61*.
- **Niezarządzane**: w tym następujące elementy:

- Agenci OfficeScan, którzy nie są zarządzani przez serwer OfficeScan
- Punkty końcowe bez zainstalowanego agenta OfficeScan
- Punkty końcowe, z którymi serwer OfficeScan nie może się skomunikować
- Punkty końcowe, których stanu zabezpieczeń nie można zweryfikować

  Szczegółowe informacje zawiera sekcja *Zgodność z zabezpieczeniami dla niezarządzanych punktów końcowych na stronie 15-74*.

Zgodność z zabezpieczeniami dla agentów zarządzanych

Funkcja Zgodność z zabezpieczeniami generuje raport zgodności, który pomaga ocenić stan zabezpieczeń agentów OfficeScan zarządzanych przez serwer OfficeScan. Funkcja Zgodność z zabezpieczeniami może generować raporty zgodności na żądanie lub zgodnie z harmonogramem.

Na ekranie **Ocena ręczna** wyświetlane są następujące karty:

- **Usługi**: Użyj tej karty w celu sprawdzenia, czy usługi agenta działają.

  Szczegółowe informacje zawiera sekcja *Usługi na stronie 15-62*.

- **Składniki**: Użyj tej karty w celu sprawdzenia, czy Agenci OfficeScan mają aktualne składniki.

  Szczegółowe informacje zawiera sekcja *Składniki na stronie 15-63*.

- **Zgodność skanowania**: Użyj tej karty w celu sprawdzenia, czy Agenci OfficeScan regularnie uruchamiają skanowanie.

  Szczegółowe informacje zawiera sekcja *Zgodność skanowania na stronie 15-66*.

- **Ustawienia**: Użyj tej karty w celu sprawdzenia, czy ustawienia agenta są spójne z ustawieniami na serwerze.

  Szczegółowe informacje zawiera sekcja *Ustawienia na stronie 15-68*.

Uwaga

Na karcie **Składniki** mogą zostać wyświetleni Agenci OfficeScan, na których uruchomiona jest bieżąca i wcześniejsze wersje produktu. W przypadku innych kart wyświetlani są tylko Agenci OfficeScan w wersji 10.5, 10.6 lub nowszej.

Ważne

- Funkcja Zgodność z zabezpieczeniami sprawdza stan połączenia Agenci OfficeScan przed wygenerowaniem raportu zgodności. Raport zgodności uwzględnia agentów online i offline, ale nie uwzględnia agentów w trybie niezależnym.
- Konta użytkowników oparte na rolach:
  - Każde konto użytkownika konsoli Web ma całkowicie niezależny zestaw ustawień raportu zgodności. Wszelkie zmiany dokonane w ustawieniach raportu zgodności dla danego konta użytkownika nie wpłyną na ustawienia innych kont użytkowników.
  - Zakres raportu jest zależny od uprawnień do domeny agentów konta użytkownika. Jeśli na przykład przyznano uprawnienia konta użytkownika do zarządzania domenami A i B, raporty konta użytkownika będą wyświetlać tylko dane agentów należących do domen A i B.

    Szczegółowe informacje o kontach użytkowników zawiera temat *Administracja oparta na rolach na stronie 14-3*.

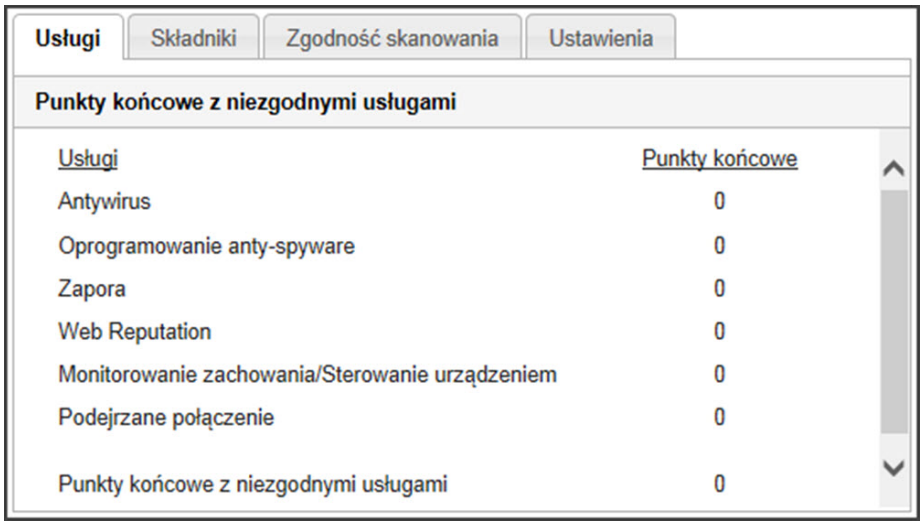
Usługi

Funkcja Zgodność z zabezpieczeniami sprawdza, czy działają następujące usługi agenta OfficeScan:

- Antywirus
- Oprogramowanie anty-spyware
- Zapora
- Usługa Web Reputation
- Usługa Monitorowanie zachowań/kontrola urządzeń (nazywana także usługą zapobiegania nieautoryzowanym zmianom firmy Trend Micro)

- Ochrona danych
- Podejrzane połączenie

Niezgodny agent jest zliczany co najmniej dwa razy w raporcie zgodności.



ILUSTRACJA 15-3. Raport zgodności - karta Usługi

- W kategorii **Punkty końcowe z niezgodnymi usługami**
- W kategorii, w której Agent OfficeScan jest niezgodny. Jeśli na przykład usługa Antywirus agenta OfficeScan nie działa, agent jest zliczany w kategorii **Antywirus**. Jeśli nie działa więcej niż jedna usługa, agent jest zliczany w każdej kategorii, w której jest niezgodny.

Uruchom ponownie niedziałające usługi z poziomu konsoli Web lub agenta OfficeScan. Jeśli usługi będą działać poprawnie po ponownym uruchomieniu, agent nie będzie wyświetlany jako niezgodny podczas następnej oceny.

Składniki

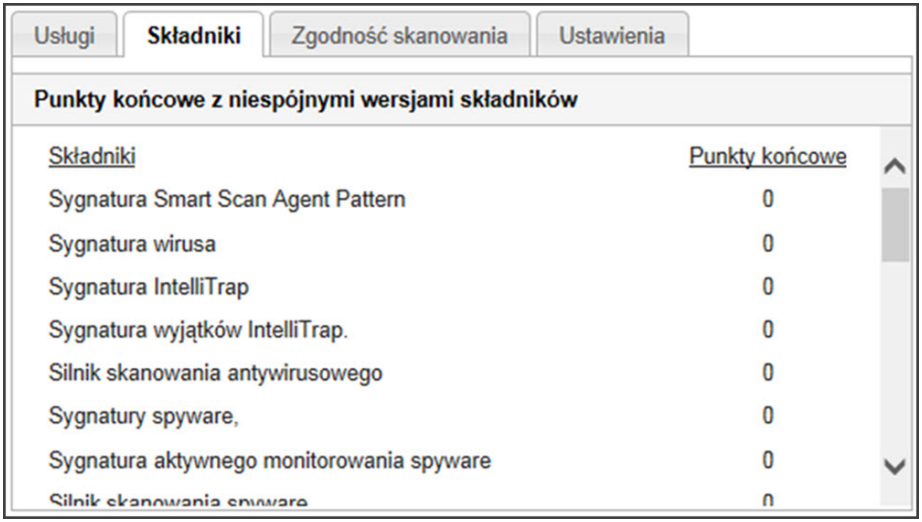
Funkcja Zgodność z zabezpieczeniami umożliwia wykrycie niezgodności wersji składników między serwerem OfficeScan i agentami OfficeScan. Niezgodności

pojawiają się zwykle wtedy, gdy agenci nie mogą połączyć się z serwerem w celu aktualizacji składników. Jeżeli agent pobierze aktualizacje z innego źródła (na przykład z serwera Trend Micro ActiveUpdate Server), może dojść do sytuacji, kiedy wersja składnika agenta będzie nowsza niż wersja na serwerze.

Funkcja Zgodność z zabezpieczeniami sprawdza następujące składniki:

- Sygnatura Agenta Smart Scan
- Sygnatura wirusów
- Sygnatura IntelliTrap
- Sygnatura wyjątków IntelliTrap
- Silnik skanowania antywirusowego, 32-bitowe/64-bitowe
- Sygnatura spyware/grayware
- Sygnatura aktywnego monitorowania oprogramowania spyware
- Silnik skanowania spyware/grayware (32/64-bitowe)
- Szablon usługi Usuwania Szkód
- Silnik usług Usuwania Szkód (32-bitowy/64-bitowy)
- Ogólna sygnatura zapory
- Ogólny sterownik zapory (32/64-bitowe)
- Sterowniki głównego monitora zachowań, 32-bit/64-bit
- Główna usługa monitorowania zachowania, wersja 32-bitowa/64-bitowa
- Sygnatura konfiguracji monitorowania zachowania
- Sygnatura podpisu cyfrowego
- Sygnatura stosowania zasad
- Sygnatura wykrywania funkcji Monitorowanie zachowań (32-bitowa/64-bitowa)
- Globalna lista numerów IP C&C
- Sygnatura reguły istotności
- Sterownik wczesnego czystego rozruchu (32/64-bitowe)
- Sygnatura Memory Scan Trigger Pattern (32/64-bitowe)
- Sygnatura kontroli pamięci
- Sygnatura zapobiegania wykorzystaniu przeglądarki
- Ujednolicona sygnatura analizatora skryptów
- Sygnatura monitorowania inspekcji programów
- Sygnatura przywracania po uszkodzeniach
- Sygnatura wczesnego uruchamiania ochrony przed złośliwym oprogramowaniem (32/64-bitowe)
- Silnik analizy kontekstowej (32/64 bity)
- Sygnatura analizy kontekstowej
- Mechanizm obsługi zapytań analizy kontekstowej (32/64 bity)
- Silnik skanowania w poszukiwaniu zagrożeń zaawansowanych (32/64 bity)
- Wzorzec korelacji zagrożeń zaawansowanych
- Wersja programu

Niezgodny agent jest zliczany co najmniej dwa razy w raporcie zgodności.



ILUSTRACJA 15-4. Raport zgodności - karta Składniki

- W kategorii **Punkty końcowe z niespójnymi wersjami składników**
- W kategorii, w której agent jest niezgodny. Jeśli na przykład wersja sygnatury Smart Scan Agent Pattern jest niespójna z wersją na serwerze, agent jest zliczany w kategorii **Smart Scan Agent Pattern**. Jeśli niespójna jest więcej niż jedna wersja składnika, agent jest zliczany w każdej kategorii, w której jest niezgodny.

Aby rozwiązać niespójności wersji składników, należy zaktualizować nieaktualne składniki na agentach lub serwerze.

Zgodność skanowania

Funkcja Zgodność z zabezpieczeniami pozwala ustalić, czy funkcje Skanuj teraz oraz Skanowanie zaplanowane są uruchamiane regularnie, i czy zostały ukończone w rozsądnym czasie.

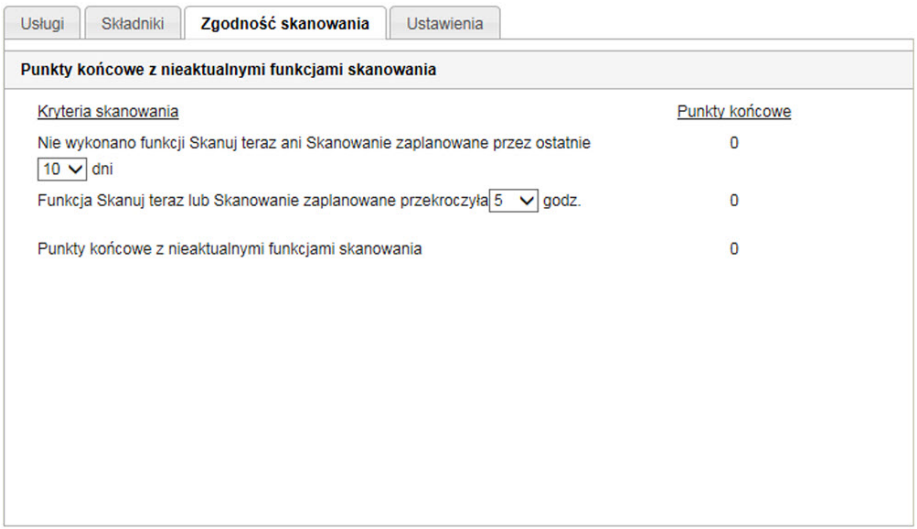
Uwaga

Funkcja Zgodność z zabezpieczeniami może raportować stan skanowania zaplanowanego tylko w przypadku, gdy na agentach włączono skanowanie zaplanowane.

Funkcja Zgodność z zabezpieczeniami używa następujących kryteriów zgodności skanowania:

- **Nie wykonano funkcji Skanuj teraz ani Skanowanie zaplanowane przez ostatnie (x) dni**: Agent OfficeScan jest niezgodny, jeśli nie wykonał funkcji Skanuj teraz ani Skanowanie zaplanowane przez określoną liczbę dni.
- **Czas trwania funkcji Skanuj teraz lub Skanowanie zaplanowane przekroczył (x) godzin**: Agent OfficeScan jest niezgodny, jeśli czas trwania ostatniego wykonywania funkcji Skanuj teraz lub Skanowanie zaplanowane przekroczył określoną liczbę godzin.

Niezgodny agent jest zliczany co najmniej dwa razy w raporcie zgodności.



ILUSTRACJA 15-5. Raport zgodności - karta Zgodność skanowania

- W kategorii **Punkty końcowe z nieaktualnym skanowaniem**
- W kategorii, w której agent jest niezgodny. Jeśli na przykład czas trwania ostatniego zaplanowanego skanowania przekroczył określoną liczbę godzin, agent jest zliczany w kategorii **Czas trwania funkcji Skanuj teraz lub Skanowanie zaplanowane przekroczył <x> godzin**. Jeśli agent spełnia więcej niż jedno kryterium zgodności skanowania, agent jest zliczany w każdej kategorii, w której jest niezgodny.

Należy uruchomić funkcję Skanuj teraz lub Skanowanie zaplanowane na agentach, którzy nie wykonali zadań skanowania lub nie mogli zakończyć skanowania.

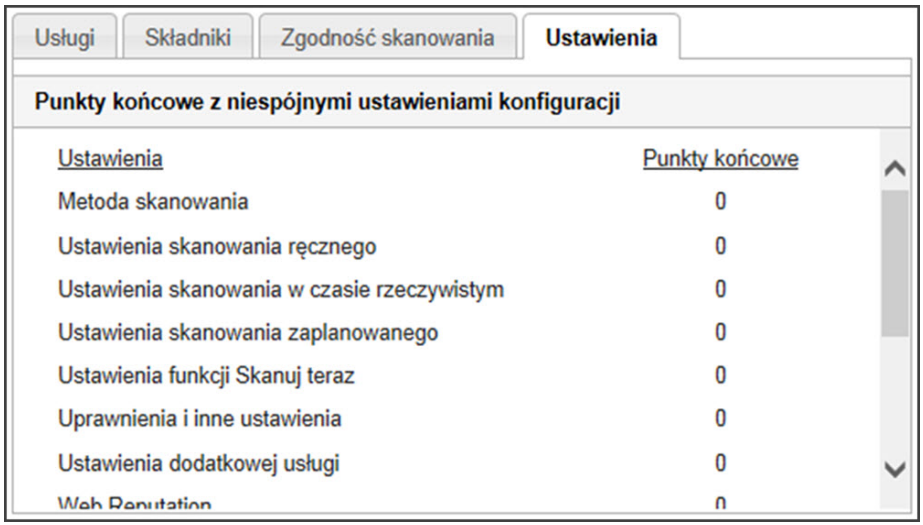
Ustawienia

Funkcja Zgodność z zabezpieczeniami pozwala ustalić, czy agenci i ich domeny nadrzędne w drzewie agentów mają takie same ustawienia. Do niespójności ustawień może dojść, jeżeli agenci zostali przeniesieni do innej domeny, w której stosowany jest inny zbiór ustawień, lub gdy użytkownik agenta posiadający odpowiednie uprawnienia ręcznie skonfigurował ustawienia w konsoli Agent OfficeScan.

Program OfficeScan weryfikuje następujące ustawienia:

- Metoda skanowania
- Ustawienia skanowania ręcznego
- Ustawienia skanowania w czasie rzeczywistym
- Ustawienia skanowania zaplanowanego
- Ustawienia funkcji Skanuj teraz
- Uprawnienia i inne ustawienia
- Dodatkowe ustawienia usługi
- Usługa Web Reputation
- Monitorowanie zachowań
- Kontrola urządzeń
- Lista dozwolonych spyware/grayware
- Ustawienia Zapobieganie utracie danych
- Podejrzane połączenie
- Lista zaufanych programów
- Przesyłanie próbek
- Predykcyjne uczenie maszynowe

Niezgodny agent jest zliczany co najmniej dwa razy w raporcie zgodności.



ILUSTRACJA 15-6. Raport zgodności - karta Ustawienia

- W kategorii **Punkty końcowe z niezgodnymi ustawieniami konfiguracji**
- W kategorii, w której agent jest niezgodny. Jeśli na przykład ustawienia metody skanowania na agencie i w jego domenie nadrzędnej są niespójne, agent jest zliczany w kategorii **Metoda skanowania**. Jeśli niespójny jest więcej niż jeden zestaw ustawień, agent jest zliczany w każdej kategorii, w której jest niezgodny.

Aby rozwiązać niespójności ustawień, należy zastosować ustawienia domeny do agenta.

Raporty zgodności na żądanie

Funkcja Zgodność z zabezpieczeniami może generować raporty zgodności na żądanie. Raporty pomagają ocenić stan zabezpieczeń agentów OfficeScan zarządzanych przez serwer OfficeScan.

Więcej informacji o raportach zgodności zawiera temat *Zgodność z zabezpieczeniami dla agentów zarządzanych na stronie 15-61*.

Generowanie raportów zgodności na żądanie

Procedura

1. Przejdź do opcji **Ocena** > **Zgodność z zabezpieczeniami** > **Raport ręczny**.
2. Przejdź do sekcji **Zakres drzewa agentów**.
3. Wybierz domenę główną lub domenę i kliknij opcję **Ocena**.
4. Wyświetl raport zgodności dla usług agenta.

   Szczegółowe informacje na temat usług agenta zawiera sekcja *Usługi na stronie 15-62*.

   a. Kliknij kartę **Usługi**.

   b. W obszarze **Punkty końcowe z niezgodnymi usługami** sprawdź liczbę agentów z niezgodnymi usługami.

   c. Kliknij łącze z liczbą, aby wyświetlić wszystkich odnośnych agentów w drzewie agentów.

   d. Wybierz agentów z wyników zapytania.

   e. Kliknij opcję **Ponownie uruchom agenta OfficeScan**, aby ponownie uruchomić usługę.

   > **Uwaga**
   >
   > Jeśli po przeprowadzeniu kolejnej oceny agent nadal jest wyświetlany jako niezgodny, należy ręcznie uruchomić ponownie usługę na punkcie końcowym agenta.

   f. Aby zapisać listę agentów w pliku tekstowym, kliknij polecenie **Eksportuj**.

5. Wyświetl raport zgodności dla składników agenta.

   Szczegółowe informacje na temat składników agenta zawiera sekcja *Składniki na stronie 15-63*.

   a. Kliknij kartę **Składniki**.

b. W obszarze **Punkty końcowe z niespójnymi wersjami składników** sprawdź liczbę agentów z wersjami składników, które są niezgodne z wersjami na serwerze.

c. Kliknij łącze z liczbą, aby wyświetlić wszystkich odnośnych agentów w drzewie agentów.

Uwaga

Jeśli co najmniej jeden agent ma bardziej aktualny składnik niż serwer OfficeScan, należy ręcznie zaktualizować serwer OfficeScan.

---

d. Wybierz agentów z wyników zapytania.

e. Kliknij polecenie **Aktualizuj teraz**, aby wymusić pobranie składników przez agentów.

Uwaga

- Aby zapewnić agentom możliwość uaktualnienia programu agenta, wyłącz opcję **Agenci OfficeScan mogą aktualizować składniki, ale nie mogą uaktualniać programu agenta ani instalować pakietów Hot Fix** w sekcji **Agenci** > **Zarządzanie agentami > Ustawienia** > **Uprawnienia i inne ustawienia**.agenciagent
- Ogólny sterownik zapory należy zaktualizować, ponownie uruchamiając punkt końcowy, a nie klikając polecenie **Aktualizuj teraz**.

---

f. Aby zapisać listę agentów w pliku tekstowym, kliknij polecenie **Eksportuj**.

6. Wyświetl raport zgodności dla skanowania.

Szczegółowe informacje na temat skanowania zawiera sekcja *Zgodność skanowania na stronie 15-66*.

a. Kliknij kartę **Zgodność skanowania**.

b. W obszarze **Punkty końcowe z nieaktualnym skanowaniem** skonfiguruj następujące opcje:

- Liczba dni, w ciągu których agent nie wykonał funkcji Skanuj teraz lub Skanowanie zaplanowane

- Liczba godzin czasu trwania funkcji Skanuj teraz lub Skanowanie zaplanowane

Uwaga

Jeżeli liczba dni lub godzin zostanie przekroczona, agent jest traktowany jako niezgodny.

c. Kliknij opcję **Ocena** obok sekcji **Zakres drzewa agentów**.

d. W obszarze **Punkty końcowe z nieaktualnym skanowaniem** sprawdź liczbę agentów spełniających kryteria skanowania.

e. Kliknij łącze z liczbą, aby wyświetlić wszystkich odnośnych agentów w drzewie agentów.

f. Wybierz agentów z wyników zapytania.

g. Kliknij opcję **Skanuj teraz**, aby zainicjować funkcję Skanuj teraz na agentach.

Uwaga

Aby uniknąć powtórzenia skanowania, opcja **Skanuj teraz** zostanie wyłączona, jeśli funkcja Skanuj teraz trwała dłużej niż określona liczba godzin.

h. Aby zapisać listę agentów w pliku tekstowym, kliknij polecenie **Eksportuj**.

7. Wyświetl raport zgodności dla ustawień.

Szczegółowe informacje na temat ustawień zawiera sekcja *Ustawienia na stronie 15-68*.

a. Kliknij kartę **Ustawienia**.

b. W obszarze **Komputery z niezgodnymi ustawieniami konfiguracji** sprawdź liczbę agentów z ustawieniami, które są niezgodne z ustawieniami domeny drzewa agentów.

c. Kliknij łącze z liczbą, aby wyświetlić wszystkich odnośnych agentów w drzewie agentów.

d. Wybierz agentów z wyników zapytania.

e. Kliknij opcję **Zastosuj ustawienia domeny**.

f. Aby zapisać listę agentów w pliku tekstowym, kliknij polecenie **Eksportuj**.

Zaplanowane raporty zgodności

Funkcja Zgodność z zabezpieczeniami może generować raporty zgodności zgodnie z harmonogramem. Raporty pomagają ocenić stan zabezpieczeń agentów OfficeScan zarządzanych przez serwer OfficeScan.

Więcej informacji o raportach zgodności zawiera temat *Zgodność z zabezpieczeniami dla agentów zarządzanych na stronie 15-61*.

Konfigurowanie ustawień zaplanowanych raportów zgodności

Procedura

1. Przejdź do opcji **Ocena** > **Zgodność z zabezpieczeniami** > **Raport zaplanowany**.
2. Wybierz opcję **Włącz zaplanowane raportowanie**.
3. Wprowadź tytuł raportu.
4. Wybierz jeden lub wszystkie następujące elementy:
   - *Usługi na stronie 15-62*
   - *Składniki na stronie 15-63*
   - *Zgodność skanowania na stronie 15-66*
   - *Ustawienia na stronie 15-68*
5. Wprowadź adresy e-mail, które będą odbierać powiadomienia o zaplanowanych raportach zgodności.

Uwaga

Skonfiguruj ustawienia powiadomień e-mail, aby umożliwić pomyślne wysyłanie powiadomień e-mail. Szczegółowe informacje zawiera sekcja *Ustawienia powiadamiania administratorów na stronie 14-37*.

6. Określ harmonogram.
7. Kliknij przycisk **Zapisz**.

Zgodność z zabezpieczeniami dla niezarządzanych punktów końcowych

Funkcja Zgodność z zabezpieczeniami może wyszukiwać niezarządzane punkty końcowe w sieci, do której należy serwer OfficeScan. W celu wyszukania punktów końcowych należy użyć usługi Active Directory i adresów IP.

Możliwe stany zabezpieczeń niezarządzanych punktów końcowych są następujące:

TABELA 15-8. Stan zabezpieczeń niezarządzanych punktów końcowych

STAN	OPIS
Zarządzanie przez inny serwer OfficeScan	Agenci OfficeScan zainstalowani na komputerach są zarządzani przez inny serwer OfficeScan. Agenci OfficeScan są w trybie online, a ich wersja programu OfficeScan ma numer bieżący lub wcześniejszy.
Agent OfficeScan niezainstalowany	Na punkcie końcowym nie jest zainstalowany serwer Agent OfficeScan.
Nieosiągalny	Serwer OfficeScan nie może połączyć się z punktem końcowym i określić jego stanu zabezpieczeń.

Stan	Opis
Nieukończona ocena usługi Active Directory	Punkt końcowy należy do domeny Active Directory, ale serwer OfficeScan nie może określić jego stanu zabezpieczeń. **Uwaga** Lista agentów, którzy są zarządzani przez serwer, jest przechowywana w bazie danych serwera OfficeScan. Serwer przeszukuje usługę Active Directory pod względem identyfikatorów GUID komputerów i porównuje je z identyfikatorami GUID zapisanymi w bazie danych. Jeśli identyfikator GUID nie znajduje się w bazie danych, punkt końcowy zostanie przyporządkowany do kategorii Nieukończona ocena usługi Active Directory.

Aby uruchomić ocenę zabezpieczeń, należy wykonać następujące czynności:

1. Zdefiniuj zakres przeszukiwania. Szczegółowe informacje zawiera sekcja *Definiowanie ustawień przeszukiwania i zakresu obiektów usługi Active Directory / adresów IP na stronie 15-75*.

2. Sprawdź niezabezpieczone komputery z wyników przeszukiwania. Szczegółowe informacje zawiera sekcja *Wyświetlanie wyników zapytania na stronie 15-78*.

3. Zainstaluj agenta OfficeScan Szczegółowe informacje zawiera sekcja *Instalowanie zgodne z zabezpieczeniami na stronie 5-69*.

4. Skonfiguruj przeszukiwanie zaplanowane. Szczegółowe informacje zawiera sekcja *Konfigurowanie oceny przeszukiwania zaplanowanego na stronie 15-79*.

Definiowanie ustawień przeszukiwania i zakresu obiektów usługi Active Directory / adresów IP

Podczas pierwszego wyszukiwania należy zdefiniować zakres obiektów usługi Active Directory/adresów IP. Dotyczy do obiektów usługi Active Directory oraz adresów IP, które będą okresowo lub na żądanie przeszukiwane przez serwer OfficeScan. Po zdefiniowaniu zakresu należy rozpocząć proces przeszukiwania.

Uwaga

Aby zdefiniować zakres obiektów usługi Active Directory, program OfficeScan najpierw zostać zintegrowany z usługą Active Directory. Szczegółowe informacje o integracji zawiera temat *Integracja usługi Active Directory na stronie 2-41*.

Procedura

1. Przejdź do opcji **Ocena** > **Niezarządzane punkty końcowe**.
2. W sekcji **Zakres obiektów usługi Active Directory/adresów IP** kliknij opcję **Zdefiniuj zakres**.

   Zostanie wyświetlony nowy ekran.
3. Aby zdefiniować zakres obiektów usługi Active Directory:

   a. Przejdź do sekcji **Zakres obiektów usługi Active Directory**.

   b. Wybierz opcję **Zastosuj ocenę na żądanie**, aby wysyłać żądania przeszukiwania w czasie rzeczywistym i uzyskiwać dokładniejsze wyniki. Wyłączenie tej opcji powoduje, że program OfficeScan przeszukuje bazę danych, a nie poszczególnych agentów OfficeScan. Przeszukiwanie tylko bazy danych może być szybsze, ale jest mniej dokładne.

   c. Wybierz obiekty do przeszukania. W przypadku pierwszego przeszukiwania należy wybrać obiekt, który ma mniej niż 1,000 kont, a następnie zapisać łączny czas realizacji polecenia przeszukiwania. Te dane należy następnie wykorzystywać jako wynik porównawczy.
4. Aby zdefiniować zakres adresów IP:

   a. Przejdź do sekcji **Zakres adresów IP**.

   b. Wybierz opcję **Włącz zakres adresów IP**.

   c. Podaj zakres adresów IP. Aby dodać lub usunąć zakresy adresów IP, naciśnij przycisk plusa lub minusa.

   - W przypadku serwera OfficeScan korzystającego wyłącznie z protokołu IPv4 wpisz zakres adresów IPv4.

- W przypadku serwera OfficeScan korzystającego wyłącznie z protokołu IPv6 wpisz prefiks IPv6 i długość.
- W przypadku serwera OfficeScan z dwoma stosami wpisz zakres adresów IPv4 i/lub prefiks IPv6 i długość.

  Limit zakresu adresów IPv6 wynosi 16 bitów i jest podobny do limitu zakresu adresów IPv4. Z tego powodu prefiks powinien mieć długość od 112 do 128.

TABELA 15-9. Długości prefiksu i liczba adresów IPv6

DŁUGOŚĆ	LICZBA ADRESÓW IPV6
128	2
124	16
120	256
116	4 096
112	65 536

5. W obszarze Ustawienia zaawansowane określ porty używane przez serwery OfficeScan do komunikacji z agentami. Numer portu jest losowo generowany przez program instalacyjny podczas instalacji serwera OfficeScan.

   Aby sprawdzić, jaki port komunikacyjny jest używany przez serwer OfficeScan, przejdź do **Agenci** > **Zarządzanie agentami** i wybierz domenę. Numer portu wyświetlany jest obok kolumny zawierającej adresy IP. Firma Trend Micro zaleca zapisywanie numerów portów, ponieważ mogą się okazać pomocne w przyszłości.

   a. Kliknij polecenie **Określ porty**.

   b. Wpisz numer portu i kliknij polecenie **Dodaj**. Powtórz tę czynność w przypadku wszystkich numerów portów, które chcesz dodać.

   c. Kliknij przycisk **Zapisz**.

6. Aby sprawdzić łączność punktu końcowego przy użyciu określonego numeru portu, wybierz opcję **Zgłoś niedostępny punkt końcowy, sprawdzając port <x>**. Jeśli połączenie nie jest nawiązywane, program OfficeScan natychmiast traktuje punkt końcowy jako nieosiągalny. Domyślny numer portu to 135.

Włączenie tej opcji powoduje przyspieszenie przeszukiwania. Jeśli nie można nawiązać połączenia z punktem końcowym, serwer OfficeScan może uznać punkt końcowy za nieosiągalny bez konieczności wykonywania dodatkowych zadań związanych z weryfikacją połączenia.

7. Aby zapisać zakres i rozpocząć przeszukiwanie, kliknij polecenie **Zapisz i oceń ponownie**. Aby tylko zapisać ustawienia, kliknij polecenie **Tylko zapisz**.

   Zostanie wyświetlony ekran **Zarządzanie poza serwerem** zawierający wyniki przeszukiwania.

   Uwaga

   Przeszukiwanie może trwać długo, zwłaszcza jeśli określono szeroki zakres. Nie wolno rozpoczynać kolejnej operacji przeszukiwania, jeśli nie został wyświetlony ekran funkcji zarządzania serwerem zewnętrznym z wynikami przeszukiwania. W przeciwnym razie bieżąca sesja przeszukiwania zostanie przerwana i zostanie uruchomiona nowa sesja.

Wyświetlanie wyników zapytania

Wyniki wyszukiwania są wyświetlane w sekcji **Stan zabezpieczeń**. Niezarządzany punkt końcowy może mieć jeden z następujących stanów:

- Zarządzanie przez inny serwer OfficeScan
- Agent OfficeScan niezainstalowany
- Nieosiągalny
- Nieukończona ocena usługi Active Directory

Procedura

1. W sekcji **Stan zabezpieczeń** kliknij łącze z numerem, aby wyświetlić wszystkie odnośne komputery.
2. Za pomocą funkcji wyszukiwania i wyszukiwania zaawansowanego wyszukaj i wyświetl tylko te komputery, które spełniają określone kryteria wyszukiwania.

W przypadku korzystania z funkcji wyszukiwania zaawansowanego należy podać następujące elementy:

- Zakres adresów IPv4
- Prefiks IPv6 i długość (prefiks powinien mieć długość od 112 do 128)
- Nazwa punktu końcowego
- Nazwa serwera OfficeScan
- Drzewo usługi Active Directory
- Stan zabezpieczeń

Program OfficeScan nie zwróci wyników, jeśli nazwa jest niekompletna. Jeśli pełna nazwa nie jest znana, można użyć znaku wieloznacznego (*).

3. Aby zapisać listę komputerów w pliku tekstowym, kliknij polecenie **Eksportuj**.
4. W przypadku agentów OfficeScan zarządzanych przez inny serwer OfficeScan należy za pomocą narzędzia Agent Mover zmienić serwer agentów OfficeScan na bieżący serwer OfficeScan. Dodatkowe informacje dotyczące tego narzędzia zawiera sekcja *Agent Mover na stronie 15-23*.

Konfigurowanie oceny przeszukiwania zaplanowanego

Serwer OfficeScan należy skonfigurować do okresowego przeszukiwania obiektów usługi Active Directory i adresów IP w celu upewnienia się, że są na nich zaimplementowane odpowiednie wytyczne zabezpieczeń.

Procedura

1. Przejdź do opcji **Ocena** > **Niezarządzane punkty końcowe**.
2. Kliknij pozycję **Zdefiniuj harmonogram** w górnej części drzewa agentów.
3. Włącz zaplanowane przeszukiwanie.
4. Określ harmonogram.

5. Kliknij przycisk **Zapisz**.

Trend Micro Virtual Desktop Support

Optymalizacja pulpitów wirtualnych za pomocą funkcji Trend Micro Virtual Desktop Support. Ta funkcja kontroluje zadania agentów OfficeScan znajdujących się na pojedynczym serwerze wirtualnym.

Korzystanie z wielu pulpitów na jednym serwerze oraz wykonywanie zadań skanowania na żądanie lub aktualizacji składników pochłania znaczną część zasobów komputera. Za pomocą tej funkcji można zabronić agentom wykonywania zadań skanowania lub aktualizacji składników w tym samym czasie.

Jeżeli na przykład na serwerze VMware vCenter znajdują się trzy wirtualne pulpity, na których uruchomieni są Agenci OfficeScan, program OfficeScan może uruchomić funkcję Skanuj teraz i wdrożyć aktualizacje dla wszystkich trzech agentów równocześnie. Funkcja Virtual Desktop Support rozpozna, że agenci znajdują się na tym samym serwerze fizycznym. Funkcja Virtual Desktop Support zezwoli na uruchomienie zadania pierwszemu agentowi i wstrzyma wykonanie zadania pozostałym dwóm do momentu zakończenia zadania przez pierwszego agenta.

Funkcja Virtual Desktop Support może być używana na następujących platformach:

- VMware vCenter™ (VMware View™)
- Citrix™XenServer™ (Citrix XenDesktop™)
- Microsoft Hyper-V™ Server

Jeśli administratorzy używają innych aplikacji do wirtualizacji, serwer OfficeScan może także pełnić rolę emulowanego hypervisora w celu zarządzania agentami wirtualnymi.

Więcej informacji na temat tych platform znajduje się w witrynach internetowych VMware View, Citrix XenDesktop lub Microsoft Hyper-V.

Aby zoptymalizować skanowanie na żądanie lub usunąć identyfikatory GUID z obrazów base lub golden, należy użyć narzędzia tworzenia szablonów OfficeScan VDI Pre-Scan Template Generation Tool.

Instalacja funkcji Virtual Desktop Support

Virtual Desktop Support to natywna funkcja programu OfficeScan, która jest jednak licencjonowana oddzielnie. Po zainstalowaniu serwera OfficeScan ta funkcja jest dostępna, ale nie działa. Instalacja tej funkcji oznacza pobranie pliku z serwera ActiveUpdate (lub niestandardowego źródła aktualizacji, jeśli zostało skonfigurowane). Po umieszczeniu pliku na serwerze OfficeScan można aktywować funkcję Virtual Desktop Support, aby włączyć jej pełną funkcjonalność. Instalacja i aktywacja są wykonywane za pomocą programu Plug-In Manager.

Uwaga

Funkcja Virtual Desktop Support nie jest w pełni obsługiwana w środowiskach wykorzystujących wyłącznie protokół IPv6. Szczegółowe informacje zawiera sekcja *Ograniczenia serwera wykorzystującego wyłącznie protokół IPv6 na stronie A-3*.

Instalacja obsługi programu Virtual Desktop

Procedura

1. Otwórz konsolę Web programu OfficeScan i kliknij polecenie **Dodatki** w menu głównym.
2. Na ekranie **Plug-in Manager** przejdź do części **Trend Micro Virtual Desktop Support** i kliknij opcję **Pobieranie**.

   Rozmiar pakietu zostanie wyświetlony obok przycisku **Pobierz**.

   Program Plug-In Manager zapisuje pobrany pakiet w lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Download\Product`.

   Uwaga

   Jeśli program Plug-in Manager nie może pobrać pliku, wznowi automatycznie pobieranie po 24 godzinach. Aby ręcznie uruchomić pobieranie pakietu przez program Plug-in Manager, uruchom ponownie usługę OfficeScan Plug-in Manager z poziomu konsoli Microsoft Management Console.

3. Monitoruj postęp pobierania. Można opuścić ten ekran podczas pobierania.

   W przypadku wystąpienia problemów podczas pobierania pakietu należy sprawdzić dzienniki aktualizacji serwera w konsoli produktu programu OfficeScan. W menu głównym kliknij opcję **Dzienniki** > **Aktualizacje serwera**.

   Po pobraniu pakietu przez program Plug-in Manager zostanie wyświetlony nowy ekran z funkcją Virtual Desktop Support.

   Uwaga

   Jeśli ekran funkcji Virtual Desktop Support nie zostanie wyświetlony, sprawdź przyczyny i sposoby rozwiązania problemu w temacie *Rozwiązywanie problemów z programem Plug-in Manager na stronie 17-13*.

4. Aby natychmiast zainstalować funkcję Virtual Desktop Support, kliknij przycisk **Instaluj teraz**. Aby zainstalować w późniejszym momencie:

   a. Kliknij przycisk **Instaluj później**.

   b. Zostanie wyświetlony ekran **Plug-in Manager**.

   c. Przejdź do sekcji **Trend Micro Virtual Desktop Support** i kliknij przycisk **Instaluj**.

5. Przeczytaj umowę licencyjną i zaakceptuj jej warunki, klikając przycisk **Akceptuję**.

   Rozpocznie się instalacja.

6. Monitoruj postęp instalacji. Po zakończeniu instalacji wyświetlona zostanie wersja funkcji Virtual Desktop Support.

Licencja Virtual Desktop Support

Korzystając z programu Plug-in Manager, można wyświetlać, aktywować i odnawiać licencję Virtual Desktop Support.

Kod aktywacyjny należy uzyskać z firmy Trend Micro, a następnie użyć go w celu włączenia pełnej funkcjonalności Virtual Desktop Support.

Aktywacja lub odnowienie obsługi funkcji Virtual Desktop Support

Procedura

1. Otwórz konsolę Web programu OfficeScan i kliknij polecenie **Dodatki** w menu głównym.
2. Na ekranie **Plug-in Manager** przejdź do części **Trend Micro Virtual Desktop Support** i kliknij opcję **Zarządzaj programem**.
3. Kliknij opcję **Wyświetl informacje o licencji**.
4. Na wyświetlonym ekranie **Szczegóły dotyczące licencji produktu** kliknij polecenie **Nowy kod aktywacyjny**.
5. Na wyświetlonym ekranie wpisz Kod aktywacyjny i kliknij przycisk **Zapisz**.
6. Na ekranie Szczegóły dotyczące licencji kliknij opcję **Informacja o aktualizacji**, aby odświeżyć ekran ze szczegółami nowej licencji i stanem funkcji. Ekran ten zawiera także łącze do witryny internetowej firmy Trend Micro, na której znajdują się szczegółowe informacje o licencji.

Wyświetlanie informacji o licencji funkcji Virtual Desktop Support

Procedura

1. Otwórz konsolę Web programu OfficeScan i kliknij polecenie **Dodatki** > **Zarządzaj programem [Trend Micro Virtual Desktop Support]** w menu głównym.
2. Kliknij opcję **Wyświetl informacje o licencji**.
3. Zapoznaj się ze szczegółami licencjami na wyświetlonym ekranie.

   W sekcji Szczegóły licencji Virtual Desktop Support znajdują się następujące informacje:

- **Stan**: wyświetlana jest wartość „Aktywowane”, „Nieaktywowane” lub „Wygasłe”.
- **Wersja**: wyświetlana jest wartość „Pełna” lub „Próbna”. Jeśli używane są obie wersje, wyświetlana jest wersja „Pełna”.
- **Data wygaśnięcia**: jeśli funkcja Virtual Desktop Support ma przypisanych wiele licencji, jest wyświetlana najpóźniejsza data wygaśnięcia. Na przykład, jeśli licencje wygasają w dniach 31-12-2010 i 30-06-2010, wyświetlana jest data 31-12-2010.
- **Stanowiska**: wyświetla liczbę agentów OfficeScan, którzy mogą korzystać z funkcji Virtual Desktop Support.
- **Kod aktywacyjny**: wyświetla kod aktywacyjny.

Przypomnienia dotyczące licencji są wyświetlane w następujących przypadkach:

Jeśli użytkownik dysponuje licencją na pełną wersję:

- Podczas okresu próbnego korzystania z funkcji. Czas trwania okresu próbnego różni się w zależności od regionu. Informacje na ten temat można uzyskać u przedstawiciela firmy Trend Micro.
- Po wygaśnięciu licencji i upływie okresu próbnego. W tym okresie nie ma możliwości korzystania z pomocy technicznej.

Jeśli użytkownik dysponuje licencją na wersję próbną

- Po wygaśnięciu licencji. W tym okresie nie ma możliwości korzystania z pomocy technicznej.

4. Kliknij opcję **Zobacz szczegóły dotyczące licencji w trybie online**, aby wyświetlić informacje o licencji w witrynie internetowej firmy Trend Micro.
5. Aby zaktualizować zawartość ekranu na podstawie najnowszych informacji o licencji, kliknij opcję **Aktualizuj informacje**.

Połączenia z serwerem wirtualnym

Dodając połączenia z VMware vCenter 4 (VMware View 4), Citrix XenServer 5.5 (Citrix XenDesktop 4) lub Microsoft Hyper-V Server, można zoptymalizować zadania

skanowania na żądanie lub aktualizacji składników. Serwery OfficeScan komunikują się z określonymi serwerami wirtualnymi, aby ustalić, którzy Agenci OfficeScan znajdują się na tym samym serwerze fizycznym.

W przypadku innych serwerów VDI serwer OfficeScan udostępnia funkcję emulowanego hypervisora wirtualnego, aby zarządzać agentami wirtualnymi na innych platformach. Hypervisor programu OfficeScan przetwarza żądania agentów wirtualnych w kolejności, w jakiej zostały odebrane przez serwer. Serwer OfficeScan przetwarza jedno żądanie jednocześnie i umieszcza inne żądania w kolejce.

Dodawanie połączeń z serwerem

Procedura

1. Otwórz konsolę Web programu OfficeScan i kliknij polecenie **Dodatki** > **Zarządzaj programem [Trend Micro Virtual Desktop Support]** w menu głównym.
2. Wybierz opcję **VMware vCenter Server**, **Citrix XenServer**, **Microsoft Hyper-V** lub **Inne aplikacje do wirtualizacji**.

   Uwaga

   W przypadku wybrania opcji **Inne aplikacje do wirtualizacji** dalsze informacje nie są wymagane. Serwer OfficeScan odpowiada na żądania agentów w kolejności, w jakiej zostały odebrane przez serwer.

3. Uruchom połączenie z serwerem.
4. Określ następujące informacje:
   - W przypadku serwerów VMware vCenter i Citrix XenServer:
     - Adres IP
     - Port
     - Protokół połączenia (HTTP lub HTTPS)
     - Nazwa użytkownika

- Hasło

- W przypadku serwerów Microsoft Hyper-V:
  - nazwa hosta lub adres IP,
  - Domena\nazwa_użytkownika

  Uwaga

  Konto logowania musi być kontem w domenie należącym do grupy Administratorzy

  - Hasło

5. Opcjonalnie włącz połączenie z serwerem VMware vCenter lub Citrix XenServer przez serwer proxy.
   a. Podaj nazwę serwera proxy lub jego adres IP i numer portu.
   b. Jeżeli serwer proxy wymaga uwierzytelniania, wpisz nazwę użytkownika i hasło.
6. Kliknij **Sprawdź połączenie**, aby sprawdzić, czy serwer OfficeScan może połączyć się z serwerem.

   Uwaga

   Szczegółowe informacje dotyczące rozwiązywania problemów z połączeniami z serwerem Microsoft Hyper-V znajdują się w części *Rozwiązywanie problemów z połączeniami z Microsoft Hyper-V na stronie 15-89*.
7. Kliknij przycisk **Zapisz**.

Dodawanie dodatkowych połączeń z serwerem

Procedura

1. Otwórz konsolę Web programu OfficeScan i kliknij polecenie **Dodatki** > **Zarządzaj programem [Trend Micro Virtual Desktop Support]** w menu głównym.
2. Kliknij polecenie **Dodaj nowe połączenie z serwerem vCenter**, **Dodaj nowe połączenie z serwerem XenServer** lub **Dodaj nowe połączenie z serwerem Hyper-V**.
3. Powtórz powyższe kroki, podając prawidłowe informacje o serwerze.
4. Kliknij przycisk **Zapisz**.

Usuwanie ustawień połączenia

Procedura

1. Otwórz konsolę Web programu OfficeScan i przejdź do opcji **Dodatki** > **Zarządzaj programem [Trend Micro Virtual Desktop Support]** w menu głównym.
2. Kliknij **Usuń to połączenie**.
3. Kliknij przycisk **Ok**, aby potwierdzić usunięcie tego ustawienia.
4. Kliknij przycisk **Zapisz**.

Zmiana pojemności skanowania VDI

Administratorzy mogą zwiększyć liczbę punktów końcowych VDI, które wykonują jednocześnie skanowanie, modyfikując plik `vdi.ini`. Firma Trend Micro zaleca dokładne monitorowanie wpływu zmiany pojemności VDI, aby upewnić się, że zasoby systemowe mogą obsłużyć zwiększony poziom skanowania.

Procedura

1. Na komputerze serwera OfficeScan przejdź do lokalizacji <*Folder instalacji serwera*>`PCCSRV\Private\vdi.ini`.

2. Znajdź ustawienia `[TaskController]`.

   Domyślne ustawienia TaskController są następujące:

   - Klienty OfficeScan 10.5:

     ```
     [TaskController]

     Controller_00_MaxConcurrentGuests=1

     Controller_01_MaxConcurrentGuests=3
     ```

     Gdzie:

     - `Controller_00_MaxConcurrentGuests=1` oznacza maksymalną liczbę klientów, które mogą jednocześnie wykonywać skanowanie.
     - `Controller_01_MaxConcurrentGuests=3` oznacza maksymalną liczbę klientów, które mogą jednocześnie wykonywać aktualizacje.

   - W przypadku klientów OfficeScan 10.6 i OfficeScan 11.0 (lub nowszych) agenci:

     ```
     [TaskController]

     Controller_02_MaxConcurrentGuests=1

     Controller_03_MaxConcurrentGuests=3
     ```

     Gdzie:

     - `Controller_02_MaxConcurrentGuests=1` oznacza maksymalną liczbę klientów, które mogą jednocześnie wykonywać skanowanie.
     - `Controller_03_MaxConcurrentGuests=3` oznacza maksymalną liczbę klientów, które mogą jednocześnie wykonywać aktualizacje.

3. Zwiększ lub zmniejsz odpowiednio liczbę dla każdego kontrolera.

   Minimalna wartość dla wszystkich ustawień to 1.

Maksymalna wartość dla wszystkich ustawień to 65536.

4. Zapisz i zamknij plik `vdi.ini`.

5. Ponownie uruchom OfficeScan Master Service.

6. Monitoruj wykorzystanie procesora, pamięci i dysku przez punkty końcowe VDI. Powtarzając kroki od 1 do 5, zmodyfikuj ponownie ustawienia kontrolera, aby odpowiednio zwiększyć lub zmniejszyć liczbę jednoczesnych operacji skanowania dla danego środowiska VDI.

Rozwiązywanie problemów z połączeniami z Microsoft Hyper-V

Połączenie Microsoft Hyper-V do komunikacji między serwerem a agentem używa usług WMI (Windows Management Instrumentation) oraz DCOM. Połączenie z serwerem Hyper-V może być blokowane przez wytyczne dla zapory sieciowej.

Serwer Hyper-V prowadzi nasłuch na porcie 135, a następnie do dalszej komunikacji otwiera losowo wybrany port. Gdy zapora blokuje transmisję WMI lub jeden z tych dwóch portów, komunikacja z serwerem nie powiedzie się. Administratorzy mogą zmodyfikować wytyczne dla zapory sieciowej tak, aby umożliwić komunikację z serwerem Hyper-V.

Przed modyfikacją ustawień zapory sprawdź wszystkie ustawienia połączenia, w tym adres IP, domenę\nazwęużytkownika i hasło.

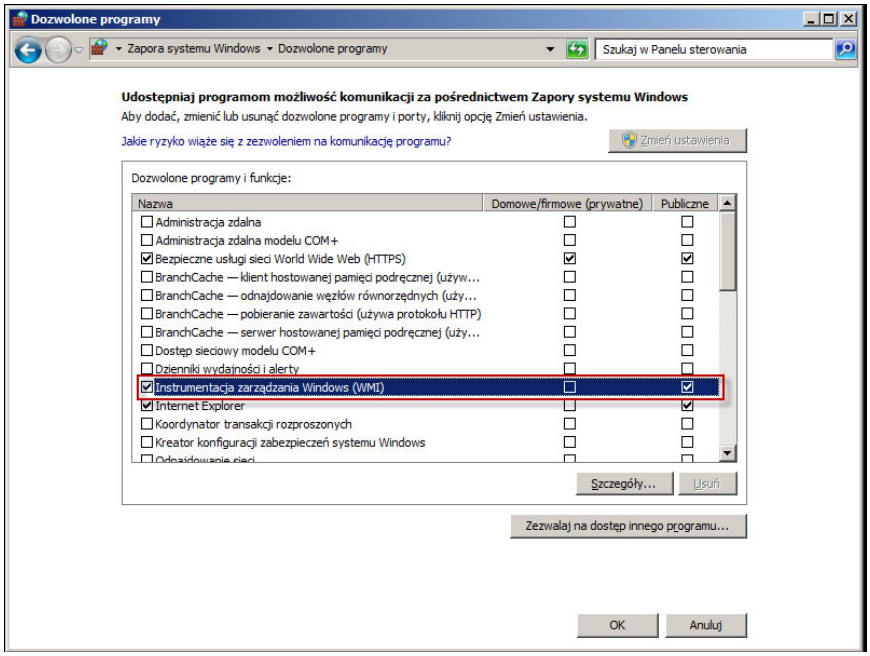
Przepuszczanie transmisji WMI przez zaporę Windows

Procedura

1. Na serwerze Hyper-V otwórz ekran **Programy dozwolone przez zaporę Windows**.

   W systemach Windows 2008 R2 kliknij polecenie **Panel sterowania** > **System i zabezpieczenia** > **Zapora Windows** > **Pozwól programowi przejść przez zaporę Windows**.

2. Wybierz opcję **Windows Management Instrumentation (WMI)**.



ILUSTRACJA 15-7. Ekran Programy dozwolone przez zaporę Windows

3. Kliknij przycisk **Zapisz**.

4. Sprawdź ponownie połączenie Hyper-V.

Otwieranie portu w zaporze Windows lub zewnętrznego producenta

Procedura

1. Na serwerze Hyper-V sprawdź, czy zapora pozwala na komunikację przez port 135 i sprawdź ponownie połączenie Hyper-V.

Szczegółowe informacje dotyczące otwierania portów znajdują się w dokumentacji zapory.

2. Jeśli połączenie z serwerem Hyper-V nie powiedzie się, skonfiguruj usługę WMI tak, aby używała zawsze tego samego portu.

   Szczegóły na temat *ustawiania stałego portu w usłudze WMI* znajdują się w dokumencie:

   http://msdn.microsoft.com/en-us/library/windows/desktop/bb219447(v=vs.85).aspx

3. Otwórz w zaporze porty 135 oraz nowy stały port (24158).

4. Sprawdź ponownie połączenie Hyper-V.

Narzędzie tworzenia szablonu skanowania wstępnego VDI

Aby zoptymalizować skanowanie na żądanie lub usunąć identyfikatory GUID z obrazów base lub golden, należy użyć narzędzia tworzenia szablonów OfficeScan VDI Pre-Scan Template Generation Tool. Narzędzie przeprowadza skanowanie obrazów base lub golden i je certyfikuje. Podczas skanowania duplikatów obrazów, program OfficeScan sprawdza jedynie części, które uległy zmianie. Dzięki temu czas skanowania jest krótszy.

Porada

Firma Trend Micro zaleca tworzenie szablonów skanowania wstępnego po dokonaniu aktualizacji systemu Windows lub po instalacji nowego oprogramowania.

Tworzenie szablonu skanowania wstępnego

Procedura

1. Na komputerze serwera OfficeScan przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\TCacheGen`.

2. Wybierz wersję narzędzia tworzenia szablonów VDI Pre-Scan Template Generation Tool. Dostępne są następujące wersje:

TABELA 15-10. Wersje narzędzia tworzenia szablonów VDI Pre-Scan Template Generation Tool

NAZWA PLIKU	INSTRUKCJA
TCacheGen.exe	Wybierz ten plik, aby uruchomić narzędzie bezpośrednio na platformie 32-bitowej.
TCacheGen_x64.exe	Wybierz ten plik, aby uruchomić narzędzie bezpośrednio na platformie 64-bitowej.
TCacheGenCli.exe	Wybierz ten plik, aby uruchomić to narzędzie z poziomu wiersza poleceń na platformie 32-bitowej.
TCacheGenCli_x64.exe	Wybierz ten plik, aby uruchomić to narzędzie z poziomu wiersza poleceń na platformie 64-bitowej.

3. Skopiuj wersję narzędzia wybraną w poprzednim kroku na punkt końcowy.
4. Uruchom narzędzie.
   - Aby uruchomić narzędzie bezpośrednio:
     a. Kliknij dwukrotnie plik `TCacheGen.exe` lub `TCacheGen_x64.exe`.
     b. Wybierz pozycję **Utwórz szablon skanowania wstępnego** i kliknij przycisk **Dalej**.
   - Aby uruchomić to narzędzie z poziomu wiersza poleceń:
     a. Otwórz wiersz polecenia i przejdź do lokalizacji `<Folder instalacji agenta>`.
     b. Wpisz następujące polecenie:

        ```
        TCacheGenCli Generate_Template
        ```

        Lub

        ```
        TcacheGenCli_x64 Generate_Template
        ```

Uwaga

Przed utworzeniem szablonu skanowania wstępnego i usunięciem identyfikatora GUID narzędzie wykona skanowanie obrazu pod kątem obecności zagrożeń bezpieczeństwa.

Po utworzeniu szablonu skanowania wstępnego narzędzie zamknie agenta OfficeScan. Nie należy ponownie ładować agenta OfficeScan. Jeżeli Agent OfficeScan zostanie załadowany ponownie, należy jeszcze raz utworzyć szablon skanowania wstępnego.

Usuwanie identyfikatorów GUID z szablonów

Procedura

1. Na komputerze serwera OfficeScan przejdź do lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\TCacheGen`.

2. Wybierz wersję narzędzia tworzenia szablonów VDI Pre-Scan Template Generation Tool. Dostępne są następujące wersje:

   TABELA 15-11. Wersje narzędzia tworzenia szablonów VDI Pre-Scan Template Generation Tool

NAZWA PLIKU	INSTRUKCJA
TCacheGen.exe	Wybierz ten plik, aby uruchomić narzędzie bezpośrednio na platformie 32-bitowej.
TCacheGen_x64.exe	Wybierz ten plik, aby uruchomić narzędzie bezpośrednio na platformie 64-bitowej.
TCacheGenCli.exe	Wybierz ten plik, aby uruchomić to narzędzie z poziomu wiersza poleceń na platformie 32-bitowej.
TCacheGenCli_x64.exe	Wybierz ten plik, aby uruchomić to narzędzie z poziomu wiersza poleceń na platformie 64-bitowej.

3. Skopiuj wersję narzędzia wybraną w poprzednim kroku na punkt końcowy.

4. Uruchom narzędzie.

   - Aby uruchomić narzędzie bezpośrednio:

a. Kliknij dwukrotnie plik `TCacheGen.exe` lub `TCacheGen_x64.exe`.

b. Wybierz pozycję **Usuń GUID z szablonu** i kliknij przycisk **Dalej**.

- Aby uruchomić to narzędzie z poziomu wiersza poleceń:

a. Otwórz wiersz polecenia i przejdź do lokalizacji `<Folder instalacji agenta>`.

b. Wpisz następujące polecenie:

```
TCacheGenCli Remove GUID
```

Lub

```
TcacheGenCli_x64 Remove GUID
```

Ustawienia agenta globalnego

Program OfficeScan stosuje globalne ustawienia agentów do wszystkich agentów lub tylko agentów o określonych uprawnieniach.

Procedura

1. Przejdź do opcji **Agenci** > **Ustawienia agenta globalnego**.
2. Skonfiguruj następujące ustawienia:

TABELA 15-12. Ustawienia agenta globalnego

KARTA	USTAWIENIE	REFERENCJE
Ustawienia zabezpieczeń	Ustawienia skanowania	*Sekcja ustawień skanowania na stronie 7-81*
	Ustawienia skanowania zaplanowanego	*Sekcja ustawień skanowania zaplanowanego na stronie 7-87*
	Ustawienia zapory	*Globalne ustawienia zapory na stronie 13-26*
	Ustawienia podejrzanego połączenia	*Konfigurowanie globalnych, zdefiniowanych przez użytkownika list adresów IP na stronie 8-6*
	Ustawienia monitorowania zachowań	*Konfigurowanie globalnych ustawień monitorowania zachowań na stronie 9-14*
System	Ustawienia usługi Certified Safe Software Service	*Konfigurowanie globalnych ustawień skanowania na stronie 7-79*
	Usługa proxy Smart Protection	*Konfigurowanie ustawień serwera proxy usługi Global Smart Protection na stronie 15-54*
	Aktualizacje	• *Serwer ActiveUpdate jako źródło aktualizacji agentów OfficeScan na stronie 6-39* • *Konfigurowanie zarezerwowanego miejsca na dysku na potrzeby aktualizacji agentów OfficeScan na stronie 6-51*
	Ponowne uruchamianie usług	*Ponowne uruchomienie usługi Agent OfficeScan Service na stronie 15-12*

KARTA	USTAWIENIE	REFERENCJE
Sieć	Konfiguracja proxy	*Automatyczne ustawienia proxy dla agenta OfficeScan na stronie 15-57*
	Preferowany adres IP	*Adresy IP agentów na stronie 5-11*
	Komunikacja serwer-agent	*Rozszerzone szyfrowanie komunikacji serwer-agent na stronie 14-61*
	Ustawienia przepustowości dziennika wirusów / złośliwego oprogramowania	*Konfigurowanie globalnych ustawień skanowania na stronie 7-79*
	Sieć nieosiągalna	*Nieosiągalni agenci na stronie 15-48*
Kontrola agentów	Ustawienia ogólne	*Konfigurowanie globalnych ustawień skanowania na stronie 7-79*
	Ustawienia ostrzeżeń	*Konfigurowanie powiadomień dotyczących aktualizacji agenta OfficeScan na stronie 6-53*
	Konfiguracja języka agenta	*Konfiguracja języka agenta OfficeScan na stronie 15-22*

3. Kliknij przycisk **Zapisz**.

Konfigurowanie uprawnień agenta i innych ustawień

Użytkownikom można nadać uprawnienia do modyfikacji pewnych ustawień i do wykonywania zadań na wysokim poziomie na agencie OfficeScan.

Uwaga

Ustawienia antywirusowe są dostępne tylko po aktywacji funkcji antywirusowej programu OfficeScan,

Porada

Aby zachować jednolite uprawnienia i reguły w całej organizacji, użytkownikom należy nadawać ograniczone uprawnienia.

Procedura

1. Przejdź do opcji **Agenci** > **Zarządzanie agentami**.
2. W drzewie agentów kliknij ikonę domeny głównej (), aby dołączyć wszystkich agentów, lub wybierz określone domeny lub agentów.
3. Kliknij polecenie **Ustawienia** > **Uprawnienia i inne ustawienia**.
4. Na karcie **Uprawnienia** skonfiguruj następujące uprawnienia użytkownika:

TABELA 15-13. Uprawnienia agenta

UPRAWNIENIA AGENTA	REFERENCJE
Uprawnienie trybu niezależnego	*Uprawnienie trybu niezależnego Agent OfficeScan na stronie 15-19*
Uprawnienia skanowania	*Uprawnienia typu skanowania na stronie 7-62*
Uprawnienia do skanowania zaplanowanego	*Uprawnienia do skanowania zaplanowanego i inne ustawienia na stronie 7-65*
Uprawnienia do zapory	*Uprawnienia do zapory na stronie 13-24*
Uprawnienia monitorowania zachowań	*Uprawnienia monitorowania zachowań na stronie 9-16*
Lista zaufanych programów	*Uprawnienie do listy zaufanych programów na stronie 7-78*
Uprawnienia do skanowania poczty	*Uprawnienia do skanowania poczty i inne ustawienia na stronie 7-71*
Uprawnienia do ustawień proxy	*Uprawnienia do konfiguracji proxy dla agentów na stronie 15-55*
Uprawnienia do aktualizacji składników	*Konfigurowanie uprawnień aktualizacji i innych ustawień na stronie 6-48*

Uprawnienia agenta	Referencje
Zamykanie i odblokowywanie	*Przyznawanie uprawnienia do zamykania i odblokowywania agenta na stronie 15-19*
Dezinstalacja	*Przyznawanie uprawnienia do odinstalowywania agenta OfficeScan na stronie 5-81*

5. Kliknij kartę **Inne ustawienia** i skonfiguruj następujące ustawienia:

Tabela 15-14. Inne ustawienia agenta

Ustawienie	Referencje
Ustawienia aktualizacji	*Konfigurowanie uprawnień aktualizacji i innych ustawień na stronie 6-48*
Ustawienia usługi Web Reputation	*Powiadamianie użytkowników Agenta o zagrożeniach internetowych na stronie 12-14*
Ustawienia monitorowania zachowań	*Uprawnienia monitorowania zachowań na stronie 9-16*
Ustawienia ostrzegania kontaktu C&C	*Powiadomienia ostrzegania kontaktu C&C dla użytkowników agenta na stronie 12-19*
Ustawienia ostrzeżeń centralnego przywracania kwarantanny	Wyświetla powiadomienie programu na punkcie końcowym po przywróceniu pliku poddanego kwarantannie
Ustawienia przewidującego uczenia maszynowego	Wyświetla powiadomienie programu na punkcie końcowym po wykryciu nieznanego zagrożenia
Własna ochrona agenta OfficeScan	*Własna ochrona agenta OfficeScan na stronie 15-13*
Ustawienia skanowania zaplanowanego	*Przyznawanie uprawnienia do skanowania zaplanowanego i wyświetlanie powiadomienia na stronie 7-66*
Ustawienia pamięci podręcznej skanowania	*Ustawienia pamięci podręcznej skanowania na stronie 7-73*

USTAWIENIE	REFERENCJE
Ustawienia skanowania poczty POP3	*Przyznawanie uprawnienia do skanowania poczty i włączanie skanowanie poczty POP3 na stronie 7-73*
Ograniczenie dostępu do agenta OfficeScan	*Ograniczenie dostępu do konsoli agenta OfficeScan na stronie 15-17*
Powiadomienie o ponownym uruchomieniu	*Powiadamianie użytkowników agenta OfficeScan o zagrożeniach bezpieczeństwa na stronie 7-97*

6. Jeśli w drzewie agentów wybrano domeny lub agentów, kliknij przycisk **Zapisz**. Jeśli kliknięto ikonę domeny głównej, należy wybrać spośród następujących opcji:

   - **Zastosuj dla wszystkich agentów**: Stosuje ustawienia dla wszystkich istniejących agentów oraz dla wszystkich nowych agentów dodanych do istniejącej/przyszłej domeny. Przyszłe domeny są to takie domeny, które w momencie konfiguracji ustawień nie zostały jeszcze utworzone.
   - **Zastosuj tylko do przyszłych domen**: Stosuje ustawienia tylko dla agentów dodanych do przyszłych domen. Opcja ta nie będzie stosować ustawień dla nowych agentów dodanych do istniejącej domeny.

Część IV

Zapewnienie dodatkowej ochrony

Rozdział 16

Ochrona agentów zdalnych

W tym rozdziale przedstawiono instalację Serwer Przekaźnika Krawędziowego i kroki konfiguracji wymagane do zapewnienia ochrony Agenci OfficeScan opuszczających firmowy intranet.

Rozdział składa się z następujących tematów:

Serwer Przekaźnika Krawędziowego

Program Serwer Przekaźnika Krawędziowego OfficeScan zapewnia administratorom widoczność i lepszą ochronę punktów końcowych, które użytkownicy zabierają poza firmowy intranet. Po zainstalowaniu Serwer Przekaźnika Krawędziowego w strefie zdemilitaryzowanej (DMZ), Agenci OfficeScan zdalni, którzy nie mogą nawiązać funkcjonalnego połączenia z serwerem OfficeScan, nadal będą mogli wykonywać zadania przedstawione w poniższej tabeli.

Ważne

Serwer Przekaźnika Krawędziowego nie obsługuje komunikacji z wykorzystaniem protokołu IPv6.

ZADANIE	OPIS
Synchronizacja listy podejrzanych obiektów	Serwer Przekaźnika Krawędziowego otrzymuje zaktualizowane listy podejrzanych obiektów z serwera OfficeScan zgodnie ze skonfigurowanym harmonogramem i rozsyła je do agentów zdalnych. Aby uzyskać więcej informacji, patrz *Ustawienia listy podejrzanych obiektów na stronie 14-33*.
Przesyłanie próbek	Agenci zdalni, którzy wykryją nieznane zagrożenie, mogą wysłać podejrzany obiekt do skonfigurowanej usługi Virtual Analyzer. Zgłaszanie podejrzanych obiektów przez agentów zdalnych do usługi Virtual Analyzer odbywa się w następujący sposób: 1. Agenci zdalni wysyłają obiekt do Serwer Przekaźnika Krawędziowego. 2. Serwer Przekaźnika Krawędziowego przekazuje obiekt do serwera OfficeScan podczas następnej skonfigurowanej synchronizacji. 3. Serwer OfficeScan przekazuje następnie obiekt do usługi Virtual Analyzer w celu przeprowadzenia analizy. Aby uzyskać więcej informacji, patrz *Przesyłanie próbek na stronie 8-10*.

Zadanie	Opis
Przesyłanie dzienników	Serwer Przekaźnika Krawędziowego zbiera dzienniki agentów zdalnych i okresowo wysyła dane dzienników do serwera OfficeScan zgodnie ze skonfigurowanym harmonogramem.
Raport stanu	Agenci zdalni wysyłają do Serwer Przekaźnika Krawędziowego aktualizacje stanu, takie jak aktualna sygnatura i wersje składników.

Po skonfigurowaniu Serwer Przekaźnika Krawędziowego Agenci OfficeScan odbierają ustawienia i automatycznie wysyłają raporty do Serwer Przekaźnika Krawędziowego, kiedy połączenie z serwerem OfficeScan jest niedostępne.

Komunikacja między programem Serwer Przekaźnika Krawędziowego, serwerem OfficeScan i Agenci OfficeScan jest szyfrowana przy użyciu uwierzytelniania certyfikatem.

Aby uzyskać więcej informacji, patrz *Zarządzanie certyfikatami Serwer Przekaźnika Krawędziowego na stronie 16-17*.

Wymagania systemowe Serwer Przekaźnika Krawędziowego

Przed zainstalowaniem Serwer Przekaźnika Krawędziowego upewnij się, że docelowy komputer serwera spełnia minimalne wymagania systemowe.

Zasób	Wymagania
Procesor	Dwurdzeniowy 2 GHz
Pamięć	4 GB
Miejsce na dysku	50 GB
System operacyjny	Windows Server 2012 R2

Zasób	Wymagania

Karta sieciowa	• 2 karty sieciowe
	  • Jedna dla połączenia intranetowego z serwerem OfficeScan
	  • Jedna dla połączenia zewnętrznego z Agenci OfficeScan zdalnymi
	• 1 karta sieciowa skonfigurowana w celu użycia innych portów dla połączeń intranetowych i internetowych

Baza danych	• SQL Server™ 2008 R2 Express (lub nowsza) • SQL Server™ 2008 R2 (lub nowsza) **Uwaga** Podczas instalacji program instalacyjny Serwer Przekaźnika Krawędziowego OfficeScan zapewnia opcję instalacji programu SQL Server 2014 SP2 Express.

Instalacja Serwer Przekaźnika Krawędziowego

Przed zainstalowaniem Serwer Przekaźnika Krawędziowego upewnij się, że docelowy komputer serwera spełnia minimalne wymagania systemowe.

Aby uzyskać więcej informacji, patrz *Wymagania systemowe Serwer Przekaźnika Krawędziowego na stronie 16-3*.

Ważne

Serwer Przekaźnika Krawędziowego nie obsługuje komunikacji z wykorzystaniem protokołu IPv6.

Procedura

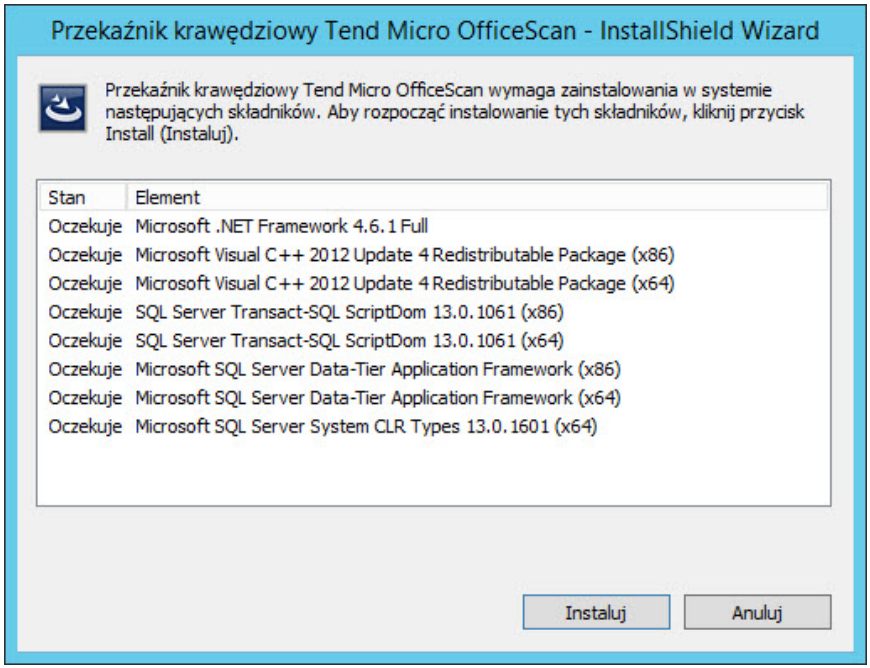
1. Znajdź folder <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\EdgeServer` na komputerze serwera OfficeScan i skopiuj ten folder na komputer docelowego serwera Serwer Przekaźnika Krawędziowego.

2. Na docelowym serwerze Przekaźnika Krawędziowego otwórz folder `EdgeServer` i uruchom plik `setup.exe`, aby rozpocząć proces instalacji.

   Pakiet instalacyjny sprawdzi wymagane składniki na serwerze.

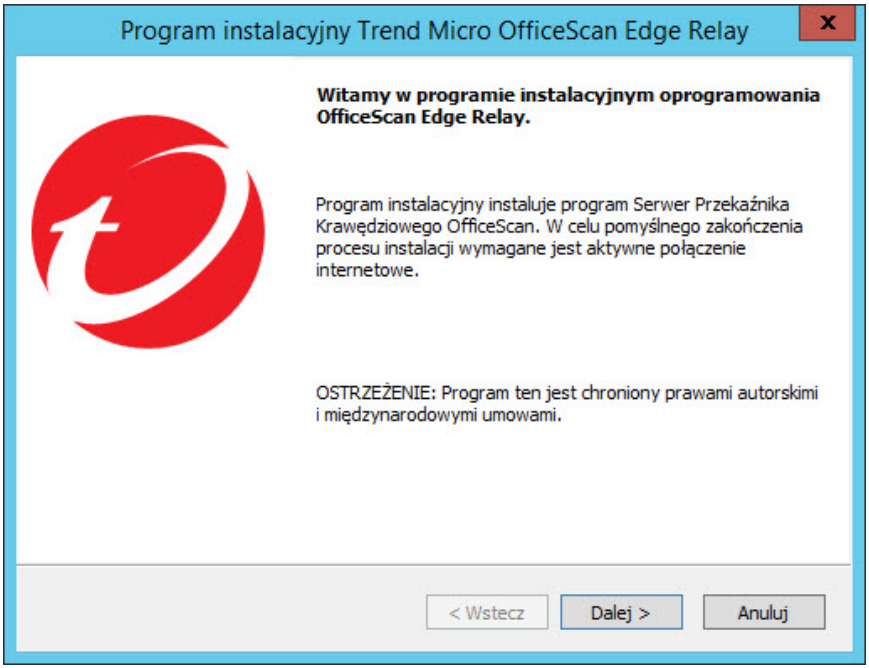
3. Jeśli dowolne z poniższych składników nie istnieją na serwerze, kliknij przycisk **Instaluj**, aby umożliwić programowi instalacyjnemu zainstalowanie brakujących składników podczas procesu instalacji Serwer Przekaźnika Krawędziowego.

   - Microsoft .NET Framework 4.5 Full
   - Microsoft Visual C++ 2012 Update 4 Redistributable Package (x64)
   - Microsoft SQL Server System CLR Types 10.00.2531 (x64)
   - SQL Server Transact-SQL ScriptDom (x64)
   - Microsoft SQL Server Data-Tier Application Framework (x64)



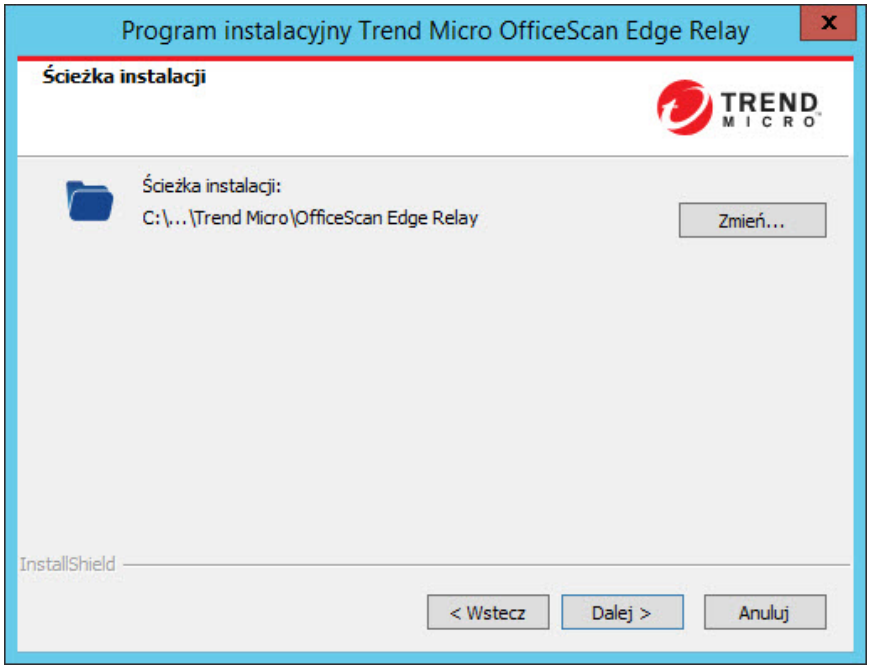
Zostanie wyświetlony ekran powitalny.

4. Kliknij przycisk **Dalej**.



Zostanie wyświetlony ekran **Ścieżka instalacji**.

5. Zaakceptuj domyślny katalog instalacyjny lub kliknij przycisk **Zmień**, aby wybrać inną lokalizację.



6. Kliknij przycisk **Dalej>**.

   Zostanie wyświetlony ekran **Serwer Przekaźnika Krawędziowego — połączenie agenta OfficeScan**.

7. Określ następujące ustawienia, których Agenci OfficeScan zdalni będą używać w celu nawiązania połączenia z programem Serwer Przekaźnika Krawędziowego:

   - **W pełni kwalifikowana nazwa domeny (FQDN)**: Wpisz nazwę FQDN serwera Serwer Przekaźnika Krawędziowego
   - **Adres IP**: Wybierz format adresu IP

   Ważne

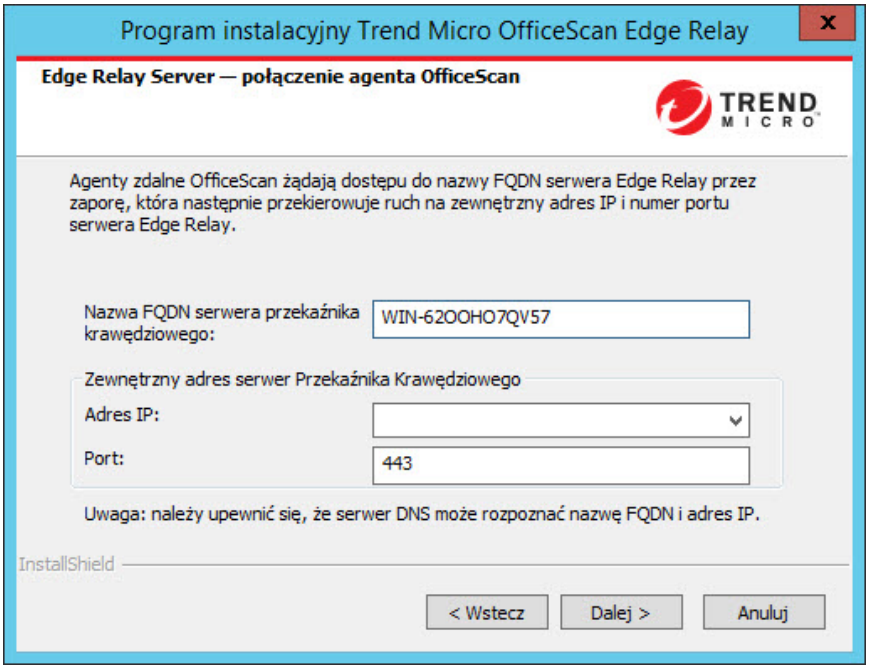
   Serwer Przekaźnika Krawędziowego nie obsługuje komunikacji z wykorzystaniem protokołu IPv6.

- **Port**: Zaakceptuj domyślny port lub określ nowy

Ważne

Należy skonfigurować zaporę i bramę, aby umożliwić:

- Przekierowanie komunikacji agentów OfficeScan z Internetu do serwera Serwer Przekaźnika Krawędziowego
- Komunikację poprzez określony port



8. Kliknij przycisk **Dalej>**.

   Zostanie wyświetlony ekran programu **Serwer Przekaźnika Krawędziowego — połączenie serwera OfficeScan**.

9. Określ następujące ustawienia, których serwer OfficeScan będzie używać w celu nawiązania połączenia z programem Serwer Przekaźnika Krawędziowego:

- **Adres IP**: Wybierz format adresu IP

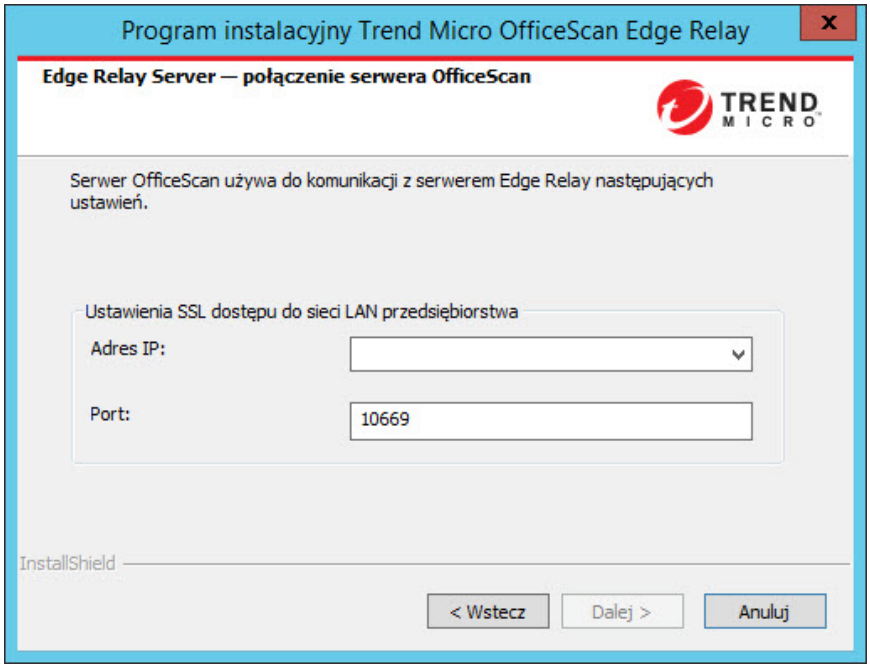
Ważne

Serwer Przekaźnika Krawędziowego nie obsługuje komunikacji z wykorzystaniem protokołu IPv6.

- **Port**: Zaakceptuj domyślny port lub określ nowy

Ważne

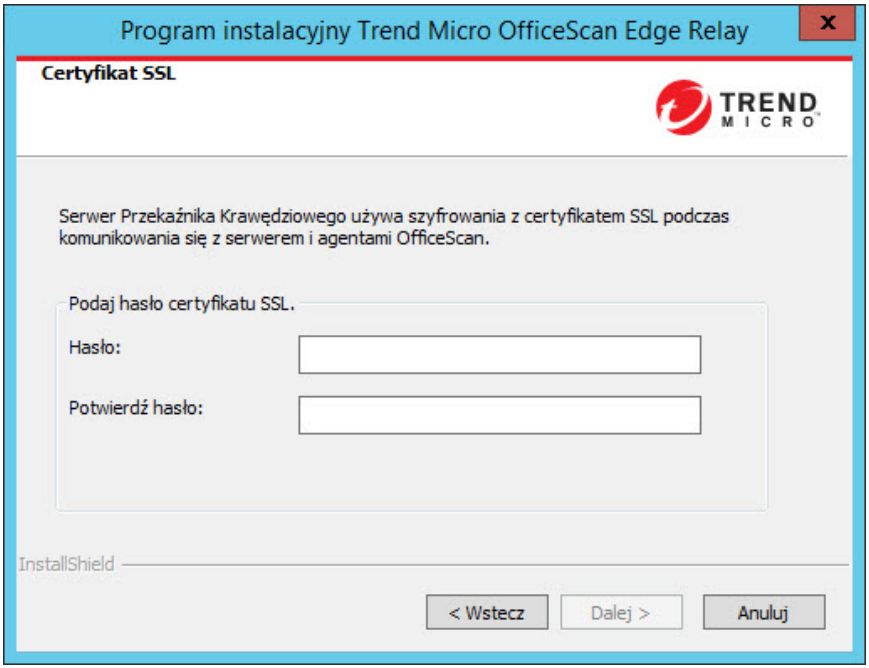
- Port serwera OfficeScan musi się różnić od portu skonfigurowanego dla Agenci OfficeScan zdalnych.
- Upewnij się, że zapora pozwala na komunikację przez określony port.



10. Kliknij przycisk **Dalej>**.

Zostanie wyświetlony ekran **Certyfikat SSL**.

11. Określ i potwierdź hasło używane dla certyfikatu Serwer Przekaźnika Krawędziowego.

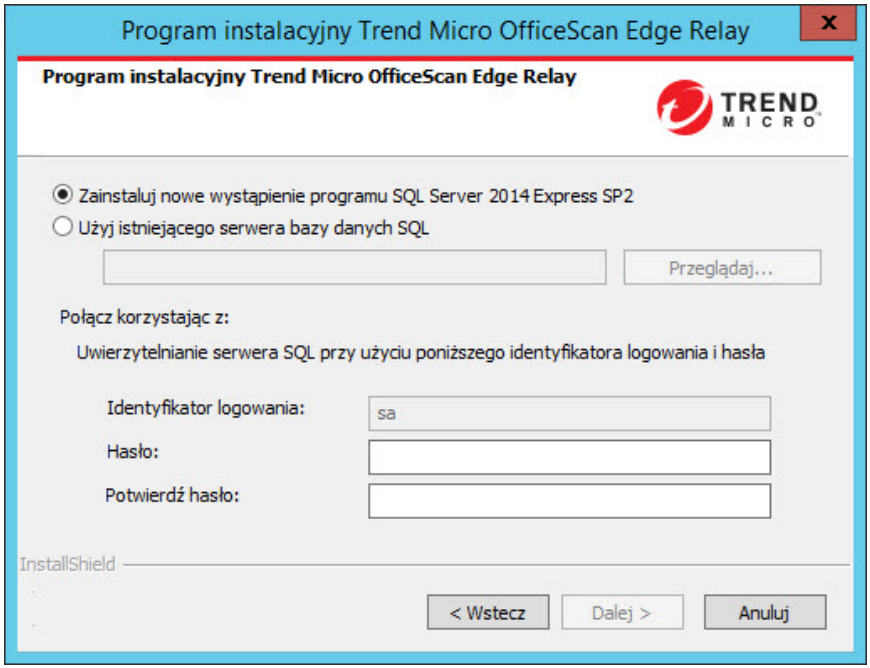


12. Kliknij przycisk **Dalej>**.

Zostanie wyświetlony ekran **Serwer bazy danych**.

13. Określ bazę danych SQL Server, która będzie używana przez Serwer Przekaźnika Krawędziowego:

- **Zainstaluj nowe wystąpienie SQL Server 2008 R2 SP2 Express**
- **Użyj istniejącego serwera bazy danych SQL**: Kliknij przycisk **Przeglądaj** w celu wybrania dostępnego serwera z listy.

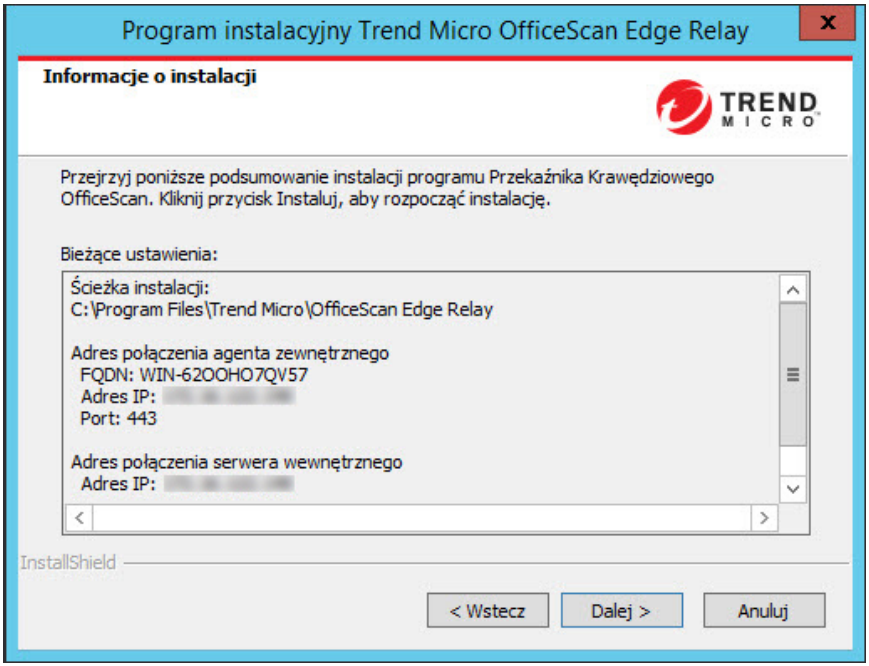


14. Określ hasło służące do połączenia z bazą danych SQL Server. Jeśli instalujesz nową bazę danych SQL Server Express, potwierdź hasło.

15. Kliknij przycisk **Dalej>**.

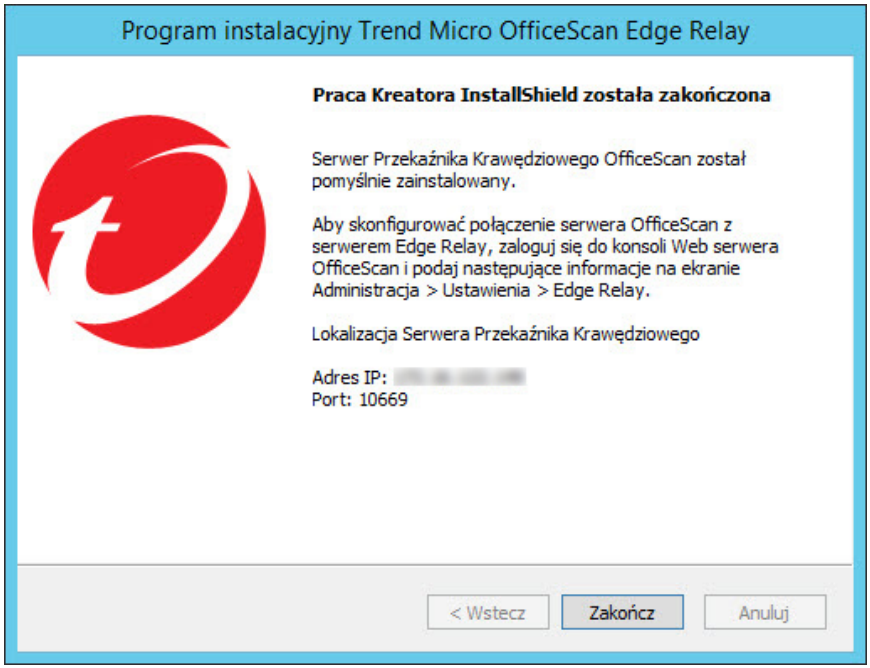
    Zostanie wyświetlony ekran **Informacje o instalacji**.

16. Kliknij przycisk **Dalej >**, aby rozpocząć instalację.



Po zakończeniu instalacji zostanie wyświetlony ekran **Praca Kreatora InstallShield została ukończona**.

17. Kliknij przycisk **Zakończ**.



Serwer Przekaźnika Krawędziowego jest gotowy do użycia. Możesz skonfigurować serwer OfficeScan w celu połączenia z programem Serwer Przekaźnika Krawędziowego.

Aby uzyskać więcej informacji, patrz *Łączenie z serwerem Przekaźnika Krawędziowego na stronie 16-14*.

Łączenie z serwerem Przekaźnika Krawędziowego

Po zainstalowaniu Serwer Przekaźnika Krawędziowego należy skonfigurować jego ustawienia połączenia na serwerze OfficeScan. Po nawiązaniu połączenia z serwerem Przekaźnika Krawędziowego, Agenci OfficeScan podlegający serwerowi OfficeScan

otrzymają ustawienia połączenia i zyskają możliwość automatycznej komunikacji z programem Serwer Przekaźnika Krawędziowego po opuszczeniu firmowego intranetu.

Procedura

1. W konsol Web OfficeScan wybierz kolejno pozycje **Administracja** > **Ustawienia** > **Przekaźnik Krawędziowy**.

   Zostanie wyświetlony ekran **Ustawienia serwera Przekaźnika Krawędziowego**.

2. Wpisz **adres IP** i **port** serwera Serwer Przekaźnika Krawędziowego.

   Uwaga

   Upewnij się, że podajesz adres IP i port skonfigurowane dla komunikacji intranetowej z serwerem Przekaźnika Krawędziowego.

3. Jeśli dane środowisko wymaga serwera proxy do komunikacji z programem Serwer Przekaźnika Krawędziowego w strefie zdemilitaryzowanej, włącz opcję **Połącz przy użyciu ustawień zewnętrznego serwera proxy**.

   Aby skonfigurować ustawienia zewnętrznego serwera proxy, kliknij **ustawienia zewnętrznego serwera proxy** w celu przekierowania na ekran **Ustawienia serwera proxy**. Skonfiguruj wymagane informacje o serwerze proxy w sekcji **Aktualizacje serwera OfficeScan**.

   Aby uzyskać więcej informacji, patrz *Konfigurowanie ustawień proxy na stronie 6-21*.

4. Kliknij przycisk **Połącz**.

   Po pomyślnym nawiązaniu połączenia z serwerem Przekaźnika Krawędziowego ekran zostanie odświeżony i pojawią się informacje o połączeniu.

   Aby uzyskać więcej informacji, patrz *Zarządzanie połączeniem serwera Serwer Przekaźnika Krawędziowego na stronie 16-16*.

Zarządzanie połączeniem serwera Serwer Przekaźnika Krawędziowego

Po nawiązaniu połączenia z serwerem Przekaźnika Krawędziowego, Agenci OfficeScan podlegający serwerowi OfficeScan otrzymają ustawienia połączenia i zyskają możliwość automatycznej komunikacji z programem Serwer Przekaźnika Krawędziowego po opuszczeniu firmowego intranetu. Następnie można monitorować stan połączenia serwera Serwer Przekaźnika Krawędziowego, konfigurować harmonogram synchronizacji i wykonywać natychmiast synchronizację na ekranie **Ustawienia Serwer Przekaźnika Krawędziowego**.

Procedura

1. W konsol Web OfficeScan wybierz kolejno pozycje **Administracja** > **Ustawienia** > **Przekaźnik Krawędziowy**.

   Zostanie wyświetlony ekran **Ustawienia serwera Przekaźnika Krawędziowego**.

2. Rozpocznij monitorowanie lub skonfiguruj ustawienia serwera Serwer Przekaźnika Krawędziowego.

USTAWIENIE	OPIS
Adres IP	Bieżący adres IP serwera Serwer Przekaźnika Krawędziowego Aby skonfigurować nowe ustawienia połączenia serwera Serwer Przekaźnika Krawędziowego, kliknij przycisk **Rozłącz** i zmodyfikuj ustawienia połączenia. Aby uzyskać więcej informacji, patrz *Łączenie z serwerem Przekaźnika Krawędziowego na stronie 16-14*.
Stan	Stan połączenia “Online” lub “Offline” między serwerem OfficeScan a programem Serwer Przekaźnika Krawędziowego

USTAWIENIE	OPIS
Zsynchronizowano	Czas ostatniej synchronizacji Serwer Przekaźnika Krawędziowego z serwerem OfficeScan Kliknij przycisk **Synchronizuj teraz**, aby natychmiast zsynchronizować serwer OfficeScan z programem Serwer Przekaźnika Krawędziowego.
Zaplanowana synchronizacja	Częstotliwość, z jaką serwer OfficeScan wykonuje synchronizację z programem Serwer Przekaźnika Krawędziowego W zależności od dostępnej przepustowości wybierz ustawienie **Co godzinę** lub **Co 15 minut** dla częstotliwości synchronizacji.

3. Kliknij przycisk **Zapisz**.

Zarządzanie certyfikatami Serwer Przekaźnika Krawędziowego

Program OfficeScan udostępnia narzędzie wiersza polecenia, które umożliwia utworzenie lub odnowienie certyfikatu serwera Serwer Przekaźnika Krawędziowego, który agenci używają do komunikacji. Po utworzeniu nowego certyfikatu Serwer Przekaźnika Krawędziowego wysyła nowy certyfikat do serwera OfficeScan, który następnie wdraża certyfikat na agentach, kiedy następnym razem połączą się z serwerem OfficeScan.

Ważne

Agenci OfficeScan zdalni muszą połączyć się z serwerem OfficeScan w celu uzyskania nowego certyfikatu Serwer Przekaźnika Krawędziowego. Agenci zdalni, którzy nie otrzymają zaktualizowanego certyfikatu, nie będą mogli już komunikować się z programem Serwer Przekaźnika Krawędziowego do momentu nawiązania połączenia z serwerem OfficeScan.

Procedura

1. Na serwerze Przekaźnika Krawędziowego otwórz edytor wiersza polecenia i przejdź do następującego katalogu:

   ```
   C:\Program Files\Trend Micro\OfficeScan Edge\OfcEdgeSvc\web
   \service
   ```

2. Uruchom narzędzie certyfikatu, wykonując następujące polecenie:

   `OfcEdgeCfg.exe --renewcert -certpwd <hasło>`

   Gdzie:

   - **`--renewcert`**: tworzy nowy certyfikat
   - **`-certpwd <hasło>`**: określa hasło dla pakietu certyfikatu

   Serwer Przekaźnika Krawędziowego utworzy nowy pakiet certyfikatu i automatycznie wyśle certyfikat do serwera OfficeScan. Serwer OfficeScan wdroży nowy certyfikat na Agenci OfficeScan następnym razem, gdy Agenci OfficeScan zgłoszą się do serwera OfficeScan.

Rozdział 17

Używanie programu Plug-In Manager

W tym rozdziale omówiono sposób konfigurowania programu Plug-in Manager oraz przedstawiono przegląd rozwiązań dodatków dostarczanych za pośrednictwem programu Plug-in Manager.

Rozdział składa się z następujących tematów:

Plug-in Manager — informacje

Program Program OfficeScan zawiera środowisko o nazwie Plug-in Manager, które integruje nowe rozwiązania w istniejącym środowisku Program OfficeScan. Aby ułatwić zarządzanie tymi rozwiązaniami, program Plug-in Manager zapewnia zestawienie danych dotyczących rozwiązań w postaci widgetów.

Uwaga

Żadne rozwiązania dodatków nie obsługują obecnie protokołu IPv6. Serwer może pobrać te rozwiązania, ale nie będzie możliwe ich zainstalowanie na agentach lub hostach wykorzystujących wyłącznie protokół IPv6.

Program Plug-in Manager zapewnia:

- **Natywne funkcje produktu**

  Niektóre natywne funkcje programu Program OfficeScan są licencjonowane oddzielnie i aktywowane za pomocą programu Plug-in Manager. W tej wersji istnieją dwie funkcje w tej kategorii, a mianowicie **Trend Micro Virtual Desktop Support** i **Ochrona danych OfficeScan**.

- **Programy dodatków**

  Programy dodatków, które nie stanowią części programu Program OfficeScan. Programy dodatków mają oddzielne licencje i konsole zarządzania. Dostęp do tych konsoli zarządzania można uzyskać z poziomu konsoli Web programu Program OfficeScan. Przykłady programów dodatków to **Trend Micro OfficeScan ToolBox** i **Trend Micro Security (dla komputerów Mac)**.

- **Karty i widgety pulpitu**

  Ekran **Pulpit** programu Program OfficeScan wymaga programu Plug-in Manager do wyświetlania kart i widgetów służących do monitorowania stanu ochrony serwera i agentów Program OfficeScan.

Niniejszy dokument zawiera ogólne omówienie instalacji programów dodatków oraz zarządzania nimi, a także przedstawia dane takich dodatków, jakie są dostępne

w widgetach. Szczegółowe informacje dotyczące konfiguracji programów i zarządzania nimi można znaleźć w dokumentacji odpowiedniego programu dodatku.

Agenci programów dodatków na punktach końcowych

Niektóre programy dodatków (takie jak Trend Micro Security (dla komputerów Mac)) mają agenta, który jest instalowany w systemie operacyjnym Windows na punkcie końcowym. Zarządzanie tymi agentami odbywa się za pomocą programu Plug-in Manager agenta OfficeScan, który działa w ramach procesu o nazwie `CNTAoSMgr.exe`.

Program Program OfficeScan instaluje program `CNTAoSMgr.exe` wraz z agentem OfficeScan. Jedynym dodatkowym wymaganiem systemowym dla programu `CNTAoSMgr.exe` jest program Microsoft XML Parser (MSXML) w wersji 3.0 lub nowszej.

Uwaga

Inne programy dodatków mają agentów, którzy nie są instalowani w systemach operacyjnych Windows, więc nie są zarządzane przez program Plug-in Manager agenta OfficeScan. Przykładem tych agentów jest program Trend Micro Security (dla komputerów Mac).

Element widget

Za pomocą widgetów można szybko wyświetlić zestawienie danych dla zainstalowanych rozwiązań dodatków. Widgety są dostępne na ekranie **Pulpit** serwera Program OfficeScan. Specjalny widget o nazwie **Informacje z programu OfficeScan i dodatków** łączy dane z agentów OfficeScan i zainstalowanych programów dodatków, a następnie wyświetla je w drzewie agentów.

Ten Podręcznik administratora zawiera przegląd widgetów i rozwiązań obsługujących widgety.

Instalacja programu Plug-in Manager

W przypadku wcześniejszych wersji programu Plug-in Manager pakiet instalacyjny programu Plug-in Manager był pobierany z serwera Trend Micro ActiveUpdate Server, a

następnie instalowany na komputerze z serwerem Program OfficeScan. W tej wersji pakiet instalacyjny został dołączony do pakietu instalacyjnego serwera Program OfficeScan w następującej lokalizacji:

<*folder instalacji serwera*>\PCCSRV\Admin\Utility\PLM\PLMSetup.exe

Wykonaj plik `PLMSetup.exe`, aby zainstalować program Plug-in Manager.

W przypadku nowych użytkowników programu Program OfficeScan serwer Program OfficeScan i program Plug-in Manager zostaną zainstalowane po zakończeniu instalacji programu Program OfficeScan. Jeśli wykonywana jest aktualizacja do nowej wersji programu Program OfficeScan, a wcześniej używano programu Plug-in Manager, konieczne będzie zatrzymanie usługi Plug-in Manager przed uruchomieniem pakietu instalacyjnego.

Wykonywanie czynności po zainstalowaniu

Po zainstalowaniu programu Plug-in Manager wykonaj następujące kroki:

Procedura

1. Otwórz konsolę Web programu Program OfficeScan i kliknij polecenie **Dodatki** w menu głównym.
2. Zarządzaj rozwiązaniami dodatków.
3. Wyświetl **Pulpit** w konsoli Web programu Program OfficeScan, aby zarządzać widgetami rozwiązań dodatków.

Zarządzanie natywnymi funkcjami programu Program OfficeScan

Natywne funkcje programu Program OfficeScan są instalowane wraz z programem Program OfficeScan i aktywowane za pomocą programu Plug-in Manager. Zarządzanie niektórymi funkcjami, takimi jak Trend Micro Virtual Desktop Support, odbywa się z poziomu programu Plug-in Manager, natomiast zarządzanie innymi funkcjami, takimi

jak Ochrona danych Program OfficeScan, jest wykonywane z poziomu konsoli Web programu Program OfficeScan.

Zarządzanie dodatkami

Programy dodatków należy instalować i aktywować niezależnie od programu Program OfficeScan. Każdy program dodatku udostępnia własną konsolę do zarządzania produktem. Konsole zarządzania są dostępne z poziomu konsoli Web programu Program OfficeScan.

Instalacja dodatku

Programy dodatków są wyświetlane w konsoli programu **Plug-in Manager**. Za pomocą konsoli można pobrać i zainstalować programy oraz zarządzać nimi. Program Plug-in Manager pobiera pakiet instalacyjny programu dodatku z serwera Trend Micro ActiveUpdate lub niestandardowego źródła aktualizacji, jeśli zostało prawidłowo skonfigurowane. Do pobrania pakietu z serwera ActiveUpdate wymagane jest połączenie internetowe.

Podczas pobierania pakietu instalacyjnego lub po uruchomieniu instalacji program Plug-in Manager tymczasowo wyłącza inne funkcje programu dodatku, takie jak pobieranie, instalowanie i uaktualnianie.

Program Plug-in Manager nie obsługuje instalacji ani zarządzania programami dodatków przez funkcję logowania jednokrotnego programu Trend Micro Control Manager.

Instalowanie programu Programy dodatków

Procedura

1. Otwórz konsolę Web programu Program OfficeScan i kliknij polecenie **Dodatki** w menu głównym.
2. Na ekranie **Plug-in Manager** przejdź do sekcji dodatku i kliknij polecenie **Pobierz**.

Wielkość pakietu programu dodatku jest wyświetlana obok przycisku **Pobieranie**. Program Plug-In Manager zapisuje pobrany pakiet w lokalizacji `<Folder instalacji serwera>\PCCSRV\Download\Product`.

Program Plug-In Manager zapisuje pobrany plik w lokalizacji `<Folder instalacji serwera>\PCCSRV\Download\Product`.

Można monitorować postęp lub opuścić ten ekran podczas pobierania.

Uwaga

W przypadku, gdy program Program OfficeScan napotka problem podczas pobierania lub instalowania pakietu, należy sprawdzić dzienniki aktualizacji serwera w konsoli Web programu Program OfficeScan. W menu głównym kliknij polecenie **Dzienniki** > **Aktualizacje serwera**.

3. Kliknij przycisk **Instaluj teraz** lub **Instaluj później**.

   - Po kliknięciu przycisku **Instaluj teraz** rozpoczyna się instalacja i pojawia się ekran postępu instalacji.
   - Po kliknięciu przycisku **Instaluj później** pojawia się ekran **Plug-in Manager**.

     Zainstaluj program dodatku, klikając przycisk **Instaluj** znajdujący się w sekcji programu dodatku na ekranie **Plug-in Manager**.

   Wyświetlony zostanie ekran **Umowa licencyjna użytkownika oprogramowania (EULA) Trend Micro**.

   Uwaga

   Nie wszystkie programy dodatków wymagają tego ekranu. Jeśli ten ekran nie zostanie wyświetlony, rozpocznie się instalacja programu dodatku.

4. Kliknij przycisk **Akceptuj**, aby zainstalować program dodatku.

   Można monitorować postęp lub opuścić ten ekran podczas instalacji.

Uwaga

W przypadku, gdy program Program OfficeScan napotka problem podczas pobierania lub instalowania pakietu, należy sprawdzić dzienniki aktualizacji serwera w konsoli Web programu Program OfficeScan. W menu głównym kliknij polecenie **Dzienniki** > **Aktualizacje serwera**.

Po zakończeniu instalacji aktualna wersja dodatku zostaje wyświetlona na ekranie **Plug-in Manager**.

Aktywowanie licencji dodatku Program dodatku

Procedura

1. Otwórz konsolę Web programu Program OfficeScan i kliknij polecenie **Dodatki** w menu głównym.
2. Na ekranie **Plug-in Manager** przejdź do sekcji dodatku i kliknij polecenie **Zarządzaj programem**.

   Zostanie wyświetlony ekran **Nowy kod aktywacyjny licencji produktu**.
3. Wpisz kod aktywacyjny lub skopiuj i wklej go do pól tekstowych.
4. Kliknij przycisk **Zapisz**.

   Zostanie wyświetlona konsola dodatku.

Wyświetlanie i odnawianie informacji o licencji

Procedura

1. Otwórz konsolę Web programu Program OfficeScan i kliknij polecenie **Dodatki** w menu głównym.
2. Na ekranie **Plug-in Manager** przejdź do sekcji dodatku i kliknij polecenie **Zarządzaj programem**.

3. W konsoli dodatku użyj hiperłącza **Wyświetl informacje o licencji**.

   Nie wszystkie programy dodatków wyświetlają hiperłącze **Wyświetl informacje o licencji** w tym samym miejscu. Szczegółowe informacje znajdują się w dokumentacji programu dodatku.

4. Zapoznaj się ze następującymi szczegółami licencjami na wyświetlonym ekranie.

OPCJA	OPIS
Stan	Wyświetlana jest wartość „Aktywowane”, „Nieaktywowane” lub „Wygasłe”.
Wersja	Wyświetlana jest wartość „Pełna” lub „Próbna”. **Uwaga** Po aktywacji wersji pełnej i próbnej wyświetlana jest wersja „Pełna”.
Stanowiska	Wyświetla liczbę punktów końcowych, którymi może zarządzać program dodatku.
Licencja utraci ważność	Jeśli program dodatku ma przypisanych wiele licencji, jest wyświetlana najpóźniejsza data wygaśnięcia. Na przykład, jeśli licencje wygasają w dniach 31-12-2011 i 30-06-2011, wyświetlana jest data 31-12-2011.
Kod aktywacyjny	wyświetla kod aktywacyjny.
Przypomnienia	W zależności od bieżącej wersji licencji dodatek wyświetla przypomnienie o dacie utraty ważności licencji w ciągu okresu wstępnego (tylko w pełnej wersji) lub po utracie ważności licencji.

Uwaga

Czas trwania okresu próbnego różni się w zależności od regionu. Okres wstępny dodatku można sprawdzić u przedstawiciela firmy Trend Micro.

Po wygaśnięciu licencji program dodatku kontynuuje działanie, ale pomoc techniczna i aktualizacje nie są już dostępne.

5. Kliknij opcję **Zobacz szczegóły dotyczące licencji w trybie online**, aby wyświetlić informacje o aktualnej licencji w witrynie internetowej firmy Trend Micro.

6. Aby zaktualizować zawartość ekranu na podstawie najnowszych informacji o licencji, kliknij opcję **Aktualizuj informacje**.

7. Kliknij polecenie **Nowy kod aktywacyjny**, aby otworzyć ekran **Nowy kod aktywacyjny licencji produktu**.

   Szczegółowe informacje zawiera sekcja *Aktywowanie licencji dodatku Program dodatku na stronie 3-4*.

Zarządzanie programem dodatku

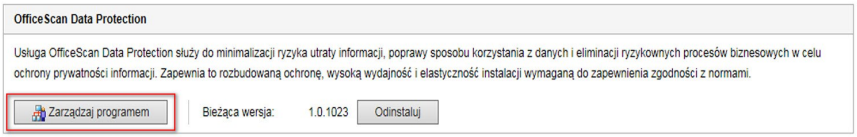
Za pomocą konsoli zarządzania programem dodatku, która jest dostępna z poziomu konsoli Web programu Program OfficeScan, można konfigurować ustawienia i wykonywać zadania związane z programem. Zadania obejmują aktywację programu i ewentualnie instalację agenta programu dodatku na punktach końcowych. Szczegółowe informacje dotyczące konfiguracji programów i zarządzania nimi można znaleźć w dokumentacji odpowiedniego dodatku.

Zarządzanie dodatkami

Procedura

1. Otwórz konsolę Web programu Program OfficeScan i kliknij polecenie **Dodatki** w menu głównym.

2. Na ekranie **Plug-in Manager** przejdź do sekcji dodatku i kliknij polecenie **Zarządzaj programem**.



ILUSTRACJA 17-1. Przycisk Zarządzaj programem

Jeśli zarządzanie programem dodatku odbywa się po raz pierwszy, program dodatku może wymagać aktywacji. Szczegółowe informacje zawiera sekcja *Aktywowanie licencji dodatku Program dodatku na stronie 3-4*.

Uaktualnianie dodatku

Nowa wersja programu dodatku jest wyświetlana w konsoli programu Plug-in Manager. Pobierz pakiet i uaktualnij program dodatku w konsoli. Program Plug-in Manager pobiera pakiet z serwera Trend Micro ActiveUpdate lub niestandardowego źródła aktualizacji, jeśli zostało prawidłowo skonfigurowane. Do pobrania pakietu z serwera ActiveUpdate wymagane jest połączenie internetowe.

Podczas pobierania pakietu instalacyjnego lub po uruchomieniu uaktualniania program Plug-in Manager tymczasowo wyłącza inne funkcje programu dodatku, takie jak pobieranie, instalowanie i uaktualnianie.

Program Plug-in Manager nie obsługuje uaktualniania programów dodatków przez funkcję jednokrotnego logowania programu Trend Micro Control Manager.

Aktualizacja Programy dodatków

Procedura

1. Otwórz konsolę Web programu Program OfficeScan i kliknij polecenie **Dodatki** w menu głównym.
2. Na ekranie **Plug-in Manager** przejdź do sekcji dodatku i kliknij polecenie **Pobierz**.

   Rozmiar pakietu uaktualnienia zostanie wyświetlony obok przycisku **Pobierz**.

Można monitorować postęp lub opuścić ten ekran podczas pobierania.

Uwaga

W przypadku, gdy program Program OfficeScan napotka problem podczas pobierania lub instalowania pakietu, należy sprawdzić dzienniki aktualizacji serwera w konsoli Web programu Program OfficeScan. W menu głównym kliknij polecenie **Dzienniki** > **Aktualizacje serwera**.

3. Po pobraniu pakietu przez program Plug-in Manager zostanie wyświetlony nowy ekran.

4. Kliknij przycisk **Uaktualnij teraz** lub **Uaktualnij później**.

   - Po kliknięciu przycisku **Uaktualnij teraz** rozpoczyna się uaktualnianie i pojawia się ekran postępu uaktualniania.
   - Po kliknięciu przycisku **Uaktualnij później** pojawia się ekran **Plug-in Manager**.

     Uaktualnij program dodatku, klikając przycisk **Uaktualnij** znajdujący się w sekcji programu dodatku na ekranie **Plug-in Manager**.

Po zakończeniu uaktualniania usługa Plug-in Manager może wymagać ponownego uruchomienia, przez co ekran **Plug-in Manager** jest chwilowo niedostępny. Gdy ekran ten stanie się dostępny, zostanie wyświetlona aktualna wersja programu dodatku.

Dezinstalacja dodatku

Program dodatku można odinstalować w następujący sposób:

- Odinstaluj program dodatku z poziomu konsoli programu Plug-in Manager.
- Odinstaluj serwer Program OfficeScan, co spowoduje dezinstalację programu Plug-in Manager i wszystkich zainstalowanych programów dodatków. Instrukcje dezinstalacji serwera Program OfficeScan zawiera sekcja *Podręcznik instalacji oraz uaktualniania programu OfficeScan*.

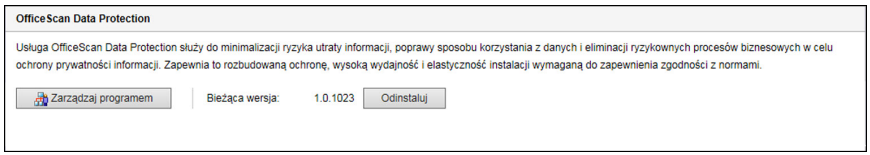
W przypadku programów dodatków z agentami na punkcie końcowym:

- Sprawdź w dokumentacji programu dodatku, czy dezinstalacja programu dodatku spowoduje również dezinstalację agenta dodatku.
- W przypadku agentów dodatków, które są zainstalowane na tym samym punkcie końcowym co Agent OfficeScan, dezinstalacja agenta OfficeScan spowoduje również dezinstalację agentów dodatku i programu Plug-in Manager agenta OfficeScan (`CNTAoSMgr.exe`).

Dezinstalacja programów dodatków z poziomu konsoli programu Plug-In Manager

Procedura

1. Otwórz konsolę Web programu Program OfficeScan i kliknij polecenie **Dodatki** w menu głównym.
2. Na ekranie **Plug-in Manager** przejdź do sekcji dodatku i kliknij polecenie **Odinstaluj**.



3. Można monitorować postęp dezinstalacji lub opuścić ten ekran podczas dezinstalacji.
4. Odśwież ekran **Plug-in Manager** po zakończeniu dezinstalacji.

   Program dodatku stanie się ponownie dostępny w celu instalacji.

Dezinstalacja programu Plug-in Manager

Odinstaluj serwer Program OfficeScan, co spowoduje dezinstalację programu Plug-In Manager i wszystkich zainstalowanych programów dodatków. Instrukcje dezinstalacji

serwera Program OfficeScan zawiera sekcja *Podręcznik instalacji oraz uaktualniania programu OfficeScan*.

Rozwiązywanie problemów z programem Plug-in Manager

Należy sprawdzić dzienniki diagnostyczne serwera Program OfficeScan i agenta OfficeScan pod kątem informacji o diagnostyce programu Plug-in Manager i programów dodatków.

Program dodatku nie jest wyświetlany w konsoli programu Plug-in Manager

Program dodatku, który jest dostępny do pobrania i instalacji, może nie być wyświetlany w konsoli programu Plug-in Manager z następujących powodów:

Procedura

1. Plug-in Manager wciąż pobiera program – dodatek, co może trochę potrwać, jeśli rozmiar pakietu programu jest duży. Należy od czasu do czasu sprawdzać ekran, aby sprawdzić czy program – dodatek jest wyświetlany.

   Uwaga

   Jeśli program Plug-in Manager nie może pobrać programu dodatku, wznowi automatycznie pobieranie po 24 godzinach. Aby ręcznie uruchomić pobieranie programu dodatku przez program Plug-in Manager, uruchom ponownie usługę Program OfficeScan Plug-in Manager.

2. Komputer serwera nie może połączyć się z Internetem. Jeśli serwer łączy się z Internetem przez serwer proxy, należy się upewnić, że połączenie internetowe może zostać nawiązane z wykorzystaniem ustawień proxy.

3. Źródłem aktualizacji programu OfficeScan nie jest serwer ActiveUpdate. W konsoli Web programu Program OfficeScan przejdź do pozycji **Aktualizacje** > **Serwer** >

Źródło aktualizacji i sprawdź źródło aktualizacji. Jeśli źródłem aktualizacji nie jest serwer ActiveUpdate, dostępne są następujące opcje:

- Wybierz serwer ActiveUpdate jako źródło aktualizacji.
- W przypadku wybrania opcji **Inne źródło aktualizacji** wybierz pierwszy wpis na liście **Inne źródło aktualizacji** i sprawdź, czy może zostać nawiązane połączenie z serwerem ActiveUpdate. Plug-in Manager obsługuje jedynie pierwszy wpis na liście.
- W przypadku wybrania opcji **Lokalizacja kopii bieżącego pliku w sieci Intranet** upewnij się, że punkt końcowy w sieci Intranet także może nawiązać połączenie z serwerem ActiveUpdate.

Problemy z instalacją agenta dodatku i wyświetlaniem na punktach końcowych

Instalacja agenta programu dodatku na punkcie końcowym może się nie powieść lub agent może nie zostać wyświetlony w konsoli agenta OfficeScan z następujących przyczyn:

Procedura

1. Program Plug-in Manager (`CNTAosMgr.exe`) nie jest uruchomiony na punkcie końcowym. Na punkcie końcowym agenta OfficeScan otwórz Menedżera zadań systemu Windows i uruchom proces `CNTAosMgr.exe`.
2. Pakiet instalacyjny agenta dodatku nie został pobrany do folderu punktu końcowego agenta OfficeScan w lokalizacji `<Folder instalacji agenta>\AU_Data\AU_Temp\{xxx}AU_Down\Product`. Sprawdź plik `Tmudump.txt` znajdujący się w folderze `\AU_Data\AU_Log\` aby poznać przyczyny niepowodzenia podczas pobierania pliku.

Uwaga

Jeśli instalacja agenta powiedzie się, informacje o agencie będą dostępne w lokalizacji `<Folder instalacji agenta>\AOSSvcInfo.xml`.

3. Instalacja agenta nie powiodła się lub wymaga działania. Stan instalacji można sprawdzić w konsoli zarządzania programu dodatku, a następnie wykonać operacje, takie jak ponowne uruchomienie punktu końcowego agenta OfficeScan po instalacji lub zainstalowanie wymaganych poprawek systemu operacyjnego przed dokonaniem instalacji.

Nie można uruchomić agentów na punktach końcowych, jeżeli ustawienie skryptu automatycznej konfiguracji programu Internet Explorer powoduje przekierowanie połączenia do serwera proxy.

Program Plug-in Manager Agent OfficeScan (`CNTAosMgr.exe`) nie może uruchomić agentów na punktach końcowych, ponieważ polecenie uruchamiające agenta powoduje przekierowanie do serwera proxy. Ten problem pojawia się, tylko gdy ustawienia proxy powodują przekierowanie ruchu HTTP użytkownika na adres 127.0.0.1.

Aby rozwiązać ten problem, użyj poprawnie zdefiniowanych reguł dla serwera proxy. Nie należy na przykład przekierowywać ruchu HTTP na adres 127.0.0.1.

Jeśli konieczne jest korzystanie z konfiguracji proxy, w ramach której kontrolowane są żądania HTTP związane z adresem 127.0.0.1, wykonaj poniższe czynności.

Procedura

1. Skonfiguruj ustawienia zapory programu Program OfficeScan za pomocą konsoli Web programu Program OfficeScan.

   Uwaga

   Ten krok należy wykonać, jeśli włączana jest zapora programu Program OfficeScan na agentach OfficeScan.

   a. W konsoli Web przejdź do pozycji **Agenci** > **Zapora** > **Reguły** i kliknij polecenie **Edytuj szablon wyjątku**.

   b. Na ekranie Edytuj szablon wyjątku kliknij przycisk **Dodaj**.

c. Użyj następujących ustawień:

- **Nazwa**: Preferowana nazwa
- **Operacja**: Zezwalaj na ruch sieciowy
- **Kierunek**: Przychodzące
- **Protokół**: TCP
- **Porty**: Dowolny numer portu z przedziału od 5000 do 49151

d. **Adresy IP**: Wybierz opcję **Pojedynczy adres IP** i określ adres IP serwera proxy (zalecane) lub wybierz opcję **Wszystkie adresy IP**.

e. Kliknij przycisk **Zapisz**.

f. Na ekranie Edytuj szablon wyjątku kliknij przycisk **Zapisz i zastosuj dla istniejących reguł**.

g. Przejdź do opcji **Agenci** > **Zapora** > **Profile** i kliknij polecenie **Przypisz profil do agentów**.

Jeśli nie istnieje żaden profil zapory, można go utworzyć, klikając przycisk Dodaj. Użyj następujących ustawień:

- **Nazwa**: Preferowana nazwa
- **Opis**: Preferowany opis
- **Reguły**: Wszystkie reguły dostępu

Po zapisaniu nowego profilu kliknij polecenie **Przypisz profil do agentów**.

2. Zmodyfikuj plik `ofcscan.ini`.

a. Za pomocą edytora tekstu otwórz plik `ofcscan.ini` w lokalizacji `<Folder instalacyjny serwera>`.

b. Wyszukaj sekcję **`[Global Setting]`** i dodaj ciąg `FWPortNum=21212` w następnym wierszu. Zmień wartość „21212” na numer portu, który został określony w kroku c powyżej.

Na przykład:

```
[Global Setting]

FWPortNum=5000
```

c. Zapisz plik.

3. W konsoli Web przejdź do opcji **Agenci** > **Ustawienia agenta globalnego** i kliknij przycisk **Zapisz**.

Wystąpił błąd w systemie, module aktualizacji lub programie Plug-in Manager. Komunikat o błędzie zawiera określony kod błędu.

Program Plug-in Manager może wyświetlić następujące kody błędów w komunikacie o błędzie. Jeśli nie możesz rozwiązać danego problemu po zapoznaniu się z rozwiązaniami przedstawionymi w poniższej tabeli, skontaktuj się z dostawcą pomocy technicznej.

TABELA 17-1. Kody błędów programu Plug-in Manager

KOD BŁĘDU	WIADOMOŚĆ, PRZYCZYNA I ROZWIĄZANIE
001	Wystąpił błąd w programie Plug-in Manager. Moduł aktualizacji programu Plug-in Manager nie odpowiada podczas sprawdzania postępu zadania aktualizacji. Być może moduł lub program obsługi polecenia nie został zainicjowany. Uruchom ponownie usługę Program OfficeScan Plug-in Manager i wykonaj ponownie zadanie.

Kod błędu	Wiadomość, przyczyna i rozwiązanie
002	Wystąpił błąd systemowy. Menedżer aktualizacji programu Plug-in Manager nie może otworzyć klucza rejestru `SOFTWARE\TrendMicro\OfficeScan\service\AoS`, ponieważ mógł on zostać usunięty. Wykonaj następujące czynności: 1. Otwórz edytor rejestru i przejdź do lokalizacji `HKEY_LOCAL_MACHINE \SOFTWARE\TrendMicro\OfficeScan\ service\AoS \OSCE_Addon_Service_CompList_Version`. Przywróć wartość 1.0.1000. 2. Uruchom ponownie usługę Program OfficeScan Plug-in Manager. 3. Pobierz lub odinstaluj program dodatku.
028	Wystąpił błąd aktualizacji. Możliwe przyczyny: • Moduł aktualizacji programu Plug-in Manager nie mógł pobrać programu dodatku. Sprawdź, czy połączenie sieciowe działa, a następnie spróbuj ponownie. • Moduł aktualizacji programu Plug-in Manager nie może zainstalować programu dodatku, ponieważ agent poprawki modułu AU zwrócił błąd. Agent poprawki programu AU jest programem, który uruchamia instalację nowych dodatków. Aby poznać dokładną przyczynę błędu, sprawdź dziennik diagnostyczny modułu ActiveUpdate zapisany w pliku `TmuDump.txt` w położeniu `\PCCSRV\Web\Service\AU_Data\AU_Log`. Wykonaj następujące czynności: 1. Otwórz edytor rejestru i przejdź do lokalizacji `HKEY_LOCAL_MACHINE \SOFTWARE\TrendMicro\OfficeScan\service\AoS \OSCE_Addon_Service_CompList_Version`. Przywróć wartość 1.0.1000. 2. Usuń klucz rejestru dodatku `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro \OfficeScan\service\AoS\OSCE_ADDON_xxxx`. 3. Uruchom ponownie usługę Program OfficeScan Plug-in Manager. 4. Pobierz i zainstaluj dodatek.

Kod błędu	Wiadomość, przyczyna i rozwiązanie
170	Wystąpił błąd systemowy. Moduł aktualizacji program Plug-in Manager nie może przetworzyć operacji przychodzącej, ponieważ aktualnie obsługuje inną operację. Wykonaj zadanie później.
202	Wystąpił błąd w programie Plug-in Manager. Program Plug-in Manager nie może obsłużyć zadania wykonywanego w konsoli Web. Odśwież konsolę Web lub uaktualnij program Plug-in Manager, jeśli dostępne jest uaktualnienie.
203	Wystąpił błąd w programie Plug-in Manager. Program Plug-in Manager napotkał błąd komunikacji między procesami (IPC) podczas próby nawiązania komunikacji z usługami zaplecza programu Plug-in Manager. Uruchom ponownie usługę Program OfficeScan Plug-in Manager i wykonaj ponownie zadanie.
Inne kody błędów	Wystąpił błąd systemowy. Podczas pobierania nowego programu dodatku program Plug-in Manager sprawdza listę programów dodatków na serwerze ActiveUpdate. Program Plug-In Manager nie mógł pobrać listy. Wykonaj następujące czynności: 1. Otwórz edytor rejestru i przejdź do lokalizacji `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`. Przywróć wartość `1.0.1000`. 2. Uruchom ponownie usługę Program OfficeScan Plug-in Manager. 3. Pobierz i zainstaluj dodatek.

Rozdział 18

Zasoby dotyczące rozwiązywania problemów

W tym rozdziale znajduje się lista zasobów, których można użyć w procesie rozwiązywania problemów związanych z serwerem OfficeScan i agentem OfficeScan.

Rozdział składa się z następujących tematów:

Inteligentny system wspierający

Inteligentny system wspierający to strona, za pomocą której można z łatwością wysyłać pliki do firmy Trend Micro w celu ich przeanalizowania. System ten ustala identyfikator GUID serwera OfficeScan i przesyła tę informację razem z plikiem. Dzięki otrzymaniu identyfikatora GUID serwera OfficeScan firma Trend Micro może przesłać opinię zwrotną dotyczącą plików wysłanych do oceny.

Narzędzie Case Diagnostic Tool

Narzędzie Case Diagnostic Tool (CDT) firmy Trend Micro gromadzi niezbędne informacje diagnostyczne w razie wystąpienia problemów w produktach używanych przez użytkowników. Włącza i wyłącza ono automatycznie funkcję stanu diagnostyki produktu i gromadzi niezbędne pliki, w zależności od kategorii problemu. Firma Trend Micro wykorzystuje te informacje w celu rozwiązania problemów związanych z produktem.

Narzędzie można uruchamiać na wszystkich platformach zgodnych z programem OfficeScan. Aby uzyskać to narzędzie i odpowiednią dokumentację, należy skontaktować się z przedstawicielem działu pomocy technicznej.

Narzędzie optymalizacji wydajności firmy Trend Micro

Firma Trend Micro udostępnia samodzielne narzędzie do optymalizacji wydajności, które identyfikuje aplikacje mogące wywoływać problemy związane z wydajnością. Narzędzie optymalizacji wydajności firmy Trend Micro, dostępne w Bazie wiedzy Trend Micro, należy uruchomić na standardowym obrazie stacji roboczej i/lub kilku docelowych stacjach roboczych podczas procesu próbnego, aby wstępnie wyeliminować problemy związane z wydajnością w bieżącej instalacji usług monitorowania zachowań oraz kontroli urządzeń.

Szczegółowe informacje można znaleźć na stronie http://esupport.trendmicro.com/solution/en-us/1056425.aspx.

Dzienniki serwera OfficeScan

Oprócz dzienników dostępnych z poziomu konsoli Web do rozwiązania problemów związanych z produktem można użyć innych typów dzienników (takich jak dzienniki diagnostyczne).

OSTRZEŻENIE!

Dzienniki diagnostyczne mogą zmniejszyć wydajność serwera i zajmować wiele miejsca na dysku. Tworzenie dzienników diagnostycznych należy włączać wyłącznie w razie konieczności i szybko wyłączyć tę opcję, kiedy tylko dane diagnostyczne przestaną być potrzebne. Dziennik diagnostyczny należy usunąć, aby zaoszczędzić miejsce na dysku twardym.

Tworzenie dzienników diagnostycznych serwera z wykorzystaniem pliku LogServer.exe

Program `LogServer.exe` można wykorzystać do zebrania dzienników diagnostycznych dotyczących następujących elementów:

- Podstawowe dzienniki serwera OfficeScan
- Skaner narażenia na atak firmy Trend Micro
- Dzienniki integracji z usługą Active Directory
- Dzienniki grupowania agentów
- Dzienniki zgodności z zabezpieczeniami
- Administracja oparta na rolach
- Smart scan

Włączanie rejestracji w dzienniku diagnostycznym

Procedura

1. Zaloguj się do konsoli Web.
2. Na banerze konsoli Web kliknij pierwszą literę „O" w słowie „OfficeScan".
3. Wybierz opcję **Włącz dziennik diagnostyczny**.
4. Określ ustawienia dziennika diagnostycznego.
5. Kliknij przycisk **Zapisz**.
6. Sprawdź plik dziennika (`ofcdebug.log`) w domyślnej lokalizacji: <*Folder instalacji serwera*>`\PCCSRV\Log`.

Wyłączanie rejestracji w dzienniku diagnostycznym

Procedura

1. Zaloguj się do konsoli Web.
2. Na banerze konsoli Web kliknij pierwszą literę „O" w słowie „OfficeScan".
3. Usuń zaznaczenie pola wyboru **Włącz dziennik diagnostyczny**.
4. Kliknij przycisk **Zapisz**.

Włączanie rejestracji w dzienniku diagnostycznym w zakresie instalacji i aktualizacji serwera

Funkcję rejestrowania w dzienniku diagnostycznym należy włączyć przed wykonaniem następujących czynności:

- Odinstaluj serwer, a następnie zainstaluj go ponownie.
- Zaktualizuj program OfficeScan do nowej wersji.

- Zdalna instalacja/uaktualnienie (funkcja rejestracji w dzienniku diagnostycznym jest włączona na punkcie końcowym, na którym uruchomiono program instalacyjny, a nie na zdalnym punkcie końcowym).

Procedura

1. Skopiuj na dysk `C:\` folder `LogServer` z lokalizacji <*Folder instalacji serwera*> `\PCCSRV\Private`.
2. Utwórz plik o nazwie `ofcdebug.ini` z następującą zawartością:

   ```
   [debug]

   debuglevel=9

   debuglog=c:\LogServer\ofcdebug.log

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1
   ```

3. Zapisz plik `ofcdebug.ini` w lokalizacji `C:\LogServer`.
4. Wykonaj odpowiednią operację (czyli instalację/ponowną instalację serwera, aktualizację do nowej wersji serwera lub zdalną instalację/uaktualnienie).
5. Sprawdź plik `ofcdebug.log` w lokalizacji `C:\LogServer`.

Dzienniki instalacji

- Dzienniki instalacji lokalnej/aktualizacji

  Nazwa pliku: `OFCMAS.LOG`

  Lokalizacja: `%windir%`

- Dziennik instalacji zdalnej/aktualizacji

- Na punkcie końcowym, na którym uruchomiono program instalacyjny:

  Nazwa pliku: `ofcmasr.log`

  Lokalizacja: `%windir%`

- Na docelowym punkcie końcowym:

  Nazwa pliku: `OFCMAS.LOG`

  Lokalizacja: `%windir%`

Dzienniki Active Directory

- Nazwa pliku: `ofcdebug.log`
- Nazwa pliku: `ofcserver.ini`

  Lokalizacja: <*Folder instalacji serwera*>`\PCCSRV\Private\`
- Nazwy plików:
  - `dbADScope.cdx`
  - `dbADScope.dbf`
  - `dbADPredefinedScope.cdx`
  - `dbADPredefinedScope.dbf`
  - `dbCredential.cdx`
  - `dbCredential.dbf`

  Lokalizacja: `<Folder instalacji serwera>\PCCSRV\HTTPDB\`

Dzienniki administracji opartej na rolach

Aby uzyskać szczegółowe informacje na temat administracji opartej na rolach, należy wykonać jedną z następujących czynności:

- Uruchom narzędzie Trend Micro Case Diagnostics Tool. Informacje zawiera temat *Narzędzie Case Diagnostic Tool na stronie 18-2*.

- Zbierz następujące dzienniki:
  - Wszystkie pliki z lokalizacji <*Folder instalacji serwera*>\PCCSRV\Private\AuthorStore.
  - *Dzienniki serwera OfficeScan na stronie 18-3*

Dzienniki grupowania agentów OfficeScan

- Nazwa pliku: `ofcdebug.log`
- Nazwa pliku: `ofcserver.ini`

  Lokalizacja: <*Folder instalacji serwera*>\PCCSRV\Private\
- Nazwa pliku: `SortingRule.xml`

  Lokalizacja: <Folder instalacji serwera>\PCCSRV\Private\SortingRuleStore\
- Nazwy plików:
  - `dbADScope.cdx`
  - `dbADScope.dbf`

  Lokalizacja: <Folder instalacji serwera>\HTTPDB\

Dzienniki aktualizacji składników

Nazwa pliku: `TmuDump.txt`

Lokalizacja: <*Folder instalacji serwera*>\PCCSRV\Web\Service\AU_Data\AU_Log

Uzyskiwanie szczegółowych informacji o aktualizacji klienta

Procedura

1. Utwórz plik o nazwie `aucfg.ini` z następującą zawartością:

```
[Debug]

level=-1

[Downloader]

ProxyCache=0
```

2. Zapisz plik w lokalizacji <*Folder instalacji serwera*>`PCCSRV\Web\Service`.
3. Ponownie uruchom OfficeScan Master Service.

Zatrzymywanie zbierania szczegółowych informacji o aktualizacji serwera

Procedura

1. Usuń plik `aucfg.ini`.
2. Ponownie uruchom OfficeScan Master Service.

Dzienniki narzędzia Agent Packager

Włączanie funkcji rejestracji przy tworzeniu elementu Agent Packager

Procedura

1. Zmodyfikuj plik `ClnExtor.ini` w lokalizacji <*Folder instalacji serwera*>`\PCCSRV\Admin\Utility\ClientPackager` w następujący sposób:

```
[Common]

DebugMode=1
```

2. Sprawdź plik `ClnPack.log` w lokalizacji `C:\`.

Wyłączanie funkcji rejestracji przy tworzeniu elementu Agent Packager

Procedura

1. Otwórz plik `ClnExtor.ini`.
2. Zmień wartość pozycji „DebugMode” z 1 na 0.

Dzienniki raportu zgodności z zabezpieczeniami

Aby otrzymać szczegółowe informacje na temat zgodności z zabezpieczeniami, należy zebrać:

- Nazwa pliku: `RBAUserProfile.ini`

  Lokalizacja: < *Folder instalacji serwera*>`\PCCSRV\Private\AuthorStore\`

- Wszystkie pliki w lokalizacji `<Folder instalacji serwera>\PCCSRV\Log \Security Compliance Report`.
- *Dzienniki serwera OfficeScan na stronie 18-3*

Dzienniki zarządzania serwerem zewnętrznym

- Nazwa pliku: `ofcdebug.log`
- Nazwa pliku: `ofcserver.ini`

  Lokalizacja: <*Folder instalacji serwera*>`\PCCSRV\Private\`
- Wszystkie pliki w lokalizacji `<Folder instalacji serwera>\PCCSRV\Log \Outside Server Management Report\`.
- Nazwy plików:
  - `dbADScope.cdx`

- `dbADScope.dbf`
- `dbClientInfo.cdx`
- `dbclientInfo.dbf`

Lokalizacja: `<Folder instalacji serwera>\HTTPDB\`

Dzienniki wykluczeń kontroli urządzeń

Aby otrzymać szczegółowe informacje na temat wyjątków kontroli urządzeń, należy zebrać:

- Nazwa pliku: `ofcscan.ini`

  Lokalizacja: < *Folder instalacji serwera*>\

- Nazwa pliku: `dbClientExtra.dbf`

  Lokalizacja: `<Folder instalacji serwera>\HTTPDB\`

- Lista wyjątków kontroli urządzeń z konsoli Web programu OfficeScan.

Dzienniki Web Reputation zintegrowanego serwera Smart Protection

Nazwa pliku: `diagnostic.log`

Lokalizacja: <*Folder instalacji serwera*>`\PCCSRV\LWCS\`

Dzienniki narzędzia ServerProtect Normal Server Migration

Aby włączyć funkcję rejestracji w dzienniku diagnostycznym dla narzędzia ServerProtect Normal Server Migration Tool:

Procedura

1. Utwórz plik o nazwie `ofcdebug.ini` z następującą zawartością:

   ```
   [Debug]

   DebugLog=C:\ofcdebug.log

   DebugLevel=9
   ```

2. Zapisz plik w lokalizacji `C:\`.

3. Sprawdź plik `ofcdebug.log` na dysku `C:\`.

Uwaga

Aby wyłączyć tworzenie dzienników diagnostycznych, należy usunąć plik `ofcdebug.ini`.

Dzienniki VSEncrypt

Program OfficeScan automatycznie tworzy dziennik diagnostyczny (`VSEncrypt.log`) w katalogu tymczasowym konta użytkownika. Na przykład `C:\Documents and Settings\<Nazwa użytkownika>\Local Settings\Temp`.

Dzienniki agenta Control Manager MCP Agent

Debuguj pliki w lokalizacji <*Folder instalacji serwera*>`\PCCSRV\CMAgent`.

- `Agent.ini`
- `Product.ini`
- Zrzut ekranu strony Ustawienia programu Control Manager
- `ProductUI.zip`

Włączanie rejestracji w dzienniku diagnostycznym w agencie MCP

Procedura

1. Zmodyfikuj plik `product.ini` w lokalizacji <*Folder instalacji serwera*>`\PCCSRV\CmAgent` w sposób następujący:

```
[Debug]

debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. Ponownie uruchom usługę OfficeScan Control Manager Agent z poziomu konsoli Microsoft Management Console.

3. Sprawdź plik `CMAgent_debug.log` w lokalizacji `C:\`.

Wyłączanie rejestracji w dzienniku diagnostycznym w agencie MCP

Procedura

1. Otwórz plik `product.ini` i usuń następujące elementy:

```
debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. Ponownie uruchom usługę OfficeScan Control Manager.

Dzienniki wirusów/złośliwego oprogramowania

Nazwa pliku:

- `dbVirusLog.dbf`
- `dbVirusLog.cdx`

Lokalizacja: <*Folder instalacji serwera*>`\PCCSRV\HTTPDB\`

Dzienniki spyware/grayware

Nazwa pliku:

- `dbSpywareLog.dbf`
- `dbSpywareLog.cdx`

Lokalizacja: <*Folder instalacji serwera*>`\PCCSRV\HTTPDB\`

Dzienniki epidemii

TYP DZIENNIKA	PLIK
Dzienniki bieżącego stanu epidemii naruszenia zapory	Nazwa pliku: `Cfw_Outbreak_Current.log` Lokalizacja: <*Folder instalacji serwera*>`\PCCSRV\Log\`
Dzienniki poprzedniego stanu epidemii naruszenia zapory	Nazwa pliku: `Cfw_Outbreak_Last.log` Lokalizacja: <*Folder instalacji serwera*>`\PCCSRV\Log\`
Dzienniki bieżącej epidemii wirusów/złośliwego oprogramowania	Nazwa pliku: `Outbreak_Current.log` Lokalizacja: <*Folder instalacji serwera*>`\PCCSRV\Log\`

TYP DZIENNIKA	PLIK
Dzienniki poprzedniej epidemii wirusów/ złośliwego oprogramowania	Nazwa pliku: `Outbreak_Last.log` Lokalizacja: <*Folder instalacji serwera*>`\PCCSRV\Log\`
Bieżące dzienniki epidemii spyware/grayware	Nazwa pliku: `Spyware_Outbreak_Current.log` Lokalizacja: <*Folder instalacji serwera*>`\PCCSRV\Log\`
Poprzednie dzienniki epidemii spyware/grayware	Nazwa pliku: `Spyware_Outbreak_Last.log` Lokalizacja: <*Folder instalacji serwera*>`\PCCSRV\Log\`

Dzienniki Virtual Desktop Support

- Nazwa pliku: `vdi_list.ini`

  Lokalizacja: <*Folder instalacji serwera*>`\PCCSRV\TEMP\`

- Nazwa pliku: `vdi.ini`

  Lokalizacja: `<Folder instalacji serwera>\PCCSRV\Private\`

- Nazwa pliku: `ofcdebug.txt`

  Lokalizacja: `<Folder instalacji serwera>\PCCSRV\`

Aby wygenerować plik `ofcdebug.txt`, włącz funkcję rejestracji w dzienniku diagnostycznym. Instrukcje dotyczące włączania rejestracji w dzienniku diagnostycznym opisano w temacie *Włączanie rejestracji w dzienniku diagnostycznym na stronie 18-4*.

Dzienniki agenta OfficeScan

Z dzienników agenta OfficeScan (na przykład dzienników diagnostycznych) można korzystać podczas rozwiązywania problemów związanych z agentami OfficeScan.

OSTRZEŻENIE!

Dzienniki diagnostyczne mogą zmniejszyć wydajność agenta i zajmować wiele miejsca na dysku. Tworzenie dzienników diagnostycznych należy włączać wyłącznie w razie konieczności i szybko wyłączyć tę opcję, kiedy tylko dane diagnostyczne przestaną być potrzebne. Dziennik diagnostyczny należy usunąć, jeżeli plik osiągnie duży rozmiar.

Tworzenie dzienników diagnostycznych agenta OfficeScan z wykorzystaniem pliku LogServer.exe

Aby włączyć funkcję rejestracji w dzienniku diagnostycznym dla agenta OfficeScan:

Procedura

1. Utwórz plik o nazwie `ofcdebug.ini` z następującą zawartością:

```
[Debug]

Debuglog=C:\ofcdebug.log

debuglevel=9

debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

2. Wyślij plik `ofcdebug.ini` do użytkowników z informacją, że należy zapisać go w lokalizacji `C:\`.

Uwaga

Program `LogServer.exe` jest automatycznie uruchamiany po każdym uruchomieniu punktu końcowego agenta OfficeScan. Poleć użytkownikom, aby NIE zamykali okna polecenia LogServer.exe otwierającego się podczas uruchamiania punktu końcowego, ponieważ sprawia to, że program OfficeScan zatrzymuje rejestrację diagnostyki. W przypadku zamknięcia okna poleceń można ponownie rozpocząć rejestrację debugowania w dzienniku, uruchamiając plik `LogServer.exe` z lokalizacji <*Folder instalacji agenta*>.

3. W przypadku każdego punktu końcowego agenta OfficeScan obecność pliku ofcdebug.log można sprawdzić w lokalizacji C:\.

Uwaga

Aby wyłączyć tworzenie dzienników diagnostycznych na agencie OfficeScan, należy usunąć plik `ofcdebug.ini`.

Dzienniki świeżej instalacji

Dla instalacji pakietu MSI:

- Nazwa pliku: `OFCNT.LOG`
- Lokalizacja: <*Folder instalacji agenta*>

Dla instalacji sieci Web:

- Nazwa pliku: `WebInstall.log`
- Lokalizacja: `C:\`

Dla instalacji zdalnych:

- Nazwa pliku: `OFCNT.LOG`
- Lokalizacja: `C:\`

Dla instalacji pakietu Autopcc i EXE:

- Nazwa pliku: `OFCNT.LOG`

- Lokalizacja: <*Folder instalacji agenta*>`%windir%\`

Dzienniki aktualizacji/poprawek

Nazwa pliku: `upgrade_rrrrmmddhhmmss.log`

Lokalizacja: <*Folder instalacji agenta*>`\Temp`

Dzienniki Usługi Usuwania Szkód Services

Włączanie funkcji rejestracji w dzienniku diagnostycznym Usługi Usuwania Szkód Services

---

Procedura

1. Otwórz plik `TSC.ini` w lokalizacji <*Folder instalacji agenta*>.
2. Zmodyfikuj poniższą linię w następujący sposób:

   `DebugInfoLevel=5`
3. Sprawdź plik `TSCDebug.log` w lokalizacji `<Folder instalacji agenta>\debug`.

Wyłączanie funkcji rejestracji w dzienniku diagnostycznym Usługi Usuwania Szkód Services

Otwórz plik `TSC.ini` i zmień wartość „`DebugInfoLevel`” z 5 na 0.

Dziennik Usługi Usuwania Szkód

Nazwa pliku: `rrrrmmdd.log`

Lokalizacja: <*Folder instalacji agenta*>`\report\`

Dzienniki programu Mail Scan

Nazwa pliku: `SmolDbg.txt`

Lokalizacja: <*Folder instalacji agenta*>

Dzienniki połączeń agentów OfficeScan

Nazwa pliku: `Conn_RRRRMMDD.log`

Lokalizacja: <*Folder instalacji agenta*>`\ConnLog`

Dzienniki aktualizacji agenta OfficeScan

Nazwa pliku: `Tmudump.txt`

Lokalizacja: <*Folder instalacji agenta*>`\AU_Data\AU_Log`

Uzyskiwanie szczegółowych informacji o aktualizacji agenta OfficeScan

Procedura

1. Utwórz plik o nazwie `aucfg.ini` z następującą zawartością:

   ```
   [Debug]

   level=-1

   [Downloader]

   ProxyCache=0
   ```

2. Zapisz plik w lokalizacji <*Folder instalacji agenta*>.

3. Załaduj ponownie Agent OfficeScan.

Uwaga

Zatrzymaj zbieranie szczegółowych informacji o aktualizacji agenta, usuwając plik `aucfg.ini` i przeładowując agenta OfficeScan.

Dzienniki silnika skanowania antywirusowego

Aby włączyć funkcję rejestracji w dzienniku diagnostycznym dla narzędzia Silnik skanowania wirusów:

Procedura

1. Otwórz Edytor rejestru (`regedit.exe`).
2. Przejdź do klucza `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters`.
3. Zmień wartość „`DebugLogFlags`” na „`00003eff`”.
4. Wykonaj czynności, w wyniku których wystąpił błąd skanowania.
5. Sprawdź plik `TMFilter.log` w lokalizacji `%windir%`.

Uwaga

Wyłącz rejestrowanie w dzienniku diagnostycznym, ustawiając wartość „`DebugLogFlags`” na „`00000000`”.

Dzienniki ochrony przed epidemią wirusów

Nazwa pliku: `OPPLogs.log`

Lokalizacja: <*Folder instalacji agenta*>`\OppLog`

Dzienniki ochrony przed epidemią wirusów/przywracania

Nazwy plików:

- `TmOPP.ini`
- `TmOPPRestore.ini`

Lokalizacja: <*Folder instalacji agenta*>\

Dzienniki diagnostyczne monitorowania zachowania

Aby włączyć funkcję rejestracji w dzienniku diagnostycznym dla monitorowania zachowania:

Procedura

1. Otwórz Edytor rejestru (`regedit.exe`).
2. Przejdź do klucza `HKLM\SOFTWARE\TrendMicro\Aegis`.
3. Zmień wartość „`DebugLogFlags`” na „`dword:00000032`”.
4. Wykonaj czynności, w wyniku których wystąpił błąd.
5. Sprawdź następujące dzienniki w folderze `C:\Program Files (x86)\Trend Micro\BM\log\`:
   - `TmCommengrrrrmmdd_nn.log`
   - `TMPEMrrrrmmdd_nn.log`

Dzienniki zapory OfficeScan

Włączanie funkcji rejestracji debugowania w dzienniku ogólnego sterownika zapory na komputerach z systemem Windows Vista/Server 2008/7/Server 2012/8/8.1/10

Procedura

1. Zmień następujące klucze/wartości rejestru:

KLUCZE REJESTRU	WARTOŚCI
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmwfp\Parameters	Typ: wartość DWORD (REG_DWORD) Nazwa: DebugCtrl Wartość: 0x00001111
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmlwf\Parameters	Typ: wartość DWORD (REG_DWORD) Nazwa: DebugCtrl Wartość: 0x00001111

2. Uruchom ponownie agenta.
3. Sprawdź pliki `wfp_log.txt` i `lwf_log.txt` w lokalizacji `C:\`.

Włączanie funkcji rejestracji w dzienniku diagnostycznym ogólnego sterownika zapory na komputerach z systemem Windows XP lub Windows Server 2003

Procedura

1. Dodaj następujące dane w kluczu `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmcfw\Parameters`:
   - Typ: wartość `DWORD (REG_DWORD)`
   - Nazwa: `DebugCtrl`
   - Wartość: `0x00001111`
2. Uruchom ponownie agenta.
3. Sprawdź plik `cfw_log.txt` w lokalizacji `C:\`.

Wyłączanie rejestracji w dzienniku diagnostycznym w module Ogólny sterownik zapory (wszystkie systemy operacyjne)

Procedura

1. Usuń plik „`DebugCtrl`” w kluczu rejestru.
2. Uruchom ponownie agenta.

Włączanie rejestracji w dzienniku diagnostycznym w module usługi zapory OfficeScan NT

Procedura

1. Zmodyfikuj plik `TmPfw.ini` w lokalizacji <*Folder instalacji agenta*> w następujący sposób:

   ```
   [ServiceSession]

   Enable=1
   ```

2. Załaduj ponownie agent.
3. Sprawdź plik `ddmmyyyy_NSC_TmPfw.log` w katalogu `C:\temp`.

Wyłączanie rejestracji w dzienniku diagnostycznym w module usługi zapory OfficeScan NT

Procedura

1. Otwórz plik `TmPfw.ini` i zmień wartość `Enable` z 1 na 0.
2. Załaduj ponownie Agent OfficeScan.

Dzienniki usługi Web Reputation i usługi skanowania poczty POP3

Włączanie funkcji rejestracji w dzienniku diagnostycznym dla usługi Web Reputation i Skanowanie poczty POP3

Procedura

- W przypadku agentów działających w systemie Windows Vista lub Windows Server 2008:

  a. Zmodyfikuj plik `TmProxy.ini` w lokalizacji <*folder instalacji agenta*> w następujący sposób:

  ```
  [InteractiveSession]

  Enable=1

  LogFolder=C:\temp

  [ServiceSession]

  Enable=1

  LogFolder=C:\temp
  ```

  b. Załaduj ponownie Agent OfficeScan.

  c. Sprawdź plik `ddmmyyyy_NSC_TmProxy.log` w katalogu `C:\temp`.

- W przypadku agentów działających w innych wersjach systemu Windows:

  a. Zmodyfikuj plik `TmOsprey.ini` w lokalizacji <*folder instalacji agenta*> w następujący sposób:

  ```
  [InteractiveSession]

  Enable=1

  LogFolder=C:\temp

  [ServiceSession]
  ```

```
Enable=1

LogFolder=C:\temp
```

b. Załaduj ponownie Agent OfficeScan.

c. Sprawdź plik `ddmmyyyy_NSC_TmProxy.log` w katalogu `C:\temp`.

Wyłączanie funkcji rejestracji w dzienniku diagnostycznym dla usługi Web Reputation i Skanowanie poczty POP3

Procedura

- W przypadku agentów działających w systemie Windows Vista lub Windows Server 2008:

  a. Zmodyfikuj plik `TmProxy.ini` w lokalizacji <*folder instalacji agenta*> w następujący sposób:

  ```
  [InteractiveSession]

  Enable=0

  LogFolder=C:\temp

  [ServiceSession]

  Enable=0

  LogFolder=C:\temp
  ```

  b. Załaduj ponownie Agent OfficeScan.

- W przypadku agentów działających w innych wersjach systemu Windows:

  a. Zmodyfikuj plik `TmOsprey.ini` w lokalizacji <*folder instalacji agenta*> w następujący sposób:

  ```
  [InteractiveSession]

  Enable=0
  ```

```
LogFolder=C:\temp

[ServiceSession]

Enable=0

LogFolder=C:\temp
```

b. Załaduj ponownie Agent OfficeScan.

Dzienniki listy wyjątków kontroli urządzeń

Nazwa pliku: `DAC_ELIST`

Lokalizacja: <*Folder instalacji agenta*>\

Dzienniki diagnostyczne Ochrona danych

Aby włączyć dzienniki diagnostyczne Ochrona danych:

Procedura

1. Uzyskaj plik `logger.cfg` od dostawcy usług obsługi technicznej.
2. Dodaj następujące dane w kluczu `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`:
   - Typ: `ciąg`
   - Nazwa: `debugcfg`
   - Wartość: `C:\Log\logger.cfg`
3. Utwórz folder o nazwie "Log" w katalogu `C:\`.
4. Skopiuj plik `logger.cfg` do folderu `Log`.
5. Zastosuj ustawienia ochrony przed utratą danych oraz kontroli urządzeń z poziomu konsoli Web, aby rozpocząć pobieranie informacji dla dzienników.

Uwaga

Wyłącz rejestrowanie diagnostyki w module Ochrona danych, usuwając pozycję `debugcfg` z klucza rejestru i uruchamiając ponownie punkt końcowy.

Dziennik zdarzeń systemu Windows

Program Podgląd zdarzeń systemu Windows rejestruje zdarzenia dotyczące działania aplikacji, takie jak logowanie czy zmiana ustawień konta.

Procedura

1. Kliknij jedną z poniższych opcji:
   - Kliknij **Początek** > **Panel sterowania** > **Wydajność i konserwacja** > **Narzędzia administracyjne** > **Zarządzanie komputerem**.
   - Otwórz konsolę MMC, w której znajduje się przystawka Podgląd zdarzeń.
2. Kliknij pozycję **Dziennik zdarzeń**.

Dzienniki narzędzia Transport Driver Interface (TDI)

Aby włączyć dzienniki narzędzia Transport Driver Interface (TDI):

Procedura

1. Dodaj następujące dane w kluczu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\Parameters`:

PARAMETR	WARTOŚCI
Klucz 1	Typ: wartość `DWORD (REG_DWORD)` Nazwa: `Debug` Wartość: `1111 (szesnastkowa)`

PARAMETR	WARTOŚCI
Klucz 2	Typ: `wartość String (REG_SZ)` Nazwa: `LogFile` Wartość: `C:\tmtdi.log`

2. Uruchom ponownie agenta.
3. Sprawdź plik `tmtdi.log` w lokalizacji `C:\`.

Uwaga

Wyłącz rejestrowanie w dzienniku diagnostycznym modułu TDI, usuwając pozycje `Debug` i `LogFile` z klucza rejestru i uruchamiając ponownie punkt końcowy.

Rozdział 19

Pomoc techniczna

W tym rozdziale omówiono następujące zagadnienia:

Zasoby dotyczące rozwiązywania problemów

Przed skontaktowaniem się z działem pomocy technicznej warto rozważyć skorzystanie z następujących zasobów online firmy Trend Micro.

Korzystanie z portalu pomocy technicznej

Portal pomocy technicznej firmy Trend Micro Support jest stale czynnym zasobem sieciowym zawierającym najbardziej aktualne informacje dotyczące typowych i nietypowych problemów.

Procedura

1. Przejdź do witryny http://esupport.trendmicro.com.
2. Wybierz jeden z dostępnych produktów lub kliknij odpowiedni przycisk, aby poszukać rozwiązań.
3. Użyj pola **Search Support** (Przeszukaj pomoc techniczną), aby znaleźć dostępne rozwiązania.
4. Jeśli rozwiązanie nie zostanie znalezione, kliknij przycisk **Kontakt z pomocą techniczną** i wybierz rodzaj potrzebnej pomocy.

Porada

Aby przesłać zgłoszenie przez Internet, odwiedź stronę o następującym adresie URL:

http://esupport.trendmicro.com/srf/SRFMain.aspx

Pracownik działu pomocy technicznej firmy Trend Micro Support zbada zgłoszenie i udzieli odpowiedzi w ciągu 24 godzin lub szybciej.

Encyklopedia zagrożeń

Większość dzisiejszego złośliwego oprogramowania to zagrożenia hybrydowe, które łączą co najmniej dwie technologie w celu ominięcia protokołów bezpieczeństwa

komputera. Firma Trend Micro zwalcza takie złożone złośliwe oprogramowanie przy użyciu produktów, które tworzą niestandardową strategię ochrony. Encyklopedia zagrożeń zapewnia wszechstronną listą nazw i objawów różnych zagrożeń hybrydowych, włącznie ze znanym złośliwym oprogramowaniem, spamem, złośliwymi adresami URL i znanymi lukami w zabezpieczeniach.

Odwiedź stronę http://about-threats.trendmicro.com/us/threatencyclopedia#malware, aby uzyskać następujące informacje:

- złośliwe oprogramowanie i mobilne kody złośliwe, które są obecnie na wolności lub aktywne;
- strony z informacjami o powiązanych zagrożeniach, które przedstawiają kompleksowo atak internetowy;
- poradniki poświęcone zagrożeniom internetowym, które przedstawiają ukierunkowane ataki i zagrożenia bezpieczeństwa;
- informacje o atakach internetowych i trendach online;
- cotygodniowe raporty o złośliwym oprogramowaniu.

Kontakt z firmą Trend Micro

W Stanach Zjednoczonych można skontaktować się z przedstawicielami firmy Trend Micro telefonicznie lub pocztą e-mail:

Adres	Trend Micro, Incorporated Trendd Micro (EMEA) Limited - Central Eastern Europe, Office in Warsaw Warsaw Trade Tower Floor 30, Chłodna 5100-867 Warszawa Irving, Texas 75062 Stany Zjednoczone
Telefon	Telefon: +1 (817) 569-8900 Bezpłatny: (888) 762-8736
Witryna internetowa	http://www.trendmicro.com

Adres e-mail	support@trendmicro.com

- Lista biur pomocy technicznej na całym świecie:

  http://www.trendmicro.pl/about/contact/index.html

- Dokumentacja produktu firmy Trend Micro:

  http://docs.trendmicro.com/pl-pl/home.aspx

Przyspieszanie przyjęcia zgłoszenia serwisowego

Aby usprawnić procedurę rozwiązywania problemów, należy przygotować następujące informacje:

- procedura odtworzenia problemu.
- informacje o urządzeniu lub sieci;
- Marka i model komputera oraz wszystkie dodatkowe podłączone urządzenia lub sprzęt
- ilość pamięci RAM i wolnego miejsca na dysku twardym;
- wersje systemu operacyjnego i dodatku Service Pack;
- Wersja zainstalowanego agenta
- Numer seryjny lub kod aktywacji
- szczegółowy opis środowiska instalacji;
- dokładny tekst komunikatu o błędzie.

Przesyłanie podejrzanej zawartości do firmy Trend Micro

Dostępnych jest wiele opcji przesyłania podejrzanej zawartości do firmy Trend Micro w celu przeprowadzenia dalszej analizy.

Usługi Email Reputation

Istnieje możliwość sprawdzenia reputacji określonego adresu IP i określenia agenta przesyłania wiadomości w celu dołączenia do globalnej listy dozwolonych:

https://ers.trendmicro.com/

Zapoznaj się z następującym wpisem Bazy wiedzy, aby wysłać próbki wiadomości do firmy Trend Micro:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

Usługi File Reputation Services

Zgromadź informacje systemowe i prześlij zawartość podejrzanego pliku do firmy Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Zanotuj numer zgłoszenia, aby można było je śledzić.

Usługi Web Reputation Services

Istnieje możliwość zapytania o ocenę bezpieczeństwa i typ zawartości adresu URL, odnośnie którego istnieje podejrzenie, że jest to witryna phishingowa lub inny tzw. „wektor infekcji" (celowo utworzone źródło zagrożeń internetowych, takich jak spyware i wirusy):

http://global.sitesafety.trendmicro.com/

Jeśli przypisana ocena jest nieprawidłowa, można wysłać prośbę o ponowne sklasyfikowanie do firmy Trend Micro.

Inne zasoby

W witrynie internetowej oprócz rozwiązań i pomocy technicznej dostępnych jest wiele innych pomocnych zasobów, które pozwalają uzyskać aktualne informacje oraz poznawać innowacje i najnowsze trendy dotyczące bezpieczeństwa.

Centrum pobierania

Od czasu do czasu firma Trend Micro może udostępnić poprawkę dla znanego problemu, który został zgłoszony, lub uaktualnienie określonego produktu albo usługi. Aby sprawdzić dostępność poprawek, odwiedź witrynę:

http://www.trendmicro.com/download/emea/?lng=emea

Jeśli poprawka nie została zastosowana (poprawki są oznaczone datą), otwórz plik Readme w celu sprawdzenia, czy poprawka ma zastosowanie do danego środowiska. Plik Readme zawiera także instrukcje instalacji.

Opinie o dokumentacji

Firma Trend Micro stara się zawsze ulepszać swoją dokumentację. W przypadku pytań, komentarzy lub sugestii dotyczących tego albo innego dokumentu firmy Trend Micro należy odwiedzić witrynę:

http://www.trendmicro.com/download/documentation/rating.asp

Dodatki

Załączniki

Dodatek A

Obsługa protokołu IPv6 w programie OfficeScan

Ten załącznik stanowi wymaganą lekturę dla użytkowników, którzy planują wdrożenie programu OfficeScan w środowisku obsługującym adresowanie IPv6. Zawarto tu informacje dotyczące obsługi protokołu IPv6 w programie OfficeScan.

Firma Trend Micro zakłada, że czytelnik jest już zaznajomiony z koncepcjami protokołu IPv6 i zadaniami związanymi z konfigurowaniem sieci obsługującej adresowanie IPv6.

Obsługa protokołu IPv6 dla serwera i agentów OfficeScan

Obsługa protokołu IPv6 została wprowadzona w programie OfficeScan w wersji 10.6. Wcześniejsze wersje programu OfficeScan nie obsługują adresowania IPv6. Obsługa protokołu IPv6 zostaje włączona automatycznie po zainstalowaniu lub zaktualizowaniu serwera OfficeScan i agentów OfficeScan spełniających wymagania protokołu IPv6.

Wymagania serwera OfficeScan

Poniżej przedstawiono wymagania protokołu IPv6 dotyczące serwera OfficeScan:

- Serwer musi być zainstalowany w systemie Windows Server 2008, Windows Server 2012 lub Windows Server 2016.
- Serwer musi używać serwera sieci Web programu IIS.
- Jeśli serwer ma zarządzać agentami IPv4 i IPv6, musi on mieć zarówno adres IPv4, jak i IPv6, a także być identyfikowany nazwą hosta. Jeśli serwer jest identyfikowany adresem IPv4, nie będzie możliwe nawiązanie połączenia między nim a agentami OfficeScan IPv6. Taka sama sytuacja zachodzi między agentami z protokołem IPv4 a serwerem identyfikowanym adresem IPv6.
- Jeśli serwer ma zarządzać tylko agentami IPv6, minimalnym wymaganiem jest posiadanie adresu IPv6. Serwer może być identyfikowany nazwą hosta lub adresem IPv6. Gdy serwer jest identyfikowany nazwą hosta, zalecane jest wprowadzenie pełnej nazwy (FQDN, Fully Qualified Domain Name). Wynika to z faktu, że w środowisku z samym protokołem IPv6 serwer WINS nie może wykonać translacji nazwy hosta na odpowiedni adres IPv6.

Uwaga

Nazwa FQDN może być podana tylko podczas wykonywania lokalnej instalacji na serwerze. W przypadku instalacji zdalnych podanie nazwy FQDN nie jest możliwe.

Wymagania agenta OfficeScan

Agent OfficeScan musi zostać zainstalowany w następujących systemach:

- Windows 7
- Windows Server 2008
- Windows Vista
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows 10
- Windows Server 2016

Zaleca się, aby Agent OfficeScan miał jednocześnie adresy IPv4 i IPv6, ponieważ niektóre obiekty, z którymi się łączy, obsługują tylko adresowanie IPv4.

Ograniczenia serwera wykorzystującego wyłącznie protokół IPv6

Poniższa tabela przedstawia ograniczenia serwera OfficeScan, który ma tylko adres IPv6.

TABELA A-1. Ograniczenia serwera wykorzystującego wyłącznie protokół IPv6

ELEMENT	OGRANICZENIE
Zarządzanie agentami	Serwer wykorzystujący wyłącznie protokół IPv6 nie może: • Instalować agentów OfficeScan na punktach końcowych wykorzystujących wyłącznie protokół IPv4. • Zarządzać agentami OfficeScan wykorzystującymi wyłącznie protokół IPv4.

Element	Ograniczenie
Aktualizacje i scentralizowane zarządzanie	Serwer wykorzystujący wyłącznie protokół IPv6 nie może wykonywać aktualizacji ze źródeł wykorzystujących wyłącznie protokół IPv4, takich jak: • Trend Micro ActiveUpdate Server • Dowolne niestandardowe źródło aktualizacji wykorzystujące wyłącznie protokół IPv4
Rejestracja, aktywacja i odnawianie produktu	Serwer wykorzystujący wyłącznie protokół IPv6 nie może połączyć się z serwerem Trend Micro Online Registration Server w celu zarejestrowania produktu, uzyskania licencji oraz aktywacji/odnowienia licencji.
Połączenie proxy	Serwer wykorzystujący wyłącznie protokół IPv6 nie może nawiązać połączenia za pośrednictwem serwera proxy wykorzystującego wyłącznie protokół IPv4.
Rozwiązania dodatków	Serwer wykorzystujący wyłącznie protokół IPv6 zawiera program Plug-in Manager, ale nie jest możliwa instalacja żadnych rozwiązań dodatków na następujących klientach: • Agenci OfficeScan lub hosty wykorzystujące wyłącznie protokół IPv4 (ze względu na brak bezpośredniego połączenia). • Agenci OfficeScan lub hosty wykorzystujące wyłącznie protokół IPv6, ponieważ żadne rozwiązania dodatków nie obsługują protokołu IPv6.

Większość tych ograniczeń można wyeliminować poprzez skonfigurowanie serwera proxy z dwoma stosami, który może wykonywać konwersję między adresami IPv4 i IPv6 (na przykład DeleGate). Serwer proxy należy umieścić między serwerem OfficeScan a obiektami, z którymi się łączy lub które obsługuje.

Ograniczenia Agent OfficeScan wykorzystującego wyłącznie protokół IPv6

Poniższa tabela przedstawia ograniczenia klienta Agent OfficeScan, który ma tylko adres IPv6.

TABELA A-2. Ograniczenia Agent OfficeScan wykorzystującego wyłącznie protokół IPv6

ELEMENT	OGRANICZENIE
Nadrzędny serwer OfficeScan	Nie jest możliwe zarządzanie klientami Agenci OfficeScan wykorzystującymi wyłącznie protokół IPv6 przez serwer OfficeScan, który wykorzystuje wyłącznie protokół IPv4.
Aktualizacje	Klient Agent OfficeScan wykorzystujący wyłącznie protokół IPv6 nie może wykonywać aktualizacji ze źródeł wykorzystujących wyłącznie protokół IPv4, takich jak: • Serwer Trend Micro ActiveUpdate Server • Serwer OfficeScan wykorzystujący wyłącznie protokół IPv4 • Agent aktualizacji wykorzystujący wyłącznie protokół IPv4 • Dowolne niestandardowe źródło aktualizacji wykorzystujące wyłącznie protokół IPv4
Żądania skanowania, zapytania usługi Web Reputation i funkcja Smart Feedback	Klient Agent OfficeScan wykorzystujący wyłącznie protokół IPv6 nie może wysyłać zapytań do źródeł Smart Protection, takich jak: • Serwer Smart Protection 2.0 (zintegrowany lub oddzielny) **Uwaga** Obsługa protokołu IPv6 została wprowadzona w wersji 2.5 serwera Smart Protection. • Sieć Trend Micro Smart Protection Network (także dla funkcji Smart Feedback)
Bezpieczeństwo oprogramowania	Klienty Agenci OfficeScan wykorzystujące wyłącznie protokół IPv6 nie mogą łączyć się z usługą Certified Safe Software Service obsługiwaną przez firmę Trend Micro.
Rozwiązania dodatków	Agenci OfficeScan wykorzystujący wyłącznie protokół IPv6 nie mogą instalować rozwiązań dodatków, ponieważ żadne rozwiązania dodatków nie obsługują protokołu IPv6.

ELEMENT	OGRANICZENIE
Połączenie proxy	Klient Agent OfficeScan wykorzystujący wyłącznie protokół IPv6 nie może nawiązać połączenia za pośrednictwem serwera proxy wykorzystującego wyłącznie protokół IPv4.

Większość tych ograniczeń można wyeliminować poprzez skonfigurowanie serwera proxy z dwoma stosami, który może wykonywać konwersję między adresami IPv4 i IPv6 (na przykład DeleGate). Serwer proxy należy umieścić między Agenci OfficeScan a obiektami, z którymi się łączą.

Konfigurowanie adresów IPv6

Konsola Web umożliwia skonfigurowanie adresu IPv6 lub zakresu adresów IPv6. Poniżej przedstawiono pewne wytyczne dotyczące konfiguracji.

- Program OfficeScan akceptuje standardowe postaci adresów IPv6.

  Na przykład:

  ```
  2001:0db7:85a3:0000:0000:8a2e:0370:7334
  ```

  ```
  2001:db7:85a3:0:0:8a2e:370:7334
  ```

  ```
  2001:db7:85a3::8a2e:370:7334
  ```

  ```
  ::ffff:192.0.2.128
  ```

- Program OfficeScan obsługuje także adresy IPv6 łącza lokalnego, takie jak:

  ```
  fe80::210:5aff:feaa:20a2
  ```

OSTRZEŻENIE!

Podczas określania adresu IPv6 należy zachować ostrożność, ponieważ w pewnych okolicznościach taki adres może nie działać w oczekiwany sposób, nawet jeśli zostanie zaakceptowany przez program OfficeScan. Na przykład agenty Agenci OfficeScan nie mogą wykonywać aktualizacji ze źródła aktualizacji, które znajduje się w innym segmencie sieci i jest identyfikowane przez adres IPv6 łącza lokalnego.

- Kiedy adres IPv6 stanowi część adresu URL, należy umieścić go w nawiasach kwadratowych ([]).
- Dla zakresów adresów IPv6 zwykle wymagany jest prefiks i jego długość. W konfiguracjach, które wymagają wyszukania adresów IP przez serwer, należy zastosować ograniczenia długości prefiksu, aby zapobiec problemom z wydajnością. Takie problemy mogą wystąpić, kiedy serwer wyszukuje znaczną liczbę adresów IP. Na przykład w przypadku funkcji Zarządzanie serwerem zewnętrznym prefiks może mieć długość tylko od 112 (65 536 adresów IP) do 128 (2 adresy IP).
- Niektóre ustawienia obejmujące adresy lub zakresy adresów IPv6 zostaną zainstalowane na agentach Agenci OfficeScan, ale agenty Agenci OfficeScan je zignorują. Jeśli na przykład skonfigurowano listę źródeł Smart Protection i umieszczono na niej Serwer Smart Protection zidentyfikowany za pomocą adresu IPv6, agenty Agenci OfficeScan wykorzystujące wyłącznie protokół IPv4 zignorują serwer i będą łączyć się z innymi źródłami Smart Protection.

Ekrany wyświetlające adresy IP

W tym temacie wymieniono miejsca w konsoli Web, w których wyświetlane są adresy IP.

LOKALIZACJA	OPIS
Drzewo agentów	We wszystkich miejscach, w których pojawia się drzewo agentów, adresy IPv6 Agenci OfficeScan wykorzystujących wyłącznie protokół IPv6 są wyświetlane w kolumnie **Adres IP**. W przypadku agentów OfficeScan z dwoma stosami ich adresy IPv6 są wyświetlane, jeśli do rejestracji na serwerze użyto adresu IPv6.<!--Agenci OfficeScan--> **Uwaga** Sterowanie adresem IP, który jest używany przez Agenci OfficeScan z dwoma stosami podczas rejestracji na serwerze, jest możliwe w sekcji **Agenci** > **Ustawienia agenta globalnego > Sieć** > **Preferowany adres IP**. Podczas eksportowania ustawień drzewa agentów do pliku adresy IPv6 są także widoczne w wyeksportowanym pliku.
Stan agenta	Szczegółowe informacje o agentach są dostępne po przejściu do sekcji **Agenci** > **Zarządzanie agentami > Stan**. Na tym ekranie widoczne są adresy IPv6 agentów OfficeScan wykorzystujących wyłącznie protokół IPv6 oraz agentów OfficeScan z dwoma stosami, którzy użyli swoich adresów IPv6 do rejestracji na serwerze.<!--Agenci OfficeScanAgenci OfficeScan-->
Dzienniki	Adresy IPv6 agentów z dwoma stosami i agentów OfficeScan wykorzystujących wyłącznie protokół IPv6 są wyświetlane w następujących dziennikach:<!--Agenci OfficeScan--> • Dzienniki wirusów/złośliwego oprogramowania • Dzienniki spyware/grayware • Dzienniki zapory • Dzienniki sprawdzania połączenia

Lokalizacja	Opis
Konsola programu Control Manager	Poniższa tabela przedstawia, które adresy IP serwera OfficeScan i Agenci OfficeScan są wyświetlane w konsoli programu Control Manager. • Serwer z dwoma stosami: IPv4 i IPv6 • Serwer wykorzystujący wyłącznie protokół IPv4: IPv4 • Serwer wykorzystujący wyłącznie protokół IPv6: IPv6 • Agent OfficeScan z dwoma stosami: Adres IP użyty podczas rejestracji agenta OfficeScan na serwerze OfficeScan <!--Agent OfficeScan--> • Agent OfficeScan wykorzystujący wyłącznie protokół IPv4: IPv4 • Agent OfficeScan wykorzystujący wyłącznie protokół IPv4: IPv6

Dodatek B

Obsługa systemu Windows Server Core

W tym dodatku przedstawiono obsługę programu OfficeScan w systemie Windows Server Core.

Obsługa systemu Windows Server Core

Windows Server Core to „minimalna” instalacja wersji systemu Windows Server. W systemie Server Core:

- Usunięto wiele opcji i funkcji systemu Windows Server.
- Serwer działa z użyciem znacznie bardziej ograniczonego podstawowego systemu operacyjnego.
- Zadania są wykonywane głównie z poziomu interfejsu wiersza polecenia.
- System operacyjny obsługuje mniejszą liczbę usług i wymaga mniej zasobów podczas uruchamiania.

Program OfficeScan obsługuje instalacje programu Agent OfficeScan w następujących wersjach systemu Windows Server Core:

- Windows Server Core 2008
- Windows Server Core 2008 R2
- Windows Server Core 2012
- Windows Server Core 2012 R2
- Windows Server Core 2016

Agent OfficeScan obsługuje system Server Core. Ta sekcja zawiera informacje dotyczące obsługi systemu Server Core.

Serwer OfficeScan nie obsługuje systemu Server Core.

Metody instalacji w systemie Windows Server Core

Następujące metody instalacji nie są obsługiwane lub są obsługiwane częściowo:

- Strona instalacyjna w sieci Web: ta metoda nie jest obsługiwana, ponieważ system Server Core nie zawiera przeglądarki Internet Explorer.

- Skaner narażenia na atak firmy Trend Micro: narzędzia Vulnerability Scanner nie można uruchomić lokalnie w systemie Server Core. Narzędzie można uruchomić na serwerze OfficeScan lub innym punkcie końcowym.

Obsługiwane są następujące metody instalacji:

- Instalacja zdalna. Szczegółowe informacje zawiera sekcja *Instalacja zdalna z konsoli Web programu OfficeScan na stronie 5-24*.
- Ustawienia skryptu logowania
- Agent Packager

Aby zainstalować agenta OfficeScan przy użyciu ustawień skryptu logowania

Procedura

1. Na docelowym punkcie końcowym otwórz wiersz polecenia.
2. Zmapuj położenie pliku `AutoPcc.exe` na serwerze OfficeScan za pomocą polecenia:

   ```
   net use <litera zmapowanego napędu> \\<nazwa hosta lub
   adres IP serwera OfficeScan>\ofcscan
   ```

   Na przykład:

   ```
   net use P: \\10.1.1.1\ofcscan
   ```

3. Podaj nazwę użytkownika i hasło dla docelowego serwera.

   Zostanie wyświetlony komunikat z informacją o powodzeniu mapowania pliku `AutoPcc.exe`.

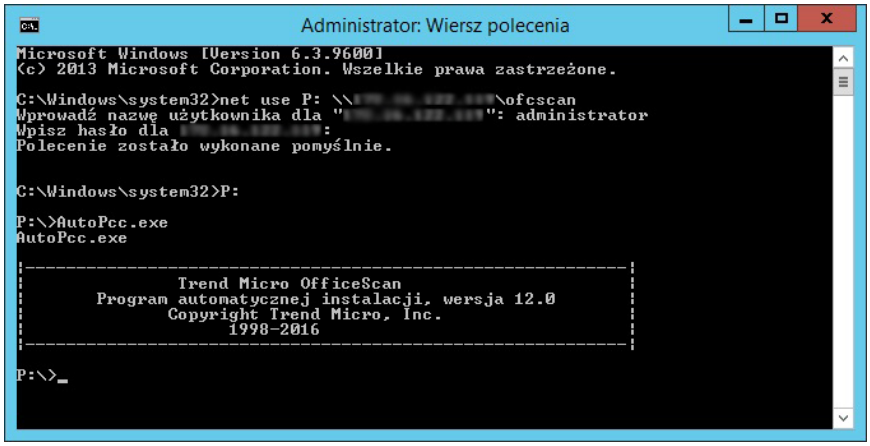
4. Wybierz położenie pliku `AutoPcc.exe`, wpisując literę zmapowanego dysku i dwukropek. Na przykład:

   ```
   P:
   ```

5. Wprowadź następujące polecenie, aby rozpocząć instalację:

`AutoPcc.exe`

Na poniższej grafice przedstawiono polecenia i wyniki w wierszu polecenia.



ILUSTRACJA B-1. Wiersz polecenia z informacją o sposobie instalacji agenta OfficeScan przy użyciu funkcji Ustawienia skryptu logowania.

Instalacja agenta OfficeScan przy użyciu pakietu agenta OfficeScan

Procedura

1. Utwórz pakiet.

   Szczegółowe informacje zawiera sekcja *Instalacja za pomocą programu Agent Packager na stronie 5-30*.

2. Otwórz wiersz polecenia.

3. Zmapuj położenie pakietu agenta OfficeScan za pomocą polecenia:

   `net use <litera zmapowanego dysku> \\<Lokalizacja pakietu agenta>`

Na przykład:

```
net use P: \\10.1.1.1\Package
```

Zostanie wyświetlony komunikat z informacją o powodzeniu mapowania pakietu agenta OfficeScan.

4. Wybierz położenie pakietu agenta OfficeScan, wpisując literę zmapowanego dysku i dwukropek. Na przykład:

   ```
   P:
   ```

5. Skopiuj pakiet agenta OfficeScan do katalogu lokalnego na punkcie końcowym ze środowiskiem Server Core, wpisując następujące polecenie:

   ```
   copy <nazwa pakietu agenta> <katalog na punkcie końcowym ze środowiskiem Server Core, do którego zostanie skopiowany pakiet>
   ```

   Na przykład:

   ```
   copy officescan.msi C:\Client Package
   ```

   Zostanie wyświetlony komunikat z informacją o powodzeniu kopiowania pakietu agenta OfficeScan.

6. Przejdź do katalogu lokalnego. Na przykład:

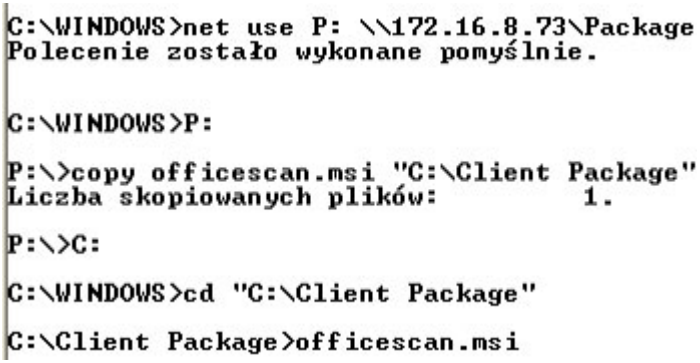
   ```
   C:
   ```

   ```
   cd C:\Client Package
   ```

7. Wpisz nazwę pliku pakietu, aby uruchomić instalację. Na przykład:

   ```
   officescan.msi
   ```

Na poniższej grafice przedstawiono polecenia i wyniki w wierszu polecenia.



ILUSTRACJA B-2. Wiersz polecenia z informacją o sposobie instalacji agenta OfficeScan przy użyciu pakietu agenta

Funkcje agenta OfficeScan w systemie Windows Server Core

Większość funkcji Agent OfficeScan, które są dostępne w systemie Windows Server 2008/2012/2016, będzie działać w systemie Server Core. Jedyną nieobsługiwaną funkcją jest tryb niezależny.

Listę funkcji dostępnych w systemie Windows Server 2008/2012/2016 zawiera temat *Funkcje agenta OfficeScan na stronie 5-3*.

Konsola agenta OfficeScan jest dostępna tylko z poziomu interfejsu wiersza polecenia.

Uwaga

Na niektórych ekranach konsoli agenta OfficeScan dostępny jest przycisk Pomoc, którego kliknięcie powoduje otwarcie pomocy kontekstowej opartej o kod HTML. Użytkownicy pracujący w systemie Windows Server Core 2008/2012/2016 nie będą mieć dostępu do Pomocy, ponieważ system ten nie posiada przeglądarki. Aby móc korzystać z pomocy, użytkownicy Ci będą musieli zainstalować przeglądarkę.

Polecenia systemu Windows Server Core

Zadania Agent OfficeScan można uruchamiać, wydając polecenia z poziomu interfejsu wiersza polecenia.

Aby wykonywać polecenia, należy przejść do lokalizacji pliku `PccNTMon.exe`. Ten proces jest odpowiedzialny za uruchamianie konsoli agenta OfficeScan. Proces ten można znaleźć w lokalizacji <*Folder instalacji agenta*>.

Poniższa tabela zawiera dostępne polecenia.

TABELA B-1. Polecenia systemu Windows Server Core

POLECENIE	OPERACJA
`pccnt <napęd lub ścieżka do folderu>`	Skanuje określony dysk lub folder w poszukiwaniu zagrożeń bezpieczeństwa Wytyczne: • Jeśli ścieżka do folderu zawiera spację, należy całą ścieżkę ująć w cudzysłów. • Skanowanie pojedynczych plików nie jest obsługiwane. Prawidłowe polecenia: • `pccnt C:\` • `pccnt D:\Files` • `pccnt "C:\Documents and Settings"` Nieprawidłowe polecenia: • `pccnt C:\Documents and Settings` • `pccnt D:\Files\example.doc`
`pccntmon -r`	Powoduje otwarcie narzędzia Monitorowanie w czasie rzeczywistym.
`pccntmon -v`	Przedstawia spis składników agenta wraz z ich wersjami
`pccntmon -u`	Aktualizuje komponenty produktu Agent OfficeScan

POLECENIE	OPERACJA
`pccntmon -n <hasło_zamknięcia>`	Zamyka program Agent OfficeScan Aby ponownie załadować agenta OfficeScan, wpisz następujące polecenie: `pccntmon`
`pccntmon -m <hasło_dezinstalacji>`	Odinstalowuje program Agent OfficeScan

POLECENIE	OPERACJA

`pccntmon -c`	Powoduje wyświetlenie następujących informacji w wierszu polecenia:
	• Metoda skanowania
	  • Smart scan
	  • Skanowanie standardowe
	• Stan sygnatur
	  • Zaktualizowane
	  • Nieaktualna
	• Usługa skanowania w czasie rzeczywistym
	  • Działa
	  • Wyłączony lub niedziałający
	• Stan połączenia agenta
	  • Online
	  • Tryb niezależny
	  • Offline
	• Usługi Web Reputation Services
	  • Dostępne
	  • Ponowne łączenie
	• Usługi File Reputation Services
	  • Dostępne
	  • Ponowne łączenie

`pccntmon -h`	Powoduje wyświetlenie wszystkich dostępnych poleceń.

Dodatek C

Obsługa systemów Windows 8/8.1/10 i Windows Server 2012/2016

W tym dodatku przedstawiono obsługę systemów Windows 8/8.1/10 i Windows Server 2012/2016 przez program OfficeScan.

Informacje o systemach Windows 8/8.1/10 i Windows Server 2012/2016

Systemy Windows 8/8.1 i Windows Server 2012/2016 udostępniają użytkownikom dwa typy trybów działania: tryb pulpitu i tryb interfejsu użytkownika systemu Windows. Użytkownicy systemu Windows 10 mogą wybrać tryb pulpitu lub tryb tabletu. Tryb pulpitu przypomina klasyczny ekran **startowy** systemu Windows.

Tryb użytkownika systemu Windows zapewnia użytkownikom nowy interfejs, który przypomina interfejs telefonów z systemem Windows. Nowe funkcje obejmują interfejs ekranu dotykowego z przewijaniem, kafelki oraz wyskakujące powiadomienia.

TABELA C-1. Kafelki i wyskakujące powiadomienia

ELEMENT STEROWANIA	OPIS
Kafelki	Kafelki przypominają ikony pulpitu używane we wcześniejszych wersjach systemu Windows. Użytkownik może kliknąć kafelek lub dotknąć go, aby uruchomić powiązaną aplikację. Aktywne kafelki zapewniają użytkownikom informacje specyficzne dla aplikacji, które są aktualizowane dynamicznie. Aplikacje mogą umieszczać informacje w kafelkach, nawet jeśli nie są uruchomione.
Wyskakujące powiadomienia	Wyskakujące powiadomienia przypominają komunikaty wyskakujące. Zapewniają one terminowe informacje na temat zdarzeń występujących podczas działania aplikacji. Wyskakujące powiadomienia pojawiają się na pierwszym planie, kiedy system Windows działa w trybie pulpitu lub wyświetla ekran blokady bądź kiedy działa inna aplikacja. **Uwaga** W zależności od aplikacji, wyskakujące powiadomienia mogą nie być wyświetlane na wszystkich ekranach lub trybach.

Obsługa kafelków i wyskakujących powiadomień przez program OfficeScan

Poniższa tabela przedstawia obsługę kafelków i wyskakujących powiadomień przez program OfficeScan w trybie interfejsu użytkownika systemu Windows.

TABELA C-2. Obsługa kafelków i wyskakujących powiadomień przez program OfficeScan

ELEMENT STEROWANIA	OBSŁUGA PRZEZ PROGRAM OFFICESCAN SUPPORT
Kafelki	Program OfficeScan udostępnia użytkownikom kafelek powiązany z programem agenta OfficeScan. Gdy użytkownik kliknie ten kafelek, system Windows przełącza się na tryb pulpitu i wyświetlany jest program agenta OfficeScan. **Uwaga** Program OfficeScan nie obsługuje aktywnych kafelków.
Wyskakujące powiadomienia	Program OfficeScan udostępnia następujące wyskakujące powiadomienia: • Wykryto podejrzany program • Skanowanie zaplanowane • Zagrożenie usunięte • Należy ponownie uruchomić komputer • Wykryto urządzenie pamięci masowej USB • Wykryto epidemię **Uwaga** Program OfficeScan wyświetla wyskakujące powiadomienia tylko w trybie interfejsu użytkownika systemu Windows.

Włączanie wyskakujących powiadomień w systemach Windows 8/8.1 i Windows Server 2012

Użytkownicy mogą włączyć wyświetlanie wyskakujących powiadomień, modyfikując **ustawienia komputera** na punkcie końcowym agenta OfficeScan. wymaga włączenia wyskakujących powiadomień przez użytkowników.

Procedura

1. Umieść wskaźnik myszy w prawym dolnym rogu ekranu, aby wyświetlić pasek **funkcji**.
2. Kliknij kolejno opcje **Ustawienia** > **Zmień ustawienia komputera**.

   Zostanie wyświetlony ekran **Ustawienia komputera**.
3. Kliknij opcję **Powiadomienia**.
4. W obszarze **Powiadomienia** ustaw następujące opcje na **Wł.**:
   - **Pokazuj powiadomienia aplikacji**
   - **Pokazuj powiadomienia aplikacji na ekranie blokady** (opcjonalnie)
   - **Odtwarzaj dźwięki powiadomień** (opcjonalnie)

Włączanie wyskakujących powiadomień w systemach Windows 10 i Windows Server 2016

Użytkownicy mogą włączyć wyświetlanie wyskakujących powiadomień, uzyskując dostęp do okna **Active Center** na punkcie końcowym Agent OfficeScan. Program OfficeScan wymaga od użytkowników włączenia wyskakujących powiadomień.

Procedura

1. Na pasku zadań kliknij ikonę powiadomień, a następnie opcję **Wszystkie ustawienia**.

2. Na ekranie Ustawienia kliknij pozycje **System** i **Powiadomienia i operacje**.

3. W sekcji **Powiadomienia** wybierz dla ustawienia **Pokaż powiadomienia aplikacji** wartość **Wł.**:

Obsługa funkcji programu OfficeScan według trybu interfejsu użytkownika

Tryb wykorzystywany przez użytkownika w systemie Windows 8/8.1 lub Windows Server 2012/2016 wpływa na przeglądarkę Internet Explorer 10 i jej nowsze wersje, a przez to na poziom obsługi zapewniany przez różne funkcje programu OfficeScan. Poniższa tabela przedstawia poziom wsparcia dla różnych funkcji programu OfficeScan w trybie pulpitu i trybie interfejsu użytkownika system Windows.

Uwaga

Niewymienione funkcje zapewniają pełne wsparcie w obu trybach działania systemu Windows.

TABELA C-3. Obsługa funkcji programu OfficeScan według trybu interfejsu użytkownika

FUNKCJA	TRYB PULPITU	INTERFEJS UŻYTKOWNIKA SYSTEMU WINDOWS
Konsola serwera Web	Pełna obsługa	Nieobsługiwane
Usługa Web Reputation	Pełna obsługa	Ograniczona obsługa • Skanowanie za pomocą protokołu HTTPS wyłączone
Zapora	Pełna obsługa	Ograniczona obsługa • Filtrowanie aplikacji wyłączone

Program Internet Explorer 10/11 i przeglądarka Microsoft Edge

Internet Explorer (IE) 10 to domyślna przeglądarka w systemach Windows 8/8.1 i Windows Server 2012. Przeglądarka Internet Explorer w wersji 10 i wyższej jest dostępna w dwóch różnych wersjach: jedna działa w interfejsie użytkownika systemu Windows, a druga w trybie pulpitu.

Microsoft Edge to domyślna przeglądarka w systemach Windows 10 i Windows Server 2016.

Uwaga

Skanowanie HTTPS jest wyłączone w przeglądarce Microsoft Edge, ponieważ nie obsługuje ona rozszerzeń za pomocą dodatków.

Przeglądarka Internet Explorer w wersji 10 i wyższej dla interfejsu użytkownika systemu Windows umożliwia przeglądanie Internetu bez użycia dodatków. Do tej pory programy dodatków dla przeglądarek internetowych nie przestrzegały żadnych ustalonych standardów, przez co jakość kodu używanego przez te dodatki mogła się różnić. Ponadto dodatki wymagają użycia dodatkowych zasobów systemowych i zwiększają ryzyko zarażenia złośliwym oprogramowaniem.

Firma Microsoft stworzyła przeglądarkę Internet Explorer w wersji 10 dla interfejsu użytkownika systemu Windows w celu stosowania nowych technologii opartych na standardach, które zastępują wcześniej stosowane rozwiązania dodatków. Poniższa tabela przedstawia listę technologii używanych przez przeglądarkę Internet Explorer w wersji 10 i wyższej zamiast starszej technologii dodatków.

Tabela C-4. Porównanie technologii opartych na standardach z programami dodatków

Możliwości	Technologia zgodna ze standardem W3C (World Wide Web)	Przykłady dodatków będących odpowiednikami
Wideo i audio	Wideo i audio HTML5	• Flash • Apple QuickTime • Silverlight
Grafika	• Kanwa HTML5 • Scalable Vector Graphics (SVG) • Przejścia i animacje CSS3 (Cascading Style Sheets, Level 3) • Transformacje CSS	• Flash • Apple QuickTime • Silverlight • Aplety Java
Magazynowanie offline	• Magazynowanie w Internecie • Interfejs API plików • IndexedDB • Interfejs API pamięci podręcznej aplikacji	• Flash • Aplety Java • Google Gears
Komunikacja sieciowa, udostępnianie zasobów, przesyłanie plików	• Wiadomości internetowe HTML • Cross-origin resource sharing (CORS)	• Flash • Aplety Java

Firma Microsoft stworzyła także przeglądarkę Internet Explorer w wersji 10 i wyższej zgodną z dodatkami, która jest przeznaczona wyłącznie dla trybu pulpitu. Jeśli użytkownicy w trybie interfejsu użytkownika systemu Windows napotkają witrynę internetową wymagającą użycia dodatkowych programów dodatków, w przeglądarce Internet Explorer w wersji 10 i wyższej pojawi się powiadomienie z monitem o przełączenie w tryb pulpitu. Po przejściu do trybu pulpitu użytkownicy mogą

wyświetlać witryny internetowe wymagające użycia lub instalacji programów dodatków innych firm.

Dodatek D

Przywracanie poprzedniej wersji programu OfficeScan

W tym dodatku przedstawiono obsługę przywracania poprzedniej wersji serwera i agenta OfficeScan.

Przywracanie poprzedniej wersji serwera Agenci OfficeScan i OfficeScan przy użyciu pakietu kopii zapasowej serwera

Procedura wycofywania programu OfficeScan obejmuje wycofanie agentów OfficeScan, a następnie wycofanie serwera OfficeScan.

Ważne

- Administratorzy mogą przywrócić serwer i agentów OfficeScan do poprzedniej wersji przy użyciu poniższej procedury tylko w przypadku, gdy administrator utworzył kopię zapasową serwera podczas procesu instalacji. Jeśli pliki kopii zapasowej serwera są niedostępne, należy sprawdzić procedury ręcznego przywracania w *Podręczniku instalacji oraz uaktualniania* dla wcześniej zainstalowanej wersji programu OfficeScan.
- Ta wersja programu OfficeScan umożliwia wycofanie tylko do następujących wersji programu OfficeScan:
  - OfficeScan 11.0 z dodatkiem Service Pack 1 i poprawką krytyczną
  - OfficeScan 11.0 z dodatkiem Service Pack 1
  - OfficeScan 11.0
  - OfficeScan 10.6 z dodatkiem Service Pack 3

Wycofywanie agentów OfficeScan

Program OfficeScan umożliwia przywrócenie Agenci OfficeScan tylko do tej samej wersji co przywracany serwer. Nie można przywrócić Agenci OfficeScan do wersji starszej niż wersja serwera.

Ważne

Przed przywróceniem serwera OfficeScan upewnij się, że przywrócono Agenci OfficeScan.

Procedura

1. Upewnij się, że Agenci OfficeScan nie umożliwiają uaktualnienia programu agenta.

   a. On the OfficeScan XG web console, go to **Agenci** > **Zarządzanie agentami**.

   b. Wybierz agentów OfficeScan do wycofania.

   c. Kliknij kartę **Ustawienia** > **Uprawnienia i inne ustawienia** > **Inne ustawienia**.

   d. Włącz opcję **Agenci OfficeScan mogą aktualizować składniki, ale nie mogą uaktualniać programu agenta ani instalować poprawek**.

2. On the OfficeScan XG web console, go to **Aktualizacje** > **Agenci** > **Źródło aktualizacji**.

3. Wybierz pozycję **Niestandardowe źródło aktualizacji**.

4. Kliknij przycisk **Dodaj** na liście **Niestandardowe źródło aktualizacji**.

   Zostanie wyświetlony nowy ekran.

5. Wpisz adresy IP agentów, którzy mają zostać wycofani do poprzedniej wersji.

6. Wpisz adres URL źródła aktualizacji.

   Na przykład:

   ```
   http://<adres IP serwera OfficeScan>:<port>/OfficeScan/download/Rollback
   ```

7. Kliknij przycisk **Zapisz**.

8. Kliknij polecenie **Powiadom wszystkich agentów**.

   Kiedy Agent OfficeScan, który ma zostać wycofany do poprzedniej wersji, wykona aktualizację ze źródła aktualizacji, Agent OfficeScan zostanie odinstalowany, a następnie zostanie zainstalowana poprzednia wersja agenta OfficeScan.

Porada

Administratorzy mogą przyspieszyć proces wycofywania, inicjując aktualizację ręczną na Agenci OfficeScan. Szczegółowe informacje zawiera sekcja *Ręczna aktualizacja agentów OfficeScan na stronie 6-47*.

9. Po zainstalowaniu poprzedniej wersji Agent OfficeScan poinformuj użytkowników o konieczności ponownego uruchomienia ich punktów końcowych.

   Po zakończeniu procesu wycofywania Agent OfficeScan będzie w dalszym ciągu podlegać temu samemu serwerowi OfficeScan.

Uwaga

Po wycofaniu agenta OfficeScan wszystkie składniki, łącznie z sygnaturami wirusów, także zostaną wycofane do poprzedniej wersji. Jeśli administratorzy nie wycofają serwera OfficeScan do poprzedniej wersji, wycofany Agent OfficeScan nie będzie mógł aktualizować składników. Administratorzy muszą zmienić źródło aktualizacji wycofanego agenta OfficeScan na standardowe, aby umożliwić dalsze wykonywanie aktualizacji składników.

Przywrócenie poprzedniej wersji serwera OfficeScan

Procedura przywracania serwera OfficeScan wymaga od administratora odinstalowania serwera OfficeScan XG, ponownego zainstalowania starszej wersji serwera, ręcznego zatrzymania usług systemu Windows, zaktualizowania rejestru systemu i zastąpienia plików serwera OfficeScan w katalogu instalacyjnym programu OfficeScan.

Ważne

Przed przywróceniem serwera OfficeScan upewnij się, że przywrócono do poprzedniej wersji Agenci OfficeScan.

Procedura

1. Odinstaluj serwer OfficeScan XG.
2. Zainstaluj poprzednią wersję serwera OfficeScan.

Porada

Firma Trend Micro nie zaleca zmiany nazwy hosta ani adresu IP podczas przywracania serwera.

Aby sprawdzić poprzednią wersję serwera, przejdź do lokalizacji <*Folder instalacji serwera*> i przejrzyj folder przywrócony podczas instalacji serwera OfficeScan XG. Nazwa folderu (wskazywana jako <Folder_wersji_do_przywrócenia>) może być jak poniżej:

- OSCE11_SP1: OfficeScan 11.0 z dodatkiem Service Pack 1
- OSCE11: OfficeScan 11.0
- OSCE106_SP3: OfficeScan 10.6 z dodatkiem Service Pack 3

3. Na komputerze serwera OfficeScan zatrzymaj następujące usługi:
   - Zapora ochrony przed intruzami (jeśli jest zainstalowana)
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - OfficeScan Active Directory Integration Service
   - OfficeScan Control Manager Agent
   - Narzędzie OfficeScan Plug-in Manager
   - OfficeScan Master Service
   - Usługa publikowania w sieci World Wide Web
4. Skopiuj wszystkie pliki i katalogi z lokalizacji `<Folder_instalacji_serwera>>\<Folder_wersji_do_przywrócenia>\` i zastąp pliki w lokalizacji `<Folder_instalacji_serwera>\PCCSRV\`.
5. Przywróć rejestr programu OfficeScan.
   a. Otwórz **Edytor rejestru** (`regedit.exe`).
   b. W lewym panelu nawigacji wybierz jeden z następujących kluczy rejestru:

- W systemach 32-bitowych: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service`
- W systemach 64-bitowych: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Officescan\service`

c. Wybierz kolejno opcje **Plik** > **Importuj...**.

d. Wybierz ogólny plik `.reg` serwera OfficeScan znajdujący się w lokalizacji `<Folder_instalacji_serwera>\<Folder_wersji_do_przywrócenia>\`.

Nazwa pliku rejestru jest w następującym formacie:

`RegBak_<Folder_wersji_do_przywrócenia>.reg`

e. Kliknij przycisk **Tak**, aby przywrócić wszystkie klucze poprzedniej wersji programu OfficeScan.

6. Opcjonalnie przywróć harmonogram tworzenia kopii zapasowej bazy danych.

a. Otwórz **Edytor rejestru** (`regedit.exe`).

b. W lewym panelu nawigacji wybierz jeden z następujących kluczy rejestru:

- W systemach 32-bitowych: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Database Backup`
- W systemach 64-bitowych: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Database Backup`

c. Wybierz kolejno opcje **Plik** > **Importuj...**.

d. Wybierz plik `.reg` bazy danych znajdujący się w lokalizacji `<Folder_instalacji_serwera>\<Folder_wersji_do_przywrócenia>\`.

Nazwa pliku rejestru jest w następującym formacie:

`RegBak_DBBak_<Folder_wersji_do_przywrócenia>.reg`

e. Kliknij przycisk **Tak**, aby przywrócić wszystkie klucze poprzedniej wersji programu OfficeScan.

7. Uruchom edytor wiersza polecenia (`cmd.exe`), a następnie wpisz następujące polecenia, aby zresetować licznik wydajności lokalnego serwera Web Classification Server:

   ```
   cd <folder instalacji serwera>\PCCSRV\LWCS

   regsvr32.exe /u /s perfLWCSPerfMonMgr.dll

   regsvr32.exe /s perfLWCSPerfMonMgr.dll
   ```

8. Uruchom ponownie następujące usługi:

   - Zapora ochrony przed intruzami (jeśli jest zainstalowana)
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - OfficeScan Active Directory Integration Service
   - OfficeScan Control Manager Agent
   - Narzędzie OfficeScan Plug-in Manager
   - OfficeScan Master Service
   - Apache 2 (jeśli używany jest serwer sieci Web Apache)
   - Usługa publikowania w sieci World Wide Web (jeśli używany jest serwer sieci Web IIS)

9. Wyczyść pamięć podręczną przeglądarki Internet Explorer i usuń ręcznie formanty ActiveX. Szczegółowe informacje dotyczące usuwania formantów ActiveX w przeglądarce Internet Explorer 9 można znaleźć na stronie http://windows.microsoft.com/en-us/internet-explorer/manage-add-ons#ie=ie-9.

   Ustawienia poprzedniej wersji serwera OfficeScan zostały przywrócone.

Porada

Administratorzy mogą potwierdzić pomyślne przywrócenie, sprawdzając numer wersji programu OfficeScan na ekranie **Informacje** (**Pomoc** > **Informacje**).

10. Opcjonalnie zarejestruj serwer OfficeScan na serwerze programu Control Manager, używając do tego celu konsoli Web.

11. Opcjonalnie zarejestruj serwer OfficeScan na serwerze Deep Discovery, używając do tego celu konsoli Web.

Uwaga

Integracja usług Deep Discovery z serwerem OfficeScan została wprowadzona w programie OfficeScan 10.6 z dodatkiem Service Pack 2.

12. Po potwierdzeniu pomyślnego wycofania programu OfficeScan usuń wszystkie pliki z lokalizacji `<Folder_instalacji_serwera>\<Folder_wersji_do przywrócenia>\`.

Dodatek E

Słownik

Pojęcia przedstawione w tym słowniku przedstawiają dalsze informacje o często używanych pojęciach związanych z punktami końcowymi oraz o produktach i technologiach firmy Trend Micro.

ActiveUpdate

Funkcja ActiveUpdate jest dostępna w wielu produktach Trend Micro. Połączona z witryną aktualizacji firmy Trend Micro funkcja ActiveUpdate pobiera przez Internet najnowsze pliki sygnatur wirusów, silniki skanowania, programy oraz pliki pozostałych składników produktu Trend Micro.

Skompresowany plik

Pojedynczy plik zawierający jeden lub wiele oddzielnych plików, a także informacje umożliwiające wyodrębnienie tych plików przy użyciu odpowiedniego programu, takiego jak WinZip.

Cookie

Mechanizm umożliwiający przechowywanie informacji o użytkowniku sieci Internet, takie jak nazwisko, preferencje i zainteresowania. Informacje są zapisywane w przeglądarce internetowej w celu ich przyszłego wykorzystania. Podczas kolejnego dostępu do witryny internetowej, w przypadku której przeglądarka przechowuje plik cookie, przeglądarka przesyła plik cookie na serwer sieci Web, gdzie jest on następnie używany do prezentowania indywidualnych stron internetowych. Można na przykład wyświetlić witrynę internetową, która rozpozna imię użytkownika.

Atak typu „odmowa usługi”

Atak typu „odmowa usługi” (DoS, Denial of Service) to rodzaj ataku na punkt końcowy lub sieć powodujący utratę możliwości korzystania z usługi, czyli zablokowanie połączenia sieciowego. Typowe ataki typu DoS mają negatywny wpływ na przepustowość sieci i przeciążają zasoby punktu końcowego, takie jak pamięć.

DHCP

Protokół dynamicznej konfiguracji hosta (DHCP, Dynamic Host Control Protocol) to protokół, który dynamicznie przypisuje adresy IP urządzeniom w sieci. Dzięki dynamicznemu adresowaniu podczas każdorazowego łączenia się urządzenia z siecią można mu przypisywać różne adresy IP. W przypadku niektórych systemów adres IP urządzenia może się zmieniać również podczas trwania połączenia. Protokół DHCP obsługuje połączenie statycznych i dynamicznych adresów IP.

DNS

System nazw domen (DNS, Domain Name System) to przeznaczona do ogólnego zastosowania usługa zapytania danych wykorzystywana w sieci Internet do przekształcania nazw hostów na adresy IP.

Gdy agent DNS wysyła do serwera DNS żądanie uzyskania nazwy i adresu hosta, serwer inicjuje proces nazywany rozwiązywaniem. W przypadku podstawowej konfiguracji DNS serwer wykonuje domyślne rozwiązywanie. Na przykład zdalny serwer wysyła do innego serwera żądanie uzyskania danych zapisanych na komputerze w bieżącej strefie. Oprogramowanie agenta na zdalnym serwerze wysyła żądanie do programu rozpoznawania nazw, który udziela odpowiedzi na podstawie plików bazy danych.

Nazwa domeny

Pełna nazwa systemu składająca się z nazwy hosta lokalnego i jego nazwy domeny, na przykład `tellsitall.com`. Nazwa domeny powinna być wystarczająca do określenia unikalnego adresu internetowego dowolnego hosta w Internecie. Proces ten nosi nazwę „rozpoznawanie nazw” i korzysta z systemu DNS (Domain Name System).

Dynamiczny adres IP

Dynamiczny adres IP jest przypisywany przez serwer DHCP. Adres MAC punktu końcowego pozostaje taki sam, jednak serwer DHCP może przypisać do punktu końcowego nowy adres IP w zależności od dostępności.

ESMTP

Protokół ESMTP (Enhanced Simple Mail Transport Protocol) obejmuje mechanizmy zabezpieczeń, uwierzytelnianie i inne, które pozwalają na oszczędzanie przepustowości i ochronę serwerów.

Umowa licencyjna użytkownika oprogramowania (EULA)

Umowa Licencyjna Użytkownika Oprogramowania lub EULA to prawna umowa pomiędzy wydawcą oprogramowania i użytkownikiem oprogramowania. Określa ona zazwyczaj ograniczenia, jakim podlega użytkownik. Użytkownik może nie zgodzić się na przystąpienie do umowy, nie klikając pozycji „Akceptuję" podczas instalacji. Kliknięcie pozycji „Nie akceptuję" powoduje oczywiście zakończenie procesu instalacji produktu.

Wielu użytkowników nieświadomie zgadza się na instalację spyware oraz innych typów grayware na swoich komputerach, klikając przycisk „Akceptuję" na monitach licencji EULA wyświetlanych podczas instalacji określonych, darmowych programów.

Fałszywe alarmy

Fałszywy alarm występuje w przypadku, gdy plik zostanie nieprawidłowo zidentyfikowany przez oprogramowanie zabezpieczające jako zarażony.

FTP

Protokół transferu plików (FTP, File Transfer Protocol) to standardowy protokół używany do przesyłania przez Internet plików z serwera do klienta. Więcej informacji można znaleźć w dokumentacji RFC 959 organizacji Network Working Group.

GeneriClean

Funkcja GeneriClean, znana także jako mechanizm czyszczenia referencyjnego, to nowa technologia czyszczenia wirusów i złośliwego oprogramowania działająca nawet w przypadku braku składników czyszczenia wirusów. Używając wykrytego pliku jako bazy, funkcja GeneriClean ustala, czy wykryty plik ma odpowiadający mu proces lub usługę w pamięci i rejestrze plików, a następnie usuwa je wszystkie.

Pakiet Hot Fix

Pakiet Hot fix to sugerowane rozwiązanie pojedynczego problemu zgłaszanego przez klienta. Pakiety hot fix są specyficzne dla danego problemu, dlatego nie są wydawane dla wszystkich klientów. Pakiety hot fix dla systemu Windows zawierają programy instalacyjne, natomiast w innych systemach zazwyczaj należy zatrzymać demony programów, skopiować plik (zastępując jego odpowiednik w instalacji) i ponownie uruchomić demony.

Domyślnie pakiety Hot Fix mogą być zainstalowane na agentach OfficeScan. Aby zrezygnować z instalowania pakietów Hot Fix na agentach OfficeScan, należy zmienić ustawienia aktualizacji agentów za pomocą konsoli Web, przechodząc do **Agenci** > **Zarządzanie agentami** i klikając kartę **Ustawienia** > **Uprawnienia i inne ustawienia** > **Inne ustawienia**.

Jeśli próba instalacji pakietu hot fix na serwerze OfficeScan zakończy się niepowodzeniem, do zmiany sygnatury czasowej pakietu hot fix należy użyć narzędzia Touch Tool. Spowoduje to, że program OfficeScan zinterpretuje plik pakietu hot fix jako nowy, dzięki czemu serwer spróbuje ponownie automatycznie zainstalować ten pakiet.

Szczegółowe informacje na temat tego narzędzia zawiera sekcja *Uruchamianie narzędzia Touch Tool dla pakietów Hot Fix agenta OfficeScan na stronie 6-56*.

HTTP

Protokół przesyłania dokumentów hipertekstowych (HTTP, Hypertext Transfer Protocol) to standardowy protokół używany do przesyłania przez Internet stron internetowych (łącznie z zawartością multimedialną i grafiką) z serwera do klienta.

HTTPS

Protokół Hypertext Transfer Protocol z zastosowaniem standardu Secure Socket Layer (SSL). HTTPS to odmiana protokołu HTTP używana do realizacji bezpiecznych transakcji.

ICMP

Sporadycznie brama lub host docelowy korzysta z protokołu komunikacyjnego sterowania Internetem (ICMP, Internet Control Message Protocol) do komunikacji z hostem źródłowym, na przykład aby zgłosić błąd w przetwarzaniu datagramu. Protokół ICMP jest oparty na obsłudze protokołu IP, jakby był protokołem wyższego poziomu, jednak jest właściwie integralną częścią protokołu IP realizowaną przez każdy moduł IP. Komunikaty ICMP wysyłane są w kilku sytuacjach: na przykład gdy datagram nie może osiągnąć przeznaczenia, gdy bufor bramy jest za mały do przekazania datagramu dalej i gdy brama może przekierować hosta do przesyłania ruchu krótszą drogą. Protokół IP nie jest całkowicie niezawodny. Celem tych komunikatów kontrolnych jest zapewnienie informacji zwrotnych na temat problemów w komunikacji, a nie usprawnienie protokołów IP.

IntelliScan

IntelliScan jest metodą identyfikacji plików do skanowania. Rzeczywisty typ plików wykonywalnych (np. `.exe`) jest określany na podstawie ich zawartości. Rzeczywisty typ

zawartości plików innych, niż wykonywalne (na przykład `.txt`), jest określany na podstawie nagłówka pliku.

Korzystanie z funkcji IntelliScan zapewnia następujące korzyści:

- Optymalizacja wydajności: Funkcja IntelliScan nie wpływa na aplikacje agent, ponieważ używa zasobów systemowych w minimalnym stopniu.
- Krótszy okres skanowania: Funkcja IntelliScan wykorzystuje identyfikację rzeczywistego typu plików i skanuje wyłącznie te pliki, które są podatne na zarażenie. Czas skanowania jest więc znacznie krótszy niż podczas skanowania wszystkich plików.

IntelliTrap

Autorzy wirusów często podejmują próby ominięcia zabezpieczeń antywirusowych, stosując algorytmy kompresji w czasie rzeczywistym. Funkcja IntelliTrap pomaga zmniejszyć ryzyko dostania się takich wirusów do sieci przez blokowanie plików wykonywalnych kompresowanych w czasie rzeczywistym i traktowanie ich na równi z innymi zagrożeniami ze strony złośliwego oprogramowania. Mechanizm IntelliTrap identyfikuje takie pliki jako zagrożenia bezpieczeństwa i może błędnie blokować bezpieczne pliki, dlatego zaleca się poddanie plików kwarantannie (nie należy ich usuwać ani czyścić) po włączeniu funkcji IntelliTrap. Jeżeli użytkownicy regularnie wymieniają się plikami wykonalnymi kompresowanymi w czasie rzeczywistym, mechanizm IntelliTrap należy wyłączyć.

Mechanizm IntelliTrap opiera się na następujących składnikach:

- Silnik skanowania antywirusowego
- Sygnatura IntelliTrap
- Sygnatura wyjątków IntelliTrap

IP

„Protokół internetowy (IP) umożliwia przesyłanie bloków danych zwanych datagramami z lokalizacji źródłowych do docelowych, przy czym lokalizacjami źródłową i docelową są hosty identyfikowane przez adresy o stałej długości". (RFC 791)

Plik Java

Java jest uniwersalnym językiem programowania opracowanym przez firmę Sun Microsystems. Plik Java zawiera kod języka Java. Język Java obsługuje programowanie Internetowe w postaci niezależnych od platformy „apletów". Aplet to program napisany w języku programowania Java, który można dołączyć do kodu strony HTML.
W przypadku wyświetlania strony zawierającej aplet w przeglądarce obsługującej technologię Java kod apletu jest przesyłany na punkt końcowy i wykonywany przez wirtualną maszynę Java przeglądarki.

LDAP

Protokół dostępu do usług katalogowych (LDAP, Lightweight Directory Access Protocol) to protokół aplikacji służący do przeszukiwania i modyfikowania usług katalogowych za pomocą protokołu TCP/IP.

Port nasłuchiwania

Port nasłuchiwania służy do obsługi żądań połączeń agenta dotyczących wymiany danych.

Agent MCP

Protokół Management Communication Protocol (MCP) firmy Trend Micro to jej agent nowej generacji dla zarządzanych produktów. Protokół MCP zastępuje usługę Trend

Micro Management Infrastructure (TMI) jako środek komunikacji programu Control Manager z programem OfficeScan. Protokół MCP ma kilka nowych funkcji:

- mniejsze obciążenie sieci i rozmiaru pakietu,
- obsługa przechodzenia translacji NAT i zapory,
- Obsługuje protokół HTTPS.
- Obsługuje komunikację jedno- i dwukierunkową.
- obsługa rejestracji jednokrotnej (SSO).
- Obsługuje węzeł klastra.

Atak ze strony zagrożeń mieszanych

Ataki ze strony zagrożeń mieszanych, takich jak np. „Nimda" czy „Code Red", wykorzystują wiele punktów wejść oraz miejsc narażonych na ataki, które znajdują się w sieciach korporacyjnych.

NAT

Mechanizm translacji adresu sieciowego (NAT, Network Address Translation) to standardowa metoda translacji bezpiecznych adresów IP na tymczasowe, zewnętrzne, zarejestrowane adresy IP z puli adresów. Dzięki mechanizmowi NAT zaufane sieci z przypisanymi prywatnymi adresami IP mogą uzyskać dostęp do sieci Internet. Oznacza to również, że nie ma konieczności uzyskania zarejestrowanego adresu IP dla każdego komputera znajdującego się w sieci.

NetBIOS

Sieciowy system podstawowych operacji wejścia/wyjścia (NetBIOS, Network Basic Input Output System) to interfejs programowania aplikacji (API), który wprowadza

dodatkowe funkcje, na przykład funkcje sieciowe, do systemu BIOS dyskowego systemu operacyjnego DOS (disk operating system).

Komunikacja jednokierunkowa

Translacja NAT stała się znacznie bardziej istotnym zagadnieniem w obecnym otoczeniu sieciowym świata rzeczywistego. W związku z tym protokół MCP umożliwia komunikację jednokierunkową. Komunikacja jednokierunkowa powoduje zainicjowanie połączenia agenta MCP z serwerem oraz odpytywanie poleceń z serwera. Każde żądanie jest zapytaniem polecenia podobnym do CGI lub transmisją dziennika. Aby zmniejszyć wpływ sieci, agent MCP utrzymuje aktywne połączenie i maksymalnie je otwiera. Kolejne żądanie wykorzystuje istniejące, otwarte połączenie. Gdy połączenie zostaje przerwane, wszystkie połączenia SSL z danym komputerem centralnym korzystają z pamięci podręcznej identyfikatorów sesji, co znacznie zmniejsza czas ponownego połączenia.

Poprawka

Poprawka to zestaw pakietów hot fix i poprawek zabezpieczeń rozwiązujących różne problemy dotyczące programów. Firma Trend Micro regularnie udostępnia poprawki. Poprawki dla systemu Windows zawierają program instalacyjny, poprawki dla pozostałych systemów zazwyczaj zawierają skrypt instalacyjny.

Ataki typu phish

Phish lub phishing to coraz częściej występująca forma oszustwa, polegająca na nakłanianiu użytkowników sieci Web do przekazania prywatnych informacji w witrynie naśladującej witrynę internetową znanej firmy.

W typowym scenariuszu użytkownik otrzymuje pilną (i wyglądającą na autentyczną) wiadomość e-mail z informacją o problemach z kontem, które trzeba rozwiązać, gdyż w przeciwnym wypadku konto zostanie zamknięte. Taka wiadomość e-mail zawiera adres URL do witryny internetowej wyglądającej identycznie jak autentyczna. Jest to

zwykła kopia firmowej wiadomości e-mail oraz witryny internetowej, ale przesyłającej wprowadzone przez użytkownika dane do osób trzecich.

Wiadomość e-mail zawiera monit o zalogowanie się w witrynie i potwierdzenie określonych informacji dotyczących konta. Haker uzyskuje od użytkownika dane, takie jak nazwa logowania, hasło, numer karty kredytowej lub numer ubezpieczenia.

Oszustwa typu phish można dokonać szybko, tanio i jest to łatwe. Może być również dosyć dochodowe dla dokonujących go przestępców. Oszustwo typu phish jest trudne do wykrycia nawet dla zaawansowanych użytkowników komputerów. Jest również trudne do wykrycia dla organów ścigania. Co gorsza, prawie niemożliwe jest jego ściganie prawne.

Każdą stronę, wobec której istnieje podejrzenie stosowania phishingu, należy zgłaszać firmie Trend Micro.

Ping

Ping to narzędzie, które wysyła żądanie echa ICMP do adresu IP i czeka na odpowiedź. Polecenie ping pozwala określić, czy punkt końcowy z określonym adresem IP jest aktualnie podłączony do sieci.

POP3

POP3 to standardowy protokół umożliwiający przechowywanie i przesyłanie wiadomości e-mail z serwera do aplikacji pocztowej klienta.

Serwer proxy

Serwer proxy to serwer internetowy, który odbiera adresy URL ze specjalnym prefiksem. Serwer proxy pobiera dokumenty z lokalnej pamięci podręcznej lub zdalnego serwera, a następnie zwraca adres URL do programu zgłaszającego żądanie.

RPC

Zdalne wywołanie procedury (RPC, Remote procedure call) to protokół sieciowy umożliwiający programowi uruchomionemu na hoście wykonanie kodu na innym hoście.

Poprawka zabezpieczeń

Poprawka zabezpieczeń koncentruje się na problemach zabezpieczeń i nadaje się do instalacji na wszystkich klientach. Poprawki zabezpieczeń dla systemu Windows zawierają program instalacyjny, poprawki dla pozostałych systemów zazwyczaj zawierają skrypt instalacyjny.

Dodatek Service Pack

Dodatek Service Pack to pełny zestaw pakietów hot fix, poprawek i istotnych ulepszeń funkcji, stanowiący uaktualnienie produktu. Dodatki Service Pack, przeznaczone zarówno dla systemu Windows, jak i pozostałych systemów operacyjnych, zawierają program instalacyjny oraz skrypt instalacyjny.

SMTP

Prosty protokół przesyłania poczty (SMTP, Simple Mail Transport Protocol) to standardowy protokół służący do przesyłania przez Internet wiadomości poczty elektronicznej z serwera do serwera i z agenta do serwera.

SNMP

Prosty protokół zarządzania siecią (SNMP, Simple Network Management Protocol) to protokół zapewniający możliwość monitorowania urządzeń sieciowych w celu wykrywania zdarzeń wymagających interwencji administratora.

Pułapka SNMP

Pułapka protokołu SNMP to metoda wysyłania powiadomień do administratorów sieci używających konsoli zarządzania obsługującej ten protokół.

W programie OfficeScan można przechowywać powiadomienia w bazach informacji zarządzania (MIB). Do wyświetlenia powiadomienia pułapki SNMP można użyć przeglądarki MIB.

SSL

Secure Socket Layer (SSL) to protokół opracowany przez firmę Netscape w celu zapewnienia bezpieczeństwa danych przesyłanych protokołami warstwy aplikacji (takimi jak HTTP, Telnet lub FTP) i protokołem TCP/IP. Ten protokół zabezpieczeń zapewnia szyfrowanie danych, uwierzytelnianie serwerów, spójność wiadomości oraz opcjonalne uwierzytelnianie agenta w przypadku połączenia TCP/IP.

Certyfikat SSL

Ten certyfikat cyfrowy umożliwia ustanawianie bezpiecznych połączeń HTTPS.

TCP

Protokół kontroli transmisji (TCP, Transmission Control Protocol) to protokół typu end-to-end, obsługujący połączenia sieciowe i zaprojektowany do współpracy z uporządkowanymi hierarchicznie warstwami protokołów, które obsługują aplikacje wielosieciowe. Rozpoznawanie adresów w protokole TCP opiera się na datagramach IP. Informacje można znaleźć w dokumencie DARPA Internet Program RFC 793.

Telnet

Telnet jest standardowym interfejsem urządzeń terminalowych w protokole TCP — tworzy on „wirtualny terminal sieciowy". Więcej informacji można znaleźć w dokumentacji RFC 854 organizacji Network Working Group.

Porty trojanów

Porty trojanów są często używane przez programy typu „koń trojański" w celu połączenia się z urządzeniem typu punkty końcowe. W przypadku epidemii program OfficeScan blokuje następujące numery portów, z którym mogą korzystać konie trojańskie.

TABELA E-1. Porty trojanów

NUMER PORTU	PROGRAM TYPU KOŃ TROJAŃSKI	NUMER PORTU	PROGRAM TYPU KOŃ TROJAŃSKI
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy

Numer portu	Program typu koń trojański	Numer portu	Program typu koń trojański
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

Port zaufany

Serwer i Agent OfficeScan używają portów zaufanych do wzajemnej komunikacji.

Po zablokowaniu portów zaufanych, a następnie przywróceniu zwykłych ustawień sieciowych po epidemii Agenci OfficeScan nie od razu wznowią komunikację z serwerem. Komunikacja agent-serwer zostanie przywrócona dopiero po upływie liczby godzin podanej na ekranie Ustawienia ochrony przed epidemią.

Program OfficeScan używa portu HTTP (domyślnie o numerze 8080) jako zaufanego portu serwera. W trakcie instalacji można wprowadzić inny numer portu. Aby zablokować ten port zaufany oraz zaufany port agenta OfficeScan, należy zaznaczyć pole wyboru Blokuj porty zaufane na ekranie Blokowanie portów.

Główny program instalacyjny generuje zaufany port agenta OfficeScan losowo podczas instalacji.

Określanie portów zaufanych

Procedura

1. Uzyskaj dostęp do lokalizacji <Folder instalacji serwera>\PCCSRV.
2. Otwórz plik ofcscan.ini w edytorze tekstu, na przykład w Notatniku.
3. Aby określić zaufany port serwera, wyszukaj ciąg „Master_DomainPort" i sprawdź wartość znajdującą się obok niego.

   Przykładowo, jeżeli ciąg ma postać Master_DomainPort=80, to zaufanym portem serwera jest port 80.
4. Aby określić zaufany port agenta, wyszukaj ciąg „Client_LocalServer_Port" i sprawdź wartość znajdującą się obok niego.

   Jeśli ciąg ma na przykład postać Client_LocalServer_Port=41375, zaufanym portem agenta jest port 41375.

Komunikacja dwukierunkowa

Komunikacja dwukierunkowa jest alternatywą dla komunikacji jednokierunkowej. Oparta jest na komunikacji jednokierunkowej, lecz dzięki dodatkowemu kanałowi wykorzystującemu protokół HTTP, który zawiera powiadomienia z serwera, komunikacja dwukierunkowa może poprawić wysyłanie i przetwarzanie poleceń w czasie rzeczywistym z serwera przez agenta MCP.

UDP

Datagramowy protokół użytkownika (UDP, User Datagram Protocol) to protokół przeznaczony do komunikacji bezpołączeniowej, używany w aplikacjach razem z protokołem IP do wysyłania komunikatów do innych programów. Informacje można znaleźć w dokumencie DARPA Internet Program RFC 768.

Pliki, których nie można wyczyścić

Silnik skanowania antywirusowego nie czyści następujących plików:

TABELA E-2. Rozwiązania dotyczące plików, których nie można wyczyścić

PLIKI, KTÓRYCH NIE MOŻNA WYCZYŚCIĆ	WYJAŚNIENIE I ROZWIĄZANIE
Pliki zarażone trojanami	Trojany to programy, które wykonują nieoczekiwane lub nieautoryzowane, zazwyczaj złośliwe działanie, polegające na wyświetlaniu komunikatów, usuwaniu plików lub formatowaniu dysków. Trojany nie zarażają plików, zatem czyszczenie nie jest konieczne. Rozwiązanie: Silnik usługi Usuwania Szkód i Szablon usługi Usuwania Szkód usuwają trojany.
Pliki zarażone robakami	Robak to samodzielny program (lub zbiór programów), który ma zdolność rozpowszechniania własnych funkcjonalnych kopii lub własnych segmentów na inne systemy typu punkt końcowy. Rozpowszechnianie zazwyczaj ma miejsce przez połączenia sieciowe lub przez załączniki wiadomości e-mail. Robaków nie można wyczyścić, ponieważ ich pliki są samodzielnymi programami. Rozwiązanie: Firma Trend Micro zaleca usuwanie robaków.
Zarażone pliki zabezpieczone przed zapisem	Rozwiązanie: Usuń zabezpieczenie przed zapisem, aby umożliwić wyczyszczenie pliku.
Pliki zabezpieczone hasłem	Pliki zabezpieczone hasłem obejmują zabezpieczone hasłem pliki skompresowane lub zabezpieczone hasłem pliki programu Microsoft Office. Rozwiązanie: Usuń zabezpieczenie hasłem, aby umożliwić wyczyszczenie pliku.
Pliki kopii zapasowych	Pliki z rozszerzeniami RB0~RB9 to kopie zapasowe zarażonych plików. Proces czyszczenia tworzy kopię zapasową zarażonego pliku na wypadek, gdyby został on w trakcie procesu czyszczenia uszkodzony przez wirus/złośliwe oprogramowanie.

Pliki, których nie można wyczyścić	Wyjaśnienie i rozwiązanie
	Rozwiązanie: Jeśli program pomyślnie wyczyści zarażony plik, zachowanie kopii zapasowej nie jest konieczne. Jeżeli urządzenie typu punkt końcowy działa prawidłowo, kopię zapasową można usunąć.
Zarażone pliki w Koszu	System może nie zezwalać na usunięcie zarażonych plików z Kosza, ponieważ system jest uruchomiony.

	Rozwiązanie w systemie Windows XP lub Windows Server 2003 z systemem plików NTFS:
	1. Zaloguj się do urządzenia typu punkt końcowy, używając uprawnień administratora.
	2. Zamknij wszystkie uruchomione aplikacje, aby zapobiec zablokowaniu pliku, którego system Windows nie będzie mógł usunąć.
	3. Otwórz wiersz polecenia.
	4. Wpisz następujące polecenia w celu usunięcia tych plików:
	`cd \`
	`cd recycled`
	`del *.* /S`
	Ostatnie polecenie usuwa wszystkie pliki z Kosza.
	5. Sprawdź, czy pliki zostały przeniesione.

	Rozwiązanie w innych systemach operacyjnych (lub niekorzystających z systemu plików NTFS):
	1. Uruchom ponownie urządzenie typu punkt końcowy w trybie MS-DOS.
	2. Otwórz wiersz polecenia.
	3. Wpisz następujące polecenia w celu usunięcia tych plików:
	`cd \`
	`cd recycled`

Pliki, których nie można wyczyścić	Wyjaśnienie i rozwiązanie
	`del *.* /S` Ostatnie polecenie usuwa wszystkie pliki z Kosza.
Zarażone pliki w folderze Temp systemu Windows lub folderze plików tymczasowych programu Internet Explorer	System może nie zezwalać na wyczyszczenie zarażonych plików w folderze Temp systemu Windows lub folderze plików tymczasowych programu Internet Explorer, ponieważ urządzenie typu punkt końcowy z nich korzysta. Pliki do wyczyszczenia mogą być plikami tymczasowymi potrzebnymi do działania systemu Windows.

	Rozwiązanie w systemie Windows XP lub Windows Server 2003 z systemem plików NTFS:
	
	1. Zaloguj się do urządzenia typu punkt końcowy, używając uprawnień administratora.
	
	2. Zamknij wszystkie uruchomione aplikacje, aby zapobiec zablokowaniu pliku, którego system Windows nie będzie mógł usunąć.
	
	3. Jeśli zarażony plik znajduje się w folderze Temp systemu Windows:
	
	a. Otwórz wiersz polecenia i przejdź do folderu Temp systemu Windows (domyślna ścieżka to `C:\Windows\Temp` w przypadku urządzeń typu punkty końcowe z systemem Windows XP lub Server 2003).
	
	b. Wpisz następujące polecenia w celu usunięcia tych plików:
	
	`cd temp`
	
	`attrib -h`
	
	`del *.* /S`
	
	Ostatnie polecenie usuwa wszystkie pliki z folderu Temp systemu Windows.
	
	4. Jeśli zarażony plik znajduje się w folderze plików tymczasowych programu Internet Explorer:
	
	a. Otwórz wiersz polecenia i przejdź do folderu plików tymczasowych programu Internet Explorer Temp

Pliki, których nie można wyczyścić	Wyjaśnienie i rozwiązanie

	(domyślna ścieżka to `C:\Documents and Settings\<Nazwa użytkownika>\Local Settings\Temporary Internet Files` w przypadku urządzeń typu punkty końcowe z systemem Windows XP lub Server 2003).
	b. Wpisz następujące polecenia w celu usunięcia tych plików:
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	Ostatnie polecenie usuwa wszystkie pliki z folderu plików tymczasowych programu Internet Explorer.
	c. Sprawdź, czy pliki zostały przeniesione.

	Rozwiązanie w innych systemach operacyjnych (lub niekorzystających z systemu plików NTFS):
	1. Uruchom ponownie urządzenie typu punkt końcowy w trybie MS-DOS.
	2. Jeśli zarażony plik znajduje się w folderze Temp systemu Windows:
	a. Otwórz wiersz polecenia i przejdź do folderu Temp systemu Windows (domyślna ścieżka to `C:\Windows\Temp` w przypadku urządzeń typu punkty końcowe z systemem Windows XP lub Server 2003).
	b. Wpisz następujące polecenia w celu usunięcia tych plików:
	`cd temp`
	`attrib -h`
	`del *.* /S`
	Ostatnie polecenie usuwa wszystkie pliki z folderu Temp systemu Windows.

Pliki, których nie można wyczyścić	Wyjaśnienie i rozwiązanie

	c. Ponownie uruchom urządzenie typu punkt końcowy w zwykłym trybie.
	3. Jeśli zarażony plik znajduje się w folderze plików tymczasowych programu Internet Explorer:
	a. Otwórz wiersz polecenia i przejdź do folderu plików tymczasowych programu Internet Explorer Temp (domyślna ścieżka to `C:\Documents and Settings\<Nazwa użytkownika>\Local Settings\Temporary Internet Files` w przypadku urządzeń typu punkty końcowe z systemem Windows XP lub Server 2003).
	b. Wpisz następujące polecenia w celu usunięcia tych plików:
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	Ostatnie polecenie usuwa wszystkie pliki z folderu plików tymczasowych programu Internet Explorer.
	c. Ponownie uruchom urządzenie typu punkt końcowy w zwykłym trybie.

Pliki skompresowane za pomocą nieobsługiwanego formatu kompresji.	Rozwiązanie: rozpakuj pliki.
Pliki zablokowane lub pliki, które są obecnie uruchomione.	Rozwiązanie: odblokuj pliki lub poczekaj, aż ich wykonywanie się zakończy.
Uszkodzone pliki	Rozwiązanie: usuń pliki.

Pliki zarażone trojanami

Trojany to programy, które wykonują nieoczekiwane lub nieautoryzowane, zazwyczaj złośliwe operacje, polegające na wyświetlaniu komunikatów, usuwaniu plików lub formatowaniu dysków. Trojany nie zarażają plików, zatem czyszczenie nie jest konieczne.

Rozwiązanie: program OfficeScan korzysta z Silnik usługi Usuwania Szkód i Szablon usługi Usuwania Szkód w celu usuwania trojanów.

Pliki zarażone robakami

Robak to samodzielny program (lub zbiór programów) zdolny do rozpowszechniania własnych funkcjonalnych kopii lub segmentów w innych systemach punktów końcowych. Rozpowszechnianie zazwyczaj ma miejsce przez połączenia sieciowe lub przez załączniki wiadomości e-mail. Robaków nie można wyczyścić, ponieważ ich pliki są samodzielnymi programami.

Rozwiązanie: firma Trend Micro zaleca usuwanie robaków.

Zarażone pliki zabezpieczone przed zapisem

Rozwiązanie: Usuń zabezpieczenie przed zapisem, aby umożliwić programowi OfficeScan wyczyszczenie pliku.

Pliki zabezpieczone hasłem

Dotyczy skompresowanych plików zabezpieczonych hasłem lub plików pakietu Microsoft Office zabezpieczonych hasłem.

Rozwiązanie: usuń zabezpieczenie hasłem, aby umożliwić programowi OfficeScan wyczyszczenie tych plików.

Pliki kopii zapasowych

Pliki z rozszerzeniami RB0–RB9 to kopie zapasowe zarażonych plików. Program OfficeScan tworzy kopię zapasową zarażonego pliku na wypadek, gdyby został on w trakcie procesu czyszczenia uszkodzony przez wirus/złośliwe oprogramowanie.

Rozwiązanie: Jeśli program OfficeScan pomyślnie wyczyści zarażony plik, zachowanie kopii zapasowej nie jest konieczne. Jeżeli punkt końcowy działa normalnie, kopię zapasową można usunąć.

Indeks

B

C

D

K

L

M

N

O

P

R

S

T

U

V

W

Z

Ź

TREND MICRO INCORPORATED
Trendd Micro (EMEA) Limited - Central Eastern Europe, Office in Warsaw Warsaw Trade Tower Floor 30, Chłodna 5100-867 Warszawa
Telefon: +48 (22)486 34 50 Faks: +48 (22) 486 34 49 biuro@trendmicro.com
www.trendmicro.com
Item Code: OSPMXG7608/161028