TREND MICRO

# 10.0 Worry-Free™ Business Security Standard Edition i Advanced Edition

## Podręcznik administratora

Securing Your Journey to the Cloud

Protected Cloud

Web Security

Firma Trend Micro Incorporated zastrzega sobie prawo do wprowadzania, bez wcześniejszej zapowiedzi, zmian w tym dokumencie oraz w opisanych w nim produkt. Przed zainstalowaniem i korzystaniem z produkt należy zapoznać się z plikami „readme", uwagami do wydania oraz najnowszą wersją właściwej dokumentacji, które są dostępne w witrynie internetowej firmy Trend Micro pod adresem:

http://docs.trendmicro.com/pl-pl/smb/worry-free-business-security.aspx

Trend Micro, logo Trend Micro t-ball, TrendProtect, TrendSecure, Worry-Free, OfficeScan, ServerProtect, PC-cillin, InterScan i ScanMail są znakami handlowymi lub zastrzeżonymi znakami handlowymi firmy Trend Micro Incorporated. Pozostałe nazwy produktów i firm mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi odpowiednich właścicieli.

Copyright © 2018. Trend Micro Incorporated. Wszelkie prawa zastrzeżone.

Numer części dokumentu: WFPM108197/180326

Data wydania: Czerwiec 2018 r.

Podlega ochronie patentami USA o numerach: 5 951 698 i 7 188 369

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

## Wstęp


Wstęp ..... xiii

Dokumentacja programu Worry-Free Business Security ..... xiv

Odbiorcy ..... xiv

Konwencje przyjęte w dokumentacji ..... xv


## Rozdział 1: Wprowadzenie do programów Worry-Free Business Security Standard i Advanced


Omówienie programu Trend Micro Worry-Free Business Security ..... 1-2

Nowości w tej wersji ..... 1-2

Kluczowe funkcje i korzyści ..... 1-4

- Trend Micro Smart Protection Network ..... 1-4
- Usługi File Reputation Services ..... 1-5
- Usługi Web Reputation Services ..... 1-5
- Usługa Email Reputation (tylko w wersji Advanced) ..... 1-6
- Smart Feedback ..... 1-7
- Filtrowanie adresów URL ..... 1-8

Zalety ochrony ..... 1-8

Informacje o zagrożeniach ..... 1-9

- Wirusy i złośliwe oprogramowanie ..... 1-10
- Oprogramowanie spyware i grayware ..... 1-12
- Spam ..... 1-13
- Włamania ..... 1-13
- Złośliwe zachowanie ..... 1-13
- Fałszywe punkty dostępu ..... 1-13
- Zdarzenie typu phishing ..... 1-14
- Ataki typu „mass-mailing” ..... 1-14
- Zagrożenia z sieci WWW ..... 1-15

## Rozdział 2: Wprowadzenie

Worry-Free Business Security Network ..... 2-2

Program Security Server ..... 2-2
Scan Server ..... 2-2

Agenty ..... 2-4

Konsola internetowa ..... 2-4
Otwieranie konsoli Web ..... 2-5
Nawigacja w konsoli internetowej ..... 2-8
Ikony konsoli internetowej ..... 2-10

## Rozdział 3: instalowanie agentów

Instalacja programu Security Agent ..... 3-2
Wymagania dotyczące instalacji programu Security Agent ..... 3-2
Uwagi dotyczące instalacji programu Security Agent ..... 3-2
Dostępne funkcje programu Security Agent ..... 3-3
Instalacja programu Security Agent i obsługa protokołu IPv6 ..... 3-5

Metody instalacji programu Security Agent ..... 3-7
Instalowanie z wewnętrznej strony internetowej ..... 3-11
Instalowanie za pomocą skryptu logowania ..... 3-13
Instalowanie za pomocą narzędzia Client Packager ..... 3-15
Instalowanie za pomocą instalacji zdalnej ..... 3-19
Instalowanie za pomocą narzędzia Vulnerability Scanner ..... 3-22
Instalowanie za pomocą powiadomienia e-mail ..... 3-34
Migracja do programu Security Agent ..... 3-35
Wykonywanie zadań po instalacji w programach Security Agent . 3-36

Instalacja programu Messaging Security Agent ..... 3-38
Wymagania dotyczące instalacji programu Messaging Security Agent ..... 3-38
Instalowanie programu Messaging Security Agent (tylko w wersji Advanced) ..... 3-39

Usuwanie agentów ..... 3-41
Usuwanie agentów z konsoli internetowej ..... 3-42
Odinstalowywanie agentów z konsoli internetowej ..... 3-42
Odinstalowywanie programu Security Agent z punktu końcowego ..... 3-43

Używanie narzędzia SA Uninstall ..... 3-44
Odinstalowywanie programu Messaging Security Agent z serwera Microsoft Exchange (tylko w wersji Advanced) ..... 3-46

## Rozdział 4: Zarządzanie urządzeniami

Korzystanie z drzewa urządzeń ..... 4-2

Używanie poleceń urządzenia ..... 4-4

Dodawanie agentów do grup ..... 4-6

Dodawanie grup ..... 4-8

Dostosowanie kolumn listy urządzeń ..... 4-9

Przenoszenie agentów ..... 4-11
Przenoszenie programów Security Agent między grupami ..... 4-13
Przenoszenie agentów między serwerami Security Server za pomocą konsoli internetowej ..... 4-13
Przenoszenie programu Security Agent między serwerami Security Server za pomocą narzędzia Client Mover ..... 4-14

Replikowanie ustawień ..... 4-16
Replikowanie ustawień grupy programów Security Agent ..... 4-16
Replikowanie ustawień programu Messaging Security Agent (tylko w wersji Advanced) ..... 4-17

Importowanie i eksportowanie ustawień grup Security Agent ..... 4-18
Eksportowanie ustawień ..... 4-20
Importowanie ustawień ..... 4-20

## Rozdział 5: Zarządzanie podstawowymi ustawieniami zabezpieczeń w programach Security Agent

Zestawienie podstawowych ustawień zabezpieczeń w programach Security Agent ..... 5-2

Metody skanowania ..... 5-3
Konfiguracja metod skanowania ..... 5-5

Skanowanie w czasie rzeczywistym w programach Security Agent ..... 5-7
Konfigurowanie skanowania w czasie rzeczywistym w programach Security Agent ..... 5-8

Przewidujące uczenie maszynowe ..... 5-8
Konfigurowanie przewidującego uczenia maszynowego ..... 5-10
Monitorowanie zachowania ..... 5-11
Konfigurowanie monitorowania zachowania ..... 5-12
Zaufany program ..... 5-17
Konfigurowanie zaufanego programu ..... 5-17
Katalog kwarantanny ..... 5-18
Konfigurowanie katalogu kwarantanny ..... 5-21
Usługa Web Reputation ..... 5-21
Konfigurowanie usługi Web Reputation dla programów Security Agent ..... 5-23
Filtrowanie adresów URL ..... 5-24
Konfigurowanie filtrowania adresów URL ..... 5-24
Dozwolone/zablokowane adresy URL ..... 5-25
Konfigurowanie dozwolonych/zablokowanych adresów URL ..... 5-26
Zapora ..... 5-27
Konfigurowanie zapory ..... 5-30
Praca z wyjątkami zapory ..... 5-31
Wyłączanie zapory w grupie agentów ..... 5-34
Wyłączanie zapory na wszystkich agentach ..... 5-34
Kontrola urządzeń ..... 5-34
Konfigurowanie kontroli urządzeń ..... 5-35
Narzędzia użytkownika ..... 5-37
Konfigurowanie narzędzi użytkownika ..... 5-37
Uprawnienia agenta ..... 5-38
Konfigurowanie uprawnień agenta ..... 5-38

## Rozdział 6: Zarządzanie podstawowymi ustawieniami zabezpieczeń w programach Messaging Security Agent (tylko w wersji Advanced)

Messaging Security Agent ..... 6-2
Skanowanie wiadomości e-mail przez program Messaging Security Agent ..... 6-3

Domyślne ustawienia programu Messaging Security Agent ..... 6-4

Skanowanie w czasie rzeczywistym w programach Messaging Security Agent ..... 6-6
Konfigurowanie skanowania w czasie rzeczywistym dla programów Messaging Security Agent ..... 6-6

Ochrona antyspamowa ..... 6-7
Usługa Email Reputation ..... 6-8
Skanowanie zawartości ..... 6-10

Filtrowanie zawartości ..... 6-16
Zarządzanie regułami filtrowania zawartości ..... 6-17
Typy reguł filtrowania zawartości ..... 6-21
Dodawanie reguły filtrowania zawartości w przypadku zgodności wszystkich warunków ..... 6-22
Dodawanie reguły filtrowania zawartości w przypadku zgodności dowolnego warunku ..... 6-25
Dodawanie reguły monitorowania filtrowania zawartości ..... 6-28
Tworzenie wyjątków do reguł filtrowania zawartości ..... 6-31

Zapobieganie utracie danych ..... 6-32
Przygotowanie ..... 6-32
Zarządzanie regułami zapobiegania utracie danych ..... 6-33
Domyślne reguły zapobiegania utracie danych ..... 6-41
Dodawanie reguł zapobiegania utracie danych ..... 6-42

Blokowanie załączników ..... 6-48
Konfigurowanie blokowania załączników ..... 6-48

Usługa Web Reputation ..... 6-51
Konfigurowanie usługi Web Reputation w programach Messaging Security Agent ..... 6-52

Mobile Security ..... 6-54
Mobile Security — pomoc techniczna ..... 6-55
Konfigurowanie kontroli dostępu urządzenia ..... 6-57
Anulowanie oczekującego wymazywania urządzenia ..... 6-58
Ręczne wymazywanie zawartości urządzeń ..... 6-58
Konfigurowanie reguł zabezpieczeń ..... 6-59

Kwarantanna dla programów Messaging Security Agent ..... 6-65
Tworzenie zapytań dotyczących katalogów kwarantanny ..... 6-66

Wyświetlanie wyników zapytań dotyczących kwarantanny i podejmowanie działań ..... 6-67
Obsługa katalogów kwarantanny ..... 6-69
Konfigurowanie katalogów kwarantanny ..... 6-70
Ustawienia powiadamiania dla programów Messaging Security Agent 6-72
Konfigurowanie ustawień powiadomień dla programów Messaging Security Agent ..... 6-73
Konfigurowanie obsługi wiadomości typu spam ..... 6-74
Zarządzanie funkcją End User Quarantine ..... 6-76
Pomoc techniczna/diagnostyka firmy Trend Micro ..... 6-77
Generowanie raportów diagnostycznych ..... 6-78
Monitorowanie w czasie rzeczywistym ..... 6-79
Praca z monitorowaniem w czasie rzeczywistym ..... 6-80
Dodawanie informacji o wykluczeniu odpowiedzialności do wychodzących wiadomości e-mail ..... 6-80

## Rozdział 7: Zarządzenie skanowaniami

Skanowanie — informacje ..... 7-2
Skanowanie w czasie rzeczywistym ..... 7-2
Skanowanie ręczne ..... 7-3
Uruchamianie skanowania ręcznego ..... 7-4
Skanowanie zaplanowane ..... 7-7
Konfigurowanie skanowania zaplanowanego ..... 7-7
Cele skanowania i operacje dotyczące programów Security Agent ..... 7-11
Cele skanowania i operacje dotyczące programów Messaging Security Agent ..... 7-20

## Rozdział 8: Zarządzanie aktualizacjami

Omówienie aktualizacji ..... 8-2
Składniki, które można aktualizować ..... 8-4
Pakiety hot fix, poprawki i dodatki Service Pack ..... 8-11

Aktualizacje serwera Security Server ..... 8-12
Konfigurowanie źródła aktualizacji serwera Security Server ..... 8-14
Ręczna aktualizacja serwera Security Server ..... 8-15
Konfigurowanie zaplanowanych aktualizacji serwera Security Server ..... 8-16
Wycofywanie składników ..... 8-17

Aktualizacje programów Security Agent i Messaging Security Agent .. 8-18
Aktualizacje automatyczne ..... 8-18
Uruchamianie aktualizacji ręcznej ..... 8-19
Przypomnienia i wskazówki dotyczące aktualizacji agentów ..... 8-19

Agenty aktualizacji ..... 8-20
Konfigurowanie agentów aktualizacji ..... 8-23

## Rozdział 9: Używanie stanu aktywności

Stan aktywności ..... 9-2
Centrum akcji ..... 9-3
Wykryte zagrożenia bezpieczeństwa w czasie ..... 9-8
Podsumowanie zagrożeń typu ransomware ..... 9-17
Stan licencji ..... 9-22
Podsumowanie dla serwerów Exchange ..... 9-22
Stan agenta ..... 9-23

## Rozdział 10: Zarządzanie powiadomieniami

Korzystanie z powiadomień ..... 10-2

Konfigurowanie zdarzeń dla powiadomień ..... 10-5
Zmienne znaczników ..... 10-6

## Rozdział 11: Zarządzanie ustawieniami globalnymi

Ustawienia globalne ..... 11-2

Konfigurowanie ustawień serwera proxy w sieci Internet ..... 11-3

Konfigurowanie ustawień serwera SMTP ..... 11-4

Konfigurowanie ustawień komputerów/serwerów ..... 11-5

Konfigurowanie ustawień systemu ..... 11-10

Konfigurowanie ustawień listy wyjątków ..... 11-14

## Rozdział 12: Korzystanie z dzienników i raportów

Dzienniki ..... 12-2
Korzystanie z kwerendy dziennika ..... 12-4

Raporty ..... 12-5
Praca z raportami jednorazowymi ..... 12-6
Praca z raportami zaplanowanymi ..... 12-7
Interpretowanie raportów ..... 12-12

Wykonywanie zadań obsługi raportów i dzienników ..... 12-16

## Rozdział 13: Wykonywanie zadań administracyjnych

Zmiana hasła konsoli internetowej ..... 13-2

Praca z Plug-in Manager ..... 13-2

Zarządzanie licencją produktu ..... 13-3

Konfigurowanie ustawień aktualizacji produktu ..... 13-5

Konfigurowanie powiadomień o aktualizacji produktu ..... 13-6

Uczestnictwo w programie Smart Feedback ..... 13-7

Zmiana języka interfejsu agenta ..... 13-7

Zapisywanie i przywracanie ustawień programów ..... 13-8

Dezinstalacja programu Security Server ..... 13-10

## Rozdział 14: Korzystanie z narzędzi do zarządzania

Typy narzędzi ..... 14-2

Trend Micro Remote Manager Agent ..... 14-3
Instalowanie programu Trend Micro Remote Manager Agent (użytkownicy portalu licencjonowania klientów) ..... 14-4
Instalowanie programu Trend Micro Remote Manager Agent (użytkownicy platformy Licensing Management Platform) ..... 14-6
Zarządzanie agentami serwera zarządzanego ..... 14-7
Tworzenie i przywracanie kopii zapasowej ustawień agenta ..... 14-12

Oszczędzanie miejsca na dysku ..... 14-15
Uruchamianie programu Disk Cleaner na serwerze Security Server ..... 14-15
Uruchamianie programu Disk Cleaner na serwerze Security Server za pomocą interfejsu wiersza polecenia ..... 14-16
Oszczędzanie miejsca na dysku klientów ..... 14-17

Przenoszenie bazy danych serwera skanowania ..... 14-18

Przywracanie zaszyfrowanych plików ..... 14-18
Odszyfrowywanie i przywracanie plików w programie Security Agent ..... 14-20
Odszyfrowywanie i przywracanie plików na serwerze Security Server, w niestandardowym katalogu kwarantanny lub programie Messaging Security Agent ..... 14-21
Przywracanie wiadomości e-mail w formacie Transport Neutral Encapsulation Format ..... 14-23

Korzystanie z narzędzia ReGenID ..... 14-23

Zarządzanie dodatkami SBS i EBS ..... 14-24
Ręczne instalowanie dodatków SBS i EBS ..... 14-24
Korzystanie z dodatków SBS i EBS ..... 14-25

## Dodatek A: Ikony programu Security Agent

Sprawdzanie stanu programu Security Agent ..... A-2

Wyświetlanie ikon programu Security Agent na pasku zadań systemu Windows ..... A-4

Uzyskiwanie dostępu do konsoli Flyover ..... A-5

## Dodatek B: Obsługa protokołu IPv6 w programie Worry-Free Business Security

Obsługa protokołu IPv6 w programie Worry-Free Business Security i Security Agent ..... B-2
Wymagania programu Security Server dotyczące protokołu IPv6 ..... B-2
Wymagania dotyczące programu Messaging Security Agent ..... B-3

Ograniczenia serwera wykorzystującego wyłącznie protokół IPv6 ..... B-3
Ograniczenia Security Agent wykorzystującego wyłącznie protokół IPv6 ..... B-4
Konfigurowanie adresów IPv6 ..... B-5
Ekrany wyświetlające adresy IP ..... B-7

## Dodatek C: Pomoc techniczna

Zasoby dotyczące rozwiązywania problemów ..... C-2
Korzystanie z portalu pomocy technicznej ..... C-2
Encyklopedia zagrożeń ..... C-2
Kontakt z firmą Trend Micro ..... C-3
Przyspieszanie przyjęcia zgłoszenia serwisowego ..... C-4
Przesyłanie podejrzanej zawartości do firmy Trend Micro ..... C-5
Email Reputation Services ..... C-5
Usługi File Reputation Services ..... C-5
Usługi Web Reputation Services ..... C-5
Inne zasoby ..... C-6
Centrum pobierania ..... C-6
Opinie o dokumentacji ..... C-6

## Dodatek D: Terminologia i pojęcia związane z produktami

Poprawka krytyczna ..... D-2
Pakiet Hot Fix ..... D-2
IntelliScan ..... D-2
IntelliTrap ..... D-3
System wykrywania włamań (IDS) ..... D-3
Słowa kluczowe ..... D-5
Poprawka ..... D-10
Wyrażenia regularne ..... D-11
Listy wyłączeń ze skanowania ..... D-20

Dodatek Service Pack ..... D-27
Porty trojanów ..... D-27
Pliki, których nie można wyczyścić ..... D-29

## Indeks

Indeks ..... IN-1

# Wstęp

## Wstęp

Zapraszany do lektury *Podręcznika administratora* programu Trend Micro™ Worry-Free™ Business Security. Ten dokument dotyczy informacji wstępnych, procedur instalacji agentów oraz zarządzania programem Security Server i agentami.

# Dokumentacja programu Worry-Free Business Security

Dokumentacja programu Worry-Free Business Security obejmuje następujące składniki:

**TABELA 1. Dokumentacja programu Worry-Free Business Security**

| DOKUMENTACJA | OPIS |
|---|---|
| Podręcznik instalacji oraz uaktualniania | Dokument PDF z omówieniem wymagań i procedur odnoszących się do instalowania programu Security Server oraz instalowania serwera i agentów. |
| Podręcznik administratora | Dokument PDF z omówieniem informacji wprowadzających, procedur instalacji klienta oraz zarządzania programem Security Server i agentami |
| Pomoc | Pliki HTML skompilowane w formacie WebHelp lub CHM, zawierające instrukcje korzystania, porady i informacje dotyczące określonych zastosowań programu |
| 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 witrynę internetową<br><br>http://esupport.trendmicro.com |

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

http://docs.trendmicro.com/pl-pl/smb/worry-free-business-security.aspx

# Odbiorcy

Dokumentacja programu Worry-Free Business Security jest przeznaczona dla następujących grup użytkowników:

- **Administratorzy zabezpieczeń**: odpowiedzialni za zarządzanie programem Worry-Free Business Security, w tym programem Security Server, oraz za instalację agentów i zarządzanie nimi. Od użytkowników tego typu oczekuje się zaawansowanej wiedzy na temat zarządzania serwerem i siecią.
- **Użytkownicy końcowi**: użytkownicy, którzy mają na komputerach zainstalowane programy Security Agent. Poziom umiejętności takich osób jest różny — od początkujących po zaawansowanych.

# Konwencje przyjęte w dokumentacji

Aby ułatwić odnalezienie i zrozumienie informacji, w dokumentacji programu Worry-Free Business Security przyjęto następujące konwencje:

**TABELA 2. Konwencje przyjęte w dokumentacji**

| KONWENCJA | OPIS |
|---|---|
| WIELKIE LITERY | Akronimy, skróty, nazwy poszczególnych poleceń oraz klawisze klawiatury |
| **Pogrubienie** | Nazwy i polecenia menu, przyciski poleceń, karty, opcje oraz nazwy zadań |
| *Kursywa* | Odniesienia do innych dokumentacji oraz nowych rozwiązań technologicznych |
| <Tekst> | Oznacza, że tekst wewnątrz nawiasów ostrych należy zastąpić rzeczywistymi informacjami. Na przykład ścieżkę `C:\Program Files\<nazwa_pliku>` można zmienić na `C:\Program Files\sample.jpg`. |
| **Uwaga** | Uwagi lub zalecenia dotyczące konfiguracji |
| **Porada** | Informacje o sprawdzonych metodach oraz zaleceniach firmy Trend Micro |

| KONWENCJA | OPIS |
| --- | --- |
| OSTRZEŻENIE! | Ostrzeżenia dotyczące czynności, które mogą stwarzać zagrożenie w sieci |

# Rozdział 1

# Wprowadzenie do programów Worry-Free™ Business Security Standard i Advanced

Ten rozdział zawiera omówienie programu Worry-Free Business Security (Worry-Free Business Security).

# Omówienie programu Trend Micro Worry-Free Business Security

Program Trend Micro Worry-Free Business Security (Worry-Free Business Security) zabezpiecza użytkowników i zasoby w małych firmach przed kradzieżą danych, kradzieżą tożsamości, niebezpiecznymi witrynami internetowymi oraz spamem (tylko wersja Advanced).

W tym dokumencie przedstawiono informacje dotyczące zarówno wersji Worry-Free Business Security Standard, jak i Advanced. Części i rozdziały dotyczące wersji Advanced są oznaczone dopiskiem „(tylko w wersji Advanced)".

Program Worry-Free Business Security, bazujący na systemie Trend Micro Smart Protection Network, jest:

- **Bezpieczniejszy**: zatrzymuje wirusy, oprogramowanie szpiegowskie, spam (tylko w wersji Advanced) i zagrożenia internetowe, zanim dotrą one do klientów. Funkcja filtrowania adresów URL blokuje dostęp do niebezpiecznych witryn internetowych i pomaga zwiększyć produktywność użytkowników.
- **Inteligentniejszy**: szybkie skanowanie i ciągłość aktualizacji chronią przed nowymi zagrożeniami przy minimalnym wpływie na działanie klientów.
- **Prostszy**: łatwa instalacja i administracja prawie nie wymagająca ingerencji. Program Worry-Free Business Security wykrywa zagrożenia bardziej skutecznie, dzięki czemu można skoncentrować się na działalności firmy zamiast na problemach bezpieczeństwa.

# Nowości w tej wersji

W poniższej tabeli przedstawiono nowe funkcje i rozszerzenia zawarte w tej wersji programu Worry-Free Business Security.

| FUNKCJA/ULEPSZENIE | OPIS |
|---|---|
| Przewidujące uczenie maszynowe | Mechanizm przewidującego uczenia maszynowego może chronić sieć przed nowymi, wcześniej nierozpoznanymi lub nieznanymi zagrożeniami przy użyciu zaawansowanej analizy funkcji pliku i heurystycznego monitorowania procesów. Przewidujące uczenie maszynowe może potwierdzić przypuszczenie, że w pliku lub procesie istnieje zagrożenie, oraz określić prawdopodobny typ zagrożenia, chroniąc przed atakami typu zero-day.<br><br>Patrz *Przewidujące uczenie maszynowe na stronie 5-8*, aby uzyskać więcej informacji. |
| Skanowanie wybranych urządzeń | Oprócz ręcznego skanowania co najmniej jednej grupy urządzeń, program Worry-Free Business Security umożliwia skanowanie wybranych urządzeń w celu efektywnego zarządzania nimi w sieci. Możliwe jest także zatrzymanie trwającego skanowania wybranych urządzeń.<br><br>Patrz *Używanie poleceń urządzenia na stronie 4-4*, aby uzyskać więcej informacji. |
| Nowy wygląd informacji o stanie aktywności | Ważne informacje są wygodnie pogrupowane w prostych widgetach. Widgety ułatwiają dostęp do najważniejszych informacji, takich jak analiza zagrożeń i stan urządzenia. Ponadto nowe Centrum akcji umożliwia rozwiązywanie problemów jednym kliknięciem.<br><br>Patrz *Używanie stanu aktywności na stronie 9-1*, aby uzyskać więcej informacji. |
| Automatyczna aktualizacja produktu | Funkcja Aktualizacja produktu pozwala automatycznie pobierać i instalować aktualizacje.<br><br>Patrz *Konfigurowanie ustawień aktualizacji produktu na stronie 13-5*, aby uzyskać więcej informacji. |

| FUNKCJA/ULEPSZENIE | OPIS |
|---|---|
| Ulepszenia powiadamiania e-mail | Czytelna treść tematu wiadomości e-mail oraz konkretne podsumowanie dotyczące zdarzenia, zawierające potencjalne rozwiązanie problemu, ułatwiają podejmowanie decyzji dotyczących wymaganych działań i pozwalają szybciej rozwiązywać problemy.<br><br>Patrz *Zarządzanie powiadomieniami na stronie 10-1*, aby uzyskać więcej informacji. |
| Ochrona protokołu sieciowego HTTPS przed zagrożeniami internetowymi dla przeglądarek Google Chrome i Microsoft Edge | Program Worry-Free Business Security oferuje udoskonaloną i rozszerzoną ochronę przed złośliwymi witrynami HTTPS. Dzięki usłudze Web Reputation i regułom filtrowania adresów URL można bezpiecznie korzystać z przeglądarek Google Chrome i Microsoft Edge bez konieczności instalowania jakichkolwiek dodatków.<br><br>Patrz *Konfigurowanie ustawień komputerów/serwerów na stronie 11-5*, aby uzyskać więcej informacji. |
| Obsługa symboli wieloznacznych i zmiennych środowiskowych systemu Windows na potrzeby wyjątków monitorowania zachowania | Program Worry-Free Business Security obsługuje znaki wieloznaczne i oferuje lepszą obsługę zmiennych środowiskowych Windows dla zatwierdzonych i zablokowanych programów w Monitorowaniu zachowań. Ulepszenia te zapewniają większą elastyczność podczas definiowania wyjątków.<br><br>Patrz *Obsługiwane zmienne środowiskowe na stronie 5-16*, aby uzyskać więcej informacji. |

# Kluczowe funkcje i korzyści

Program Worry-Free Business Security udostępnia następujące funkcje i korzyści:

## 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

## Usługi File Reputation Services

Usługi File Reputation Services sprawdzają reputację każdego pliku, porównując ją ze zlokalizowaną w chmurze bazą danych. Informacje dotyczące złośliwego oprogramowania są przechowywane w otoczeniu internetowym, dlatego są one natychmiast dostępne dla wszystkich użytkowników. Wydajne sieci dostarczania zawartości i lokalne serwery buforujące redukują opóźnienie podczas procesu kontroli do minimum. Architektura typu otoczenie internetowe-klient zapewnia szybszą ochronę, eliminuje obciążenie związane z wdrażaniem plików sygnatur i umożliwia znaczne zmniejszenie ilości zasobów wykorzystywanych przez klienty.

Aby możliwe było użycie usług File Reputation, programy Security Agent muszą działać w trybie skanowania inteligentnego (Smart Scan). Takie agenty są w tym dokumencie nazywane **agentami Smart Scan**. Agenty w trybie innym niż Smart Scan nie korzystają z usług File Reputation i są określane jako **agenty skanowania standardowego**. Administratorzy programu Worry-Free Business Security mogą skonfigurować wszystkie agenty lub kilka z nich w trybie Smart Scan.

## 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 zainfekowanych. Funkcje usługi Web Reputation pozwalają upewnić się, że strony otwierane przez użytkowników są bezpieczne i wolne od zagrożeń internetowych, takich jak złośliwe oprogramowanie, spyware i oszustwa związane z wyłudzaniem informacji, mające na celu uzyskanie danych osobowych użytkowników. 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.

Agenty używające usług Web Reputation Services podlegają regułom usługi Web Reputation. Administratorzy programu Worry-Free Business Security mogą podporządkować regułom usługi Web Reputation wszystkie lub tylko niektóre agenty.

## Usługa Email Reputation (tylko w wersji Advanced)

Technologia Trend Micro Email Reputation sprawdza adresy IP, korzystając z bazy danych reputacji znanych źródeł spamu i dynamicznej usługi oceniającej reputację nadawcy wiadomości e-mail w czasie rzeczywistym. Oceny reputacji są korygowane na podstawie nieustannej analizy „zachowań" adresów IP, stopnia aktywności i danych historycznych. Złośliwe wiadomości e-mail są blokowane jeszcze po stronie Internetu na podstawie adresu IP nadawcy, dzięki czemu pliki typu zombi lub botnet nie docierają w ogóle do sieci lub komputera użytkownika.

Technologia Email Reputation identyfikuje spam na podstawie reputacji źródłowego agenta MTA (Mail Transport Agent). Zwalnia to program Security Server z konieczności wykonywania tego zadania. Po włączeniu usługi Email Reputation cały przychodzący ruch SMTP jest sprawdzany przez bazy danych adresów IP w celu ustalenia, czy źródłowy adres IP jest poprawny lub czy nie został umieszczony na czarnej liście jako znany dostawca spamu.

Istnieją dwa poziomy usługi dla usługi Email Reputation:

- **Standardowy**: usługa standardowa korzysta z bazy danych, która śledzi reputację około dwóch miliardów adresów IP. Adresy IP, które są stale powiązane

z dostarczaniem wiadomości typu spam, zostają dodane do bazy danych i rzadko są z niej usuwane.

- **Zaawansowany**: poziom zaawansowany to usługa DNS, która jest oparta na zapytaniach i przypomina usługę standardową. Podstawą tej usługi jest standardowa baza danych reputacji oraz dynamiczna baza danych reputacji, która blokuje wiadomości ze znanych i podejrzanych źródeł spamu.

Po znalezieniu wiadomości e-mail z zablokowanego lub podejrzanego adresu IP usługi Email Reputation Services blokują tą wiadomość, zanim osiągnie ona infrastrukturę przesyłania wiadomości. Jeśli usługi Email Reputation blokują wiadomości z adresu IP, który wydaje się bezpieczny, można dodać ten adres do listy dozwolonych adresów IP.

## Smart Feedback

Program 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.

Aby uzyskać więcej informacji, zobacz *Uczestnictwo w programie Smart Feedback na stronie 13-7*.

**Porada**

Do 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

## Filtrowanie adresów URL

Funkcja filtrowania adresów URL pomaga w kontrolowaniu dostępu do witryn internetowych w celu zwiększenia produktywności pracowników, ograniczenia zużycia przepustowości połączenia internetowego i tworzenia bezpieczniejszego środowiska roboczego. Można wybrać poziom filtrowania adresów URL lub dostosować listę blokowanych witryn internetowych.

# Zalety ochrony

Poniższa tabela przedstawia, w jaki sposób poszczególne składniki programu Worry-Free Business Security chronią komputery przed zagrożeniami.

**TABELA 1-1. Zalety ochrony**

| ZAGROŻENIE | OCHRONA |
|---|---|
| **Wirusy/złośliwe oprogramowanie**. Wirusy, trojany, robaki, umyślnie utworzone luki w zabezpieczeniach i oprogramowanie typu rootkit<br><br>**Spyware/grayware**. Spyware, dialery, narzędzia hakerskie, programy do łamania haseł, adware, programy-żarty i keyloggery | Skanowanie plików (skanowanie w czasie rzeczywistym, skanowanie ręczne, skanowanie zaplanowane) |
| Zagrożenia bezpieczeństwa przesyłane w wiadomościach e-mail | **Skanowanie poczty POP3** w programie Security Agent |
| Robaki/wirusy sieciowe i włamania | Zapora w programie Security Agent |
| Potencjalnie szkodliwe witryny internetowe i phishingowe | Usługa Web Reputation i filtrowanie adresów URL w programie Security Agent |
| Zagrożenia rozpowszechniane za pośrednictwem urządzeń ze złączem USB i innych urządzeń zewnętrznych | Kontrola urządzeń w programie Security Agent |
| Złośliwe zachowanie | Monitorowanie zachowania w programie Security Agent |
| Programy ransomware, które są ukierunkowane na dokumenty działające na punktach końcowych | Monitorowanie zachowania i Przewidujące uczenie maszynowe w programie Security Agent |

# Informacje o zagrożeniach

Organizacje, które nie zatrudniają osobnego personelu do spraw zabezpieczeń oraz stosują luźne reguły bezpieczeństwa, są narażone na zagrożenia, nawet jeśli dysponują podstawową infrastrukturą zabezpieczeń. Mimo wykrycia zagrożeń może się okazać, że rozprzestrzeniły się już na wielu zasobach komputerowych, a ich całkowite wyeliminowanie będzie wymagać dużo czasu i wysiłku. Nieprzewidziane koszty związane z eliminacją zagrożeń również mogą być olbrzymie.

Inteligentne rozwiązania Trend Micro do zarządzania bezpieczeństwem sieci oraz serwery działające w chmurze, stanowiące część sieci Trend Micro Smart Protection Network, identyfikują zagrożenia nowej generacji i odpowiednio na nie reagują.

## 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.

- **Programy-żarty**: Podobne do wirusów programy, często zmieniające wygląd elementów wyświetlanych na monitorze komputera.

- **Prawdopodobny wirus/złośliwe oprogramowanie**: Podejrzane pliki zawierające niektóre elementy charakterystyczne dla wirusa/złośliwego oprogramowania. Szczegółowe informacje zawiera Encyklopedia zagrożeń firmy Trend Micro:

  http://about-threats.trendmicro.com/threatencyclopedia.aspx

- **Oprogramowanie typu rootkit**: Program (lub zbiór programów), które instalują w systemie kod i wykonują go bez zgody i wiedzy użytkownika. Wykorzystują mechanizmy maskujące umożliwiające stałą i niemożliwą do wykrycia obecność na komputerze. 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.

- **Trojan**: Ten typ zagrożenia często wykorzystuje porty, aby uzyskać dostęp do komputerów lub plików 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.

- **Wirus**: Program, który się powiela. 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.
  - **Samorozpakowujące się archiwum**: Skompresowany i/lub zaszyfrowany program wykonywalny systemu Windows lub Linux™, często trojan. Kompresja plików wykonywalnych utrudnia wykrywanie wirusów przez programy antywirusowe.
  - **Wirus testowy**: 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.
  - 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.
  - **Inne**: Wirus/złośliwe oprogramowanie nieskategoryzowane jako żaden z rodzajów wirusów/złośliwego oprogramowania.

## 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 klienty 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 klient na atak.

W przypadku znalezienia aplikacji lub pliku niewykrywanego przez program Worry-Free Business Security 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 klient i mogą wymusić wybieranie wstępnie określonych numerów telefonu przez modem urządzenia typu klient. 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 klient, takie jak zamykanie i otwieranie tacy napędu CD-ROM lub wyświetlanie licznych okien komunikatów. |
| Narzędzie hakerskie | ułatwia hakerom uzyskiwanie dostępu do komputerów. |

| Typ | Opis |
|---|---|
| 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. |

## Spam

Spam obejmuje niezamówione wiadomości e-mail (wiadomości-śmieci), często o charakterze reklamowym, wysyłane masowo na wiele list pocztowych, do pojedynczych osób i grup dyskusyjnych. Istnieją dwa rodzaje spamu: niezamawiana poczta reklamowa (UCE) i niezamawiana poczta masowa (UBE).

## Włamania

Włamanie oznacza próbę uzyskania dostępu do sieci lub urządzeń typu klienty metodą siłową lub bez uprawnienia. Określenie to może także oznaczać obejście zabezpieczeń sieci lub urządzenia typu klient.

## Złośliwe zachowanie

Złośliwe zachowanie oznacza nieautoryzowane zmiany dokonane przez oprogramowanie w systemie operacyjnym, wpisach rejestru, innych programach bądź plikach i folderach.

## Fałszywe punkty dostępu

Fałszywe punkty dostępu (określane także jako „złe bliźniaki") to punkty dostępu Wi-Fi, które wydają się być prawidłowe, ale zostały skonfigurowane przez hakera w celu podsłuchiwania komunikacji bezprzewodowej.

## Zdarzenie typu phishing

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 witrynę, wobec której istnieje podejrzenie stosowania phishingu, należy zgłaszać firmie Trend Micro. Patrz *Przesyłanie podejrzanej zawartości do firmy Trend Micro na stronie C-5*, aby uzyskać więcej informacji.

## Ataki typu „mass-mailing”

Wirusy/złośliwe oprogramowanie używające poczty elektronicznej mogą rozprzestrzeniać się za pomocą wiadomości e-mail, automatyzując działania programu do obsługi poczty elektronicznej zainstalowanego na komputerze, lub poprzez rozprzestrzenianie samego wirusa/złośliwego oprogramowania. Działanie typu „mass-mailing” to sytuacja, gdy infekcja rozprzestrzenia się szybko w środowisku programu Microsoft Exchange. Firma Trend Micro opracowała mechanizm skanowania do wykrywania zachowań, które wykazują zazwyczaj ataki typu „mass-mailing”. Zachowania te są zapisane w pliku sygnatur wirusów, który jest aktualizowany poprzez serwery Trend Micro ActiveUpdate.

Program Messaging Security Agent (tylko w wersji Advanced) może podejmować specjalne operacje przeciwko atakom typu „mass mailing" za każdym razem, gdy wykryje działanie typu „mass mailing". Akcja ustawiona dla ataku typu „mass mailing" ma pierwszeństwo przed wszystkimi innymi akcjami. Domyślna akcja wykonywana przeciw atakom typu „mass mailing" to usunięcie całej wiadomości.

Na przykład: Program Messaging Security Agent został skonfigurowany tak, aby poddawał kwarantannie wiadomości, jeśli wykryje, że są zarażone robakiem lub trojanem. Zostanie również włączone wykrywanie zachowania typu „mass mailing", a agent zostanie ustawiony na usuwanie wszystkich wiadomości wykazujących zachowanie typu „mass mailing". Agent odbiera wiadomość zawierającą robaka, na przykład odmianę robaka MyDoom. Ten robak wykorzystuje własny silnik SMTP do rozsyłania się pod adresy e-mail, które gromadzi z zarażonego komputera. W przypadku wykrycia robaka MyDoom i rozpoznania jego zachowania typu mass-mailing przez agenta wiadomość zawierająca robaka zostanie usunięta — w przeciwieństwie do kwarantanny stosowanej w przypadku robaków niewykazujących zachowania typu „mass mailing".

## Zagrożenia z sieci WWW

Zagrożenia internetowe to różne typy zagrożeń pochodzących 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 zainfekowanym urządzeniu typu klient, autor 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. Zarażone urządzenie typu klient 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 sieci Web, 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”.

# Rozdział 2

# Wprowadzenie

W tym rozdziale omówiono sposób instalacji i uruchamiania programu Worry-Free Business Security.

# Worry-Free Business Security Network

Rozwiązanie Worry-Free Business Security składa się z następujących elementów:


- *Program Security Server na stronie 2-2*
- *Agenty na stronie 2-4*
- *Konsola internetowa na stronie 2-4*


# Program Security Server

Podstawowym elementem pakietu Worry-Free Business Security jest program Security Server. Program Security Server zawiera konsolę internetową — scentralizowaną internetową konsolę do zarządzania programem Worry-Free Business Security. Program Security Server instaluje agenty na klientach w sieci i nawiązuje z tymi agentami relacje typu agent-serwer. Program Security Server umożliwia wyświetlanie informacji o stanie zabezpieczeń, przeglądanie agentów, konfigurowanie zabezpieczeń systemu i pobieranie składników ze scentralizowanej lokalizacji. Program Security Server zawiera także bazę danych, w której przechowywane są dzienniki wykrytych i zgłoszonych przez agenty zagrożeń internetowych.

Program Security Server spełnia następujące ważne funkcje:

- Instaluje i monitoruje agenty oraz zarządza nimi.
- Pobiera składniki, których potrzebują agenty. Domyślnie program Security Server pobiera składniki z serwera Trend Micro ActiveUpdate, a następnie rozsyła je do agentów.

## Scan Server

Na serwerze Security Server dostępna jest usługa o nazwie Scan Server, która jest instalowana automatycznie podczas instalacji serwera Security Server. W związku z tym nie ma potrzeby instalowania jej osobno. Usługa Scan Server zostaje uruchomiona w ramach procesu o nazwie `iCRCService.exe` i jest wyświetlana pod nazwą **Usługa Trend Micro Smart Scan** w konsoli Microsoft Management Console.

Gdy programy Security Agent korzystają z metody skanowania o nazwie **Smart Scan**, usługa Scan Server pomaga tym agentom w skuteczniejszym skanowaniu. Proces Smart Scan można opisać w następujący sposób:

- Program Security Agent skanuje klienta pod kątem zagrożeń bezpieczeństwa, korzystając z **Sygnatura agenta usługi Smart Scan**, lżejszej wersji tradycyjnej sygnatury wirusów. W sygnaturze agenta usługi Smart Scan znajduje się większość sygnatur zagrożeń dostępnych w sygnaturze wirusów.
- Program Security Agent, który podczas skanowania nie jest w stanie określić, czy plik stanowi zagrożenie, sprawdza to, wysyłając zapytanie o skanowanie do usługi Scan Server. Usługa Scan Server sprawdza zagrożenie, korzystając z sygnatury **Smart Scan Pattern**, która zawiera sygnatury zagrożeń niedostępne w sygnaturze agenta usługi Smart Scan.
- Program Security Agent umieszcza wynik zapytania o skanowanie uzyskany od usługi Scan Server w pamięci podręcznej w celu zwiększenia wydajności skanowania.

Dzięki hostowaniu niektórych definicji zagrożeń usługa Scan Server pomaga zmniejszyć obciążenie sieci podczas pobierania składników przez programy Security Agent. Zamiast pobierać sygnaturę wirusów, programy Security Agent pobierają sygnaturę agenta usługi Smart Scan, której rozmiar jest znacznie mniejszy.

Gdy programy Security Agent nie są w stanie uzyskać połączenia z usługą Scan Server, wysyłają żądania skanowania do serwera Trend Micro Smart Protection Network, pełniącego tę samą funkcję, co usługa Scan Server.

Nie ma możliwości odinstalowania usługi Scan Server bez odinstalowywania serwera Security Server. Jeśli nie chcesz korzystać z usługi Scan Server:

1. Na komputerze będącym serwerem Security Server otwórz konsolę Microsoft Management Console i wyłącz opcję **Usługa Trend Micro Smart Scan**.
2. W konsoli internetowej ustaw dla programów Security Agent skanowanie standardowe, przechodząc do karty **Administracja** > **Ustawienia globalne** > **Komputer/serwer** i zaznaczając opcję **Wyłącz usługę skanowania Smart Scan**.

# Agenty

Agenty chronią klienty przed zagrożeniami. Klienty to komputery, serwery oraz serwery Microsoft Exchange. Agentami programu Worry-Free Business Security są:

**TABELA 2-1. Agenty programu Worry-Free Business Security**

| AGENT | OPIS |
|---|---|
| Security Agent | Chroni komputery i serwery przed zagrożeniami i atakami. |
| Programy Messaging Security Agent (tylko w wersji Advanced) | Chroni serwery Microsoft Exchange przed zagrożeniami pochodzącymi z wiadomości e-mail. |

Agent podlega programowi Security Server, z którego został zainstalowany. Aby dostarczyć programowi Security Server najświeższe informacje o kliencie, agent przesyła w czasie rzeczywistym informacje o stanie zdarzeń. Raportowane są takie zdarzenia, jak wykrycie wirusa, uruchomienie lub zamknięcie agenta, rozpoczęcie skanowania i zakończenie aktualizacji.

# Konsola internetowa

Konsola internetowa to centralny punkt monitorowania programów Security Agent w całej sieci firmowej. Zawiera zestaw ustawień domyślnych i wartości, które można skonfigurować zależnie od wymagań zabezpieczeń i specyfikacji. W konsoli Web zastosowano standardowe technologie internetowe, takie jak Java, CGI, HTML i HTTP.

Za pomocą konsoli internetowej można:

- Instalować agentów na punktach końcowych
- Organizować agenty w grupy logiczne w celu ich równoczesnego konfigurowania i zarządzania nimi.
- Konfigurować ustawienia produktu i rozpocząć skanowanie ręczne na punktach końcowych.

- Odbierać powiadomienia i przeglądać raporty dziennika dotyczące działań związanych z zagrożeniami.
- Odbierać powiadomienia i wysyłać alarmy o epidemii za pośrednictwem wiadomości e-mail po wykryciu zagrożeń na punktach końcowych.

## Otwieranie konsoli Web

Konsolę Web można otworzyć z dowolnego punktu końcowego w sieci za pomocą obsługiwanej przeglądarki. Aby uzyskać więcej informacji na temat wymagań przeglądarki, zapoznaj się z dokumentem *Wymagania systemowe*.

---

**Procedura**

1. Aby otworzyć konsolę internetową, wybierz jedną z następujących opcji:
   - Na punkcie końcowym, na którym zainstalowany jest program Security Server, przejdź na pulpit i kliknij skrót do programu Worry-Free Business Security.
   - Na punkcie końcowym, na którym zainstalowany jest program Security Server, kliknij następujące pozycje: **menu Start systemu Windows** > **Trend Micro Worry-Free Business Security** > **Worry-Free Business Security**.
   - Na dowolnym punkcie końcowym w sieci otwórz przeglądarkę internetową i wpisz następujące dane na pasku adresu:

     `https://{nazwa_serwera_zabezpieczeń lub adres IP}:{numer portu}/SMB`

     Na przykład:

     `https://serwer-testowy:4343/SMB`

     `https://192.168.0.10:4343/SMB`

     `http://serwer-testowy:8059/SMB`

     `http://192.168.0.10:8059/SMB`

**Porada**

Jeśli NIE JEST używany protokół SSL, wpisz ciąg `http` zamiast `https`. Domyślny port dla połączeń HTTP to 8059, a dla połączeń HTTPS to 4343.

Jeśli w danym środowisku nie jest możliwe rozpoznawanie nazw serwerów przez serwer DNS, zamiast adresów IP użyj nazw serwerów.

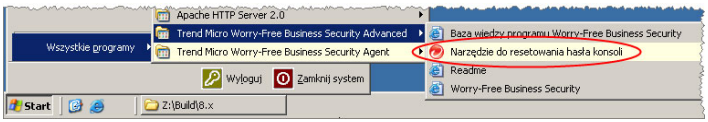
W przeglądarce wyświetlony zostanie ekran logowania do programu Worry-Free Business Security.

2. Wprowadź hasło i kliknij polecenie **Zaloguj się**.

   W przeglądarce zostanie wyświetlony ekran **Stan aktywności**.

## Co dalej

Jeśli nie możesz uzyskać dostępu do konsoli internetowej, sprawdź następujące kwestie.

| ELEMENT DO SPRAWDZENIA | SZCZEGÓŁY |
|---|---|
| Hasło | Jeżeli nie pamiętasz hasła, użyj narzędzia do resetowania hasła konsoli. Dostęp do tego narzędzia można uzyskać przy użyciu programu Security Server w folderze Trend Micro Worry-Free Business Security w menu Start systemu Windows.<br>  |
| Pamięć podręczna przeglądarki | W przypadku uaktualnienia programu Worry-Free Business Security z poprzedniej wersji pliki pamięci podręcznej przeglądarki internetowej oraz serwera proxy mogą uniemożliwić uruchomienie konsoli internetowej. Wyczyść pamięć podręczną przeglądarki internetowej oraz pamięć podręczną wszystkich serwerów proxy znajdujących się między programem Trend Micro Security Server a punktem końcowym, z którego uzyskiwany jest dostęp do konsoli Web. |

| Element do sprawdzenia | Szczegóły |
|---|---|
| Certyfikat SSL | Sprawdź poprawność działania serwera internetowego. W przypadku stosowania protokołu SSL należy sprawdzić poprawność certyfikatu SSL. Szczegółowe informacje można znaleźć w dokumentacji serwera internetowego. |
| Ustawienia katalogu wirtualnego | Jeśli konsolę internetową uruchomiono na serwerze IIS i zostanie wyświetlony poniższy komunikat, oznacza to, że mógł wystąpić problem z ustawieniami katalogu wirtualnego:<br>`Nie można wyświetlić strony`<br>`HTTP Error 403.1 - Zabronione: Odmowa dostępu do wykonywania.`<br>`Internetowe usługi informacyjne (IIS)`<br>Komunikat ten może zostać wyświetlony, gdy w celu uzyskania dostępu do konsoli użyto jednego z następujących adresów:<br>`http://{nazwa serwera}/SMB/`<br>`http://{nazwa serwera}/SMB/default.htm`<br>Jednak konsola otwiera się bez problemów, gdy zostaje użyty następujący adres:<br>`http://{nazwa serwera}/SMB/console/html/cgi/cgichkmasterpwd.exe`<br>W celu rozwiązania tego problemu należy sprawdzić uprawnienia wykonywania katalogu wirtualnego SMB.<br>Aby włączyć skrypty:<br>1. Otwórz menedżera Internetowe usługi informacyjne (IIS).<br>2. W katalogu wirtualnym SMB wybierz pozycję **Właściwości**.<br>3. Wybierz kartę Katalog wirtualny i zmień uprawnienia do wykonywania z ustawienia `Brak` na ustawienie `Skrypty`. Zmień także uprawnienia wykonywania katalogu wirtualnego instalacji klienta. |

# Nawigacja w konsoli internetowej

Konsola internetowa zawiera następujące główne sekcje:

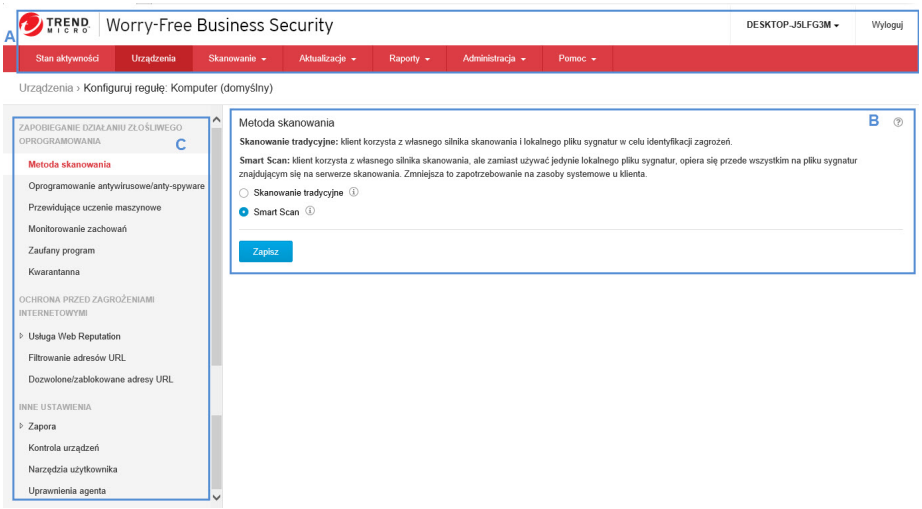



**TABELA 2-2. Główne sekcje konsoli internetowej**

| SEKCJA | OPIS |
|---|---|
| A. Menu główne | W górnej części konsoli internetowej znajduje się menu główne.<br><br>Dostępne jest również łącze **Wylogowywanie**, za pomocą którego można zakończyć bieżącą sesję. |
| B.<br><br>Obszar konfiguracji | Pod pozycjami menu głównego znajduje się obszar konfiguracji. Ten obszar można wykorzystać do wyboru opcji i konfiguracji ustawień, zależnych od wybranej pozycji menu. |

| SEKCJA | OPIS |
|---|---|
| C.<br>Pasek boczny menu (nie jest dostępny na wszystkich ekranach) | Po wybraniu grupy programów Security Agent na ekranie **Urządzenia** i kliknięciu opcji **Konfiguruj regułę** zostanie wyświetlony pasek boczny menu. Za pomocą paska bocznego można skonfigurować ustawienia zabezpieczeń oraz skanowania komputerów i serwerów należących do tej grupy.<br><br>Po wybraniu programu Messaging Security Agent na ekranie **Urządzenia** (tylko w wersji Advanced) można za pomocą paska bocznego skonfigurować ustawienia zabezpieczeń i skanowania dla serwerów Microsoft Exchange. |

**TABELA 2-3. Sekcja głównego menu**

| POZYCJA MENU | OPIS |
|---|---|
| Stan aktywności | Monitoruj ogólny stan zabezpieczeń programów Security Agent i status działania serwera Security Server |
| Urządzenia | • Dostosowywanie ustawień zabezpieczeń dotyczących agentów<br>• Replikowanie ustawień pomiędzy grupami |
| Skanowanie | • Skanuj punkty końcowe pod kątem zagrożeń<br>• Planowanie skanowania klientów |
| Aktualizacje | • Sprawdzanie na serwerze Trend Micro ActiveUpdate (lub w niestandardowym źródle aktualizacji) dostępności najnowszych zaktualizowanych składników, takich jak pliki sygnatur wirusów, silnik skanowania, składniki czyszczenia oraz program agenta<br>• Konfigurowanie źródła aktualizacji<br>• Określanie programów Security Agent jako agentów aktualizacji |
| Raporty | Generowanie raportów w celu śledzenia zagrożeń i innych zdarzeń związanych z zabezpieczeniami |

| Pozycja menu | Opis |
|---|---|
| Administracja | • Konfigurowanie powiadomień o wystąpieniu niestandardowych zdarzeń związanych z zagrożeniem lub systemem.<br>• Konfigurowanie ustawień globalnych w celu ułatwienia obsługi.<br>• Korzystanie z narzędzi do zarządzania w celu zarządzania bezpieczeństwem sieci i klientami<br>• Wyświetlanie informacji o licencji produktu, zarządzanie hasłem administratora oraz ułatwienie utrzymania stałego bezpieczeństwa środowiska wymiany informacji cyfrowych w firmie poprzez przystąpienie do programu Smart Feedback.<br>• Automatyczne pobieranie aktualizacji produktu i powiadamianie użytkowników o udostępnieniu nowego pakietu aktualizacji. |
| Pomoc | • Wyszukiwanie określonych materiałów i tematów<br>• Wyświetlanie podręcznika administratora<br>• Korzystanie z najnowszych informacji dostępnych w bazie wiedzy<br>• Wyświetlanie informacji o zabezpieczeniach, sprzedaży, pomocy technicznej i wersji |

## Ikony konsoli internetowej

Poniższa tabela zawiera opis ikon wyświetlanych w konsoli internetowej oraz objaśnienia, do czego służą.

**Tabela 2-4. Ikony konsoli internetowej**

| Ikona | Opis |
|---|---|
| | Ikona Pomoc. Służy do otwierania pomocy elektronicznej. |
| | Ikona Odśwież. Odświeża widok bieżącego ekranu. |
| | Ikona zwijania/rozwijania sekcji. Powoduje zwinięcie/rozwinięcie sekcji. Można rozwinąć jednocześnie tylko jedną sekcję. |

| IKONA | OPIS |
|---|---|
| | Ikona Informacje. Służy do wyświetlania informacji dotyczących określonego elementu. |
| | Ikona Dostosuj powiadomienia. Wyświetla opcje powiadomień. |

# Rozdział 3

# instalowanie agentów

W tym rozdziale objaśniono czynności niezbędne do zainstalowania programów Security Agent i Messaging Security Agent (tylko w wersji Advanced). Znajdują się tu również informacje na temat usuwania tych agentów.

# Instalacja programu Security Agent

Zainstaluj od nowa program Security Agent na klientach Windows (komputerach i serwerach). Użyj metody instalacji, która najlepiej odpowiada Twoim wymaganiom.

Przed rozpoczęciem instalacji programu Security Agent na klientach należy zamknąć wszystkie uruchomione aplikacje. Jeżeli podczas instalacji są uruchomione inne aplikacje, proces ten może potrwać dłużej.

**Uwaga**

Informacje o uaktualnianiu programów Security Agent do tej wersji zawiera *Podręcznik instalacji i uaktualniania*.

## Wymagania dotyczące instalacji programu Security Agent

Pełna lista wymagań dotyczących instalacji oraz zgodnych produktów innych firm jest dostępna pod adresem:

http://docs.trendmicro.com/pl-pl/smb/worry-free-business-security.aspx

## Uwagi dotyczące instalacji programu Security Agent

Przed zainstalowaniem programu Security Agent należy rozważyć poniższe kwestie:

- **Funkcje agenta:** Niektóre funkcje programu Security Agent są niedostępne na określonych platformach Windows. Aby uzyskać więcej informacji, zobacz *Dostępne funkcje programu Security Agent na stronie 3-3*.
- **Platformy x64**: dostępna jest uproszczona wersja programu Security Agent dla platform opartych na architekturze x64. Jednak nie jest obecnie możliwa obsługa platform o architekturze IA-64.
- **Obsługa IPv6**: program Security Agent można zainstalować na punktach końcowych z dwoma stosami lub wykorzystujących wyłącznie protokół IPv6. Z niektórymi metodami instalacji mogą być jednak powiązane szczególne wymagania.

Aby uzyskać więcej informacji, zobacz *Instalacja programu Security Agent i obsługa protokołu IPv6 na stronie 3-5*.

- **Listy wyjątków**: sprawdź, czy listy wyjątków poniższych funkcji zostały prawidłowo skonfigurowane:
  - **Monitorowanie zachowania**: Dodaj krytyczne aplikacje klienckie do listy Dozwolone programy, aby uniemożliwić programowi Security Agent blokowanie tych aplikacji. Aby uzyskać więcej informacji, patrz *Konfigurowanie monitorowania zachowania na stronie 5-12*.
  - **Usługa Web Reputation**: Dodaj witryny internetowe uznawane za bezpieczne do Listy dozwolonych adresów URL, aby uniemożliwić programowi Security Agent blokowanie dostępu do tych witryn. Aby uzyskać więcej informacji, patrz *Konfigurowanie usługi Web Reputation dla programów Security Agent na stronie 5-23*.
- **Katalog instalacyjny agenta**: podczas instalacji programu Security Server wyświetlany jest monit o określenie katalogu instalacji agenta (domyślnie `$ProgramFiles\Trend Micro\Security Agent`). Aby instalować programy Security Agent w innym katalogu, określ nowy katalog w sekcji **Administracja** > **Ustawienia globalne** > **System** > **Instalacja programu Security Agent**.

## Dostępne funkcje programu Security Agent

Funkcje programu Security Agent dostępne na kliencie zależą od systemu operacyjnego. Podczas instalowania agenta w konkretnym systemie operacyjnym należy pamiętać o nieobsługiwanych funkcjach.

**TABELA 3-1. Funkcje programu Security Agent**

| FUNKCJA | SYSTEM OPERACYJNY WINDOWS | | | | | |
|---|---|---|---|---|---|---|
| | 7 | 8.1 | 10 | SERVER/ SBS 2008 | SERVER 2008 R2/SBS 2011 | SERVER 2012/2012 R2/2016 |
| Skanowanie ręczne, skanowanie w czasie rzeczywistym i skanowanie zaplanowane | Tak | Tak | Tak | Tak | Tak | Tak |
| Zapora | Tak | Tak | Tak | Tak | Tak | Tak |
| Usługa Web Reputation | Tak | Tak | Tak | Tak | Tak | Tak |
| Filtrowanie adresów URL | Tak | Tak | Tak | Tak | Tak | Tak |
| Monitorowanie zachowania | Tak | Tak | Tak | Tak | Tak | Tak |
| Kontrola urządzeń | Tak | Tak | Tak | Tak | Tak | Tak |
| Usługi Damage Cleanup Services | Tak | Tak | Tak | Tak | Tak | Tak |
| Skanowanie poczty (POP3) | Tak | Tak | Tak | Tak | Tak | Tak |
| Aktualizacje ręczne i zaplanowane | Tak | Tak | Tak | Tak | Tak | Tak |

| Funkcja | System operacyjny Windows | | | | | |
|---|---|---|---|---|---|---|
| | 7 | 8.1 | 10 | Server/ SBS 2008 | Server 2008 R2/SBS 2011 | Server 2012/2012 R2/2016 |
| Agent aktualizacji | Tak | Tak | Tak | Tak | Tak | Tak |
| Menedżer dodatków agenta | Tak | Tak | Tak | Tak | Tak | Tak |
| Smart Feedback | Tak | Tak | Tak | Tak | Tak | Tak |
| Trend Micro Anti-Spam Toolbar | Tak | Tak | Tak | Nie | Nie | Nie |
| | Obsługiwane klienty e-mail:<br>• Microsoft Outlook 2007 (32-bitowy), 2010 (32- i 64-bitowy), 2013 (32- i 64-bitowy)<br>• Windows Live Mail 2011, 2012 | | | | | |
| HouseCall | Tak | Tak | Tak | Tak | Tak | Tak |
| Narzędzie Case Diagnostic Tool | Tak | Tak | Tak | Tak | Tak | Tak |
| Narzędzie Wi-Fi Advisor | Tak | Tak | Tak | Nie | Nie | Nie |

## Instalacja programu Security Agent i obsługa protokołu IPv6

W tym temacie omówiono kwestie związane z instalacją programu Security Agent na klientach z dwoma stosami lub wykorzystujących wyłącznie protokół IPv6.

### System operacyjny

Program Security Agent można zainstalować wyłącznie w następujących systemach operacyjnych, które obsługują adresowanie IPv6:

- Windows Server 2008/2008 R2 (wszystkie wersje)
- Windows 7 (wszystkie wersje)
- Windows SBS 2008/2011
- Windows 8,1 (wszystkie wersje)
- Windows 10 (wszystkie wersje)
- Windows Server 2012/2012 R2 (wszystkie wersje)
- Windows Server 2016 (Standard, Datacenter, Essentials)

Pełna lista wymagań systemowych jest dostępna pod adresem:

http://docs.trendmicro.com/pl-pl/smb/worry-free-business-security.aspx

### Obsługiwane metody instalacji

W celu zainstalowania programu Security Agent na klientach z dwoma stosami lub wykorzystujących wyłącznie protokół IPv6 można użyć wszystkich dostępnych metod instalacji. W przypadku niektórych metod instalacji programu Security Agent jej powodzenie wymaga spełnienia specjalnych wymogów.

**TABELA 3-2. Metody instalacji i obsługa protokołu IPv6**

| METODA INSTALACJI | WYMAGANIA/UWAGI |
|---|---|
| Instalacja za pomocą wewnętrznej strony internetowej i powiadomienia przesyłanego pocztą e-mail | Jeśli instalacja odbywa się na kliencie wykorzystującym wyłącznie protokół IPv6, serwer Security Server musi mieć dwa stosy lub wykorzystywać wyłącznie protokół IPv6, a jego nazwa hosta lub adres IPv6 musi stanowić część adresu URL.<br><br>W przypadku klientów z dwoma stosami adres IPv6, który jest wyświetlany na ekranie stanu instalacji, zależy od opcji wybranej w sekcji **Preferowany adres IP** na karcie **Administracja** > **Ustawienia globalne** > **Komputer/serwer** |

| METODA INSTALACJI | WYMAGANIA/UWAGI |
|---|---|
| Narzędzie Vulnerability Scanner i instalacja zdalna | Serwer Security Server wykorzystujący wyłącznie protokół IPv6 nie umożliwia instalacji programu Security Agent na klientach wykorzystujących wyłącznie protokół IPv4. Analogicznie program Security Server wykorzystujący wyłącznie protokół IPv4 nie umożliwia instalacji agenta na klientach wykorzystujących wyłącznie protokół IPv6. |

### Adresy IP programu Security Agent

Serwer Security Server zainstalowany w środowisku obsługującym adresowanie IPv6 może zarządzać następującymi programami Security Agent:

- Serwer Security Server zainstalowany na kliencie wykorzystującym tylko protokół IPv6 może zarządzać klientami wykorzystującymi tylko protokół IPv6.
- Serwer Security Server zainstalowany na kliencie z dwoma stosami, do którego przypisano adresy IPv4 i IPv6, może zarządzać programami Security Agent wykorzystującymi wyłącznie protokół IPv6, z dwoma stosami i wykorzystującymi wyłącznie protokół IPv4.

Po zainstalowaniu lub zaktualizowaniu programy Security Agent rejestrują się na serwerze Security Server przy użyciu adresu IP.

- Programy Security Agent wykorzystujące wyłącznie protokół IPv6 rejestrują się przy użyciu adresu IPv6.
- Programy Security Agent wykorzystujące wyłącznie protokół IPv4 rejestrują się przy użyciu adresu IPv4.
- Programy Security Agent z dwoma stosami rejestrują się przy użyciu adresu IPv4 lub IPv6. Adres używany przez te agenty można wybrać w sekcji **Preferowany adres IP** na karcie **Administracja** > **Ustawienia globalne** > **Komputer/serwer**.

## Metody instalacji programu Security Agent

W tym rozdziale zawarto podsumowanie różnych metod nowej instalacji programu Security Agent. Wszystkie metody instalacji wymagają posiadania uprawnień administratora na docelowych punktach końcowych.

Jeśli podczas instalowania programów Security Agent konieczne jest włączenie obsługi protokołu IPv6, należy zapoznać się z wytycznymi w temacie *Instalacja programu Security Agent i obsługa protokołu IPv6 na stronie 3-5*.

**TABELA 3-3. Metody instalacji**

| METODA INSTALACJI / OBSŁUGA SYSTEMU OPERACYJNEGO | UWAGI DOTYCZĄCE INSTALACJI | | | | | |
|---|---|---|---|---|---|---|
| | WDROŻENIE SIECI WAN | ZARZĄDZANIE CENTRALNE | WYMAGA UDZIAŁU UŻYTKOWNIKA | WYMAGA ZASOBÓW INFORMATYCZNYCH | INSTALACJA MASOWA | WYKORZYSTANIE ŁĄCZA |
| **Wewnętrzna strona internetowa**<br>Obsługiwana we wszystkich systemach operacyjnych | Tak | Tak | Tak | Nie | Nie | Niskie (przy instalacji zaplanowanej) |
| **Powiadomienie e-mail**<br>Obsługiwana we wszystkich systemach operacyjnych | Tak | Tak | Tak | Nie | 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**<br>Obsługiwana we wszystkich systemach operacyjnych z wyjątkiem<br>• Windows 7<br>• Windows 8,1<br>• Windows 10 | Nie | Tak | Nie | Tak | Tak | Niskie (przy instalacji zaplanowanej) |
| **Ustawienia skryptu logowania**<br>Obsługiwana we wszystkich systemach operacyjnych | Nie | Tak | Nie | Tak | Tak | Wysokie, jeśli instalacje rozpoczynają się jednocześnie |
| **Client Packager**<br>Obsługiwana we wszystkich systemach operacyjnych | Tak | Nie | Tak | Tak | Nie | Niskie (przy instalacji zaplanowanej) |

| Metoda instalacji / Obsługa systemu operacyjnego | Uwagi dotyczące instalacji | | | | | |
|---|---|---|---|---|---|---|
| | Wdrożenie sieci WAN | Zarządzanie centralne | Wymaga udziału użytkownika | Wymaga zasobów informatycznych | Instalacja masowa | Wykorzystanie łącza |
| **Narzędzie Trend Micro Vulnerability Scanner (TMVS)**<br>Obsługiwana we wszystkich systemach operacyjnych z wyjątkiem<br>• Windows 7<br>• Windows 8,1<br>• Windows 10 | Nie | Tak | Nie | Tak | Tak | Niskie (przy instalacji zaplanowanej) |

W przypadku instalacji w jednym oddziale oraz w organizacjach o restrykcyjnych regułach IT administratorzy mogą skorzystać z **instalacji zdalnej** lub **ustawienia skryptu logowania**.

W organizacjach, w których reguły IT nie są tak ściśle przestrzegane, firma Trend Micro zaleca instalację programów za pomocą **wewnętrznej strony internetowej**. Z tej metody mogą jednak korzystać tylko użytkownicy końcowi instalujący program Security Agent z uprawnieniami administratora.

**Instalacja zdalna** sprawdza się w przypadku sieci z usługą Active Directory. Jeśli w sieci nie ma usługi Active Directory, należy użyć wewnętrznej strony internetowej.

# Instalowanie z wewnętrznej strony internetowej

## Przed rozpoczęciem

Instalacja z wewnętrznej strony internetowej wymaga spełnienia następujących warunków:

| ELEMENT DO SPRAWDZENIA | WYMAGANIE |
|---|---|
| Program Security Server | Program Security Server musi zostać zainstalowany w następujących systemach:<br>• Windows 7, 8.1, Server 2008, 2008 R2, 2012, 2012 R2, 2016, lub SBS 2008, 2011<br>• z serwerem Internet Information Server (IIS) 7.0, 7.5, 8.0, 8.5, 10 lub Apache 2.4 |
| Docelowy punkt końcowy | • Docelowy punkt końcowy musi być zainstalowany w systemach Windows 7, 8, 8.1, 10, Server 2008, 2008 R2, 2012, 2012 R2, 2016 lub SBS 2008, 2011.<br>• Na docelowym punkcie końcowym musi być zainstalowany program Internet Explorer w wersji 9.0 lub nowszej.<br>• Aby móc zalogować się na punkcie końcowym, użytkownicy muszą korzystać z konta administratora.<br><br>**Uwaga**<br>Jeśli na docelowym punkcie końcowym zainstalowany jest system Windows 7, należy najpierw włączyć wbudowane konto administratora. System Windows 7 domyślnie wyłącza wbudowane konto administratora.<br>Więcej informacji znajduje się na stronie pomocy firmy Microsoft (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx). |

| ELEMENT DO SPRAWDZENIA | WYMAGANIE |
|---|---|
| Ustawienia zabezpieczeń programu Internet Explorer | Użytkownicy muszą wykonać następujące czynności:<br>1. Uruchom program Internet Explorer i dodaj adres URL serwera Security Server (na przykład `https://<nazwa serwera Security Server>:4343/SMB/console/html/client`) do listy zaufanych witryn. Uzyskaj dostęp do listy, klikając kolejno pozycje **Narzędzia** > **Opcje internetowe** > **,karta Zabezpieczenia**, wybierając ikonę **Zaufane witryny** i klikając pozycję **Witryny**.<br>2. Zmień ustawienia zabezpieczeń programu Internet Explorer, aby włączyć opcję **Automatyczne monitowanie dla formantów ActiveX**. Można to zrobić, klikając pozycje **Narzędzia** > **Opcje internetowe** > **karta Zabezpieczenia** i klikając pozycję **Poziom niestandardowy**. |
| IPv6 | W środowisku łączonym, składającym się z punktów końcowych wykorzystujących tylko protokół IPv4, tylko protokół IPv6 oraz klientów z dwoma stosami, program Security Server musi mieć zarówno adres IPv4, jak i adres IPv6. Dzięki temu wszystkie punkty końcowe będą mogły łączyć się z wewnętrzną stroną internetową na serwerze Security Server. |

Do użytkowników należy przesłać pocztą elektroniczną instrukcje instalacji programu Security Agent z wewnętrznej strony internetowej. Informacje na temat wysyłania drogą elektroniczną powiadomienia o instalacji znajdują się w sekcji *Instalowanie za pomocą powiadomienia e-mail na stronie 3-34*.

---

**Procedura**

1. Zaloguj się na punkcie końcowym, używając konta administratora.
2. Otwórz program Internet Explorer i wpisz jeden z poniższych adresów:
   - Serwer Security Server z połączeniem SSL:

     `https://<nazwa serwera Security Server lub adres IP>:4343/SMB/console/html/client`

   - Serwer Security Server bez połączenia SSL:

```
http://<nazwa serwera Security Server lub adres IP>:
8059/SMB/console/html/client
```

3. Kliknij opcję **Instaluj teraz**, aby rozpocząć instalację programu Security Agent.

   Rozpocznie się instalacja. Po wyświetleniu monitu zezwól na instalację formantu ActiveX. Po instalacji na pasku zadań systemu Windows pojawi się ikona programu Security Agent.

**Uwaga**

Informacje o liście ikon wyświetlanych na pasku zadań systemu Windows zawiera sekcja *Sprawdzanie stanu programu Security Agent na stronie A-2*.

### Co dalej

Jeśli użytkownicy zgłaszają, że nie mogą przeprowadzić instalacji za pomocą wewnętrznej strony internetowej, wypróbuj następujące metody rozwiązania problemu.

- Sprawdź, używając polecenia ping lub telnet, czy istnieje komunikacja między punktem końcowym a serwerem.
- Sprawdź, czy na punkcie końcowym włączono i poprawnie skonfigurowano protokół TCP/IP.
- Jeżeli do komunikacji punkt końcowy-serwer używany jest serwer proxy, sprawdź, czy jego ustawienia są prawidłowe.
- W przeglądarce internetowej usuń dodatki firmy Trend Micro i historię przeglądania.

## Instalowanie za pomocą skryptu logowania

Ustawienia skryptu logowania pozwalają zautomatyzować proces instalacji programu Security Agent na niezabezpieczonych klientach zaraz po ich zalogowaniu się w sieci. Ustawienia skryptu logowania powodują dodanie programu `AutoPcc.exe` do skryptu logowania serwera.

Program `AutoPcc.exe` instaluje program Security Agent na niezabezpieczonych klientach i aktualizuje pliki programów oraz składniki oprogramowania. Korzystanie

z programu AutoPcc za pośrednictwem skryptu logowania jest możliwe tylko na klientach należących do domeny.

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

Na końcu skryptu narzędzie Ustawienia skryptu logowania dopisuje następujące informacje:

```
\\<Server_name>\ofcscan\autopcc
```

Gdzie:

- `<Server_name>` to nazwa lub adres IP komputera, na którym zainstalowano program Security Server.
- „`ofcscan`" to nazwa udostępnionego folderu na serwerze Security Server.
- „`autopcc`" to łącze do pliku wykonywalnego autopcc, który zainstaluje program Security Agent.

Lokalizacja skryptu logowania we wszystkich wersjach systemu Windows Server (poprzez udostępniony katalog logowania do sieci):

```
\\Windows server\system drive\windir\sysvol\domain\scripts
\ofcscan.bat
```

---

**Procedura**

1. Na komputerze używanym do uruchomienia instalacji serwera otwórz `<folder instalacji programu Security Server>\PCCSRV\Admin`.
2. Kliknij dwukrotnie plik `SetupUsr.exe`.

   Zostanie załadowane narzędzie **Ustawienia skryptu logowania**. Na konsoli zostanie wyświetlone drzewo ze wszystkimi domenami sieci.
3. 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.

4. 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.

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

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

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

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

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

   Zostanie wyświetlony komunikat informujący o pomyślnej modyfikacji skryptów logowania serwera.

10. Kliknij przycisk **OK**.

    Narzędzie Ustawienia skryptu logowania powróci do ekranu początkowego.

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

## Instalowanie za pomocą narzędzia Client Packager

Program Client Packager tworzy pakiet instalacyjny, który można wysłać do użytkowników na nośniku tradycyjnym, na przykład na dysku CD-ROM. Użytkownicy uruchamiają pakiet na kliencie, aby zainstalować lub zaktualizować program Security Agent i zaktualizować jego składniki.

Program Client Packager jest szczególnie przydatny:

- Podczas instalowania programu Security Agent lub jego składników na klientach w zdalnych oddziałach z łączem internetowym o niskiej przepustowości.
- Jeśli w środowisku występują ograniczenia dotyczące połączenia internetowego, w przypadku występowania zamkniętej sieci lokalnej lub braku połączenia internetowego.

Programy Security Agent zainstalowane przy użyciu programu Client Packager przesyłają do serwera informacje o lokalizacji, w której utworzono pakiet.

---

**Procedura**

1. Na komputerze z programem Security Server przejdź do folderu `<folder instalacji serwera>\PCCSRV\Admin\Utility\ClientPackager`.
2. Kliknij dwukrotnie plik `ClnPack.exe`.

   Zostanie otwarta konsola programu Client Packager.
3. Wybierz system operacyjny, do którego chcesz utworzyć pakiet. Zainstaluj pakiet tylko na klientach, na których jest zainstalowany system operacyjny odpowiedniego typu. W przypadku zamiaru instalacji w systemie operacyjnym innego typu należy utworzyć kolejny pakiet.
4. Wybierz metodę skanowania dla pakietu.

   Szczegółowe informacje o metodach skanowania zawiera temat *Metody skanowania na stronie 5-3*.

   W zależności od wybranej metody skanowania do pakietu są dołączane różne składniki. W przypadku zastosowania skanowania Smart Scan uwzględnione zostaną wszystkie składniki poza sygnaturą wirusów. W przypadku skanowania konwencjonalnego uwzględnione zostaną wszystkie składniki poza sygnaturą agenta usługi Smart Scan.
5. Wybierz typ pakietu, który chcesz utworzyć.

**TABELA 3-4. Typy pakietów klienta**

| TYP PAKIETU | OPIS |
|---|---|
| Instaluj | Wybierz opcję **Instaluj**, aby utworzyć pakiet w postaci pliku MSI zgodnego z formatem Microsoft Installer Package. Pakiet zainstaluje program Security Agent ze składnikami aktualnie dostępnymi na serwerze Security Server.<br><br>Jeśli na kliencie docelowym zainstalowana jest wcześniejsza wersja programu Security Agent i chcesz ją uaktualnić, utwórz plik MSI za pomocą serwera Security Server, który zarządza danym agentem. W przeciwnym wypadku agent nie zostanie uaktualniony. |
| Aktualizuj | Wybierz polecenie **Aktualizuj**, aby utworzyć pakiet zawierający składniki obecnie dostępne na serwerze Security Server. Pakiet zostanie utworzony jako plik wykonywalny. Użyj tego pakietu, jeśli na kliencie, na którym zainstalowany jest program Security Agent, wystąpią problemy z uaktualnianiem składników. |

6. Kliknij opcję **Tryb cichy**, aby utworzyć pakiet, który instaluje się niezauważalnie w tle na kliencie bez wyświetlania okna stanu instalacji. Tę opcję należy włączyć w przypadku zamiaru zdalnej instalacji pakietu na kliencie.

7. Jeśli przed instalowaniem programu Security Agent nie chcesz skanować klientów pod kątem zagrożeń, kliknij opcję **Wyłącz skanowanie wstępne (tylko w przypadku nowej instalacji)**. Zrób to, jeśli masz pewność, że dany klient jest wolny od zagrożeń.

   Jeśli funkcja wstępnego skanowania jest włączona, instalator skanuje pod względem wirusów / złośliwego oprogramowania najbardziej narażone na ataki obszary komputera:

   - Obszar rozruchowy i katalog rozruchowy (pod kątem wirusów sektora rozruchowego)
   - Folder Windows
   - Folder Program files

8. 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 plik ten znajduje się w lokalizacji `<folder instalacji serwera>\PCCSRV`.

9. W obszarze Plik wyjściowy ( ... ) określ lokalizację, w której ma zostać utworzony pakiet klienta, a następnie wpisz nazwę pliku (na przykład `ClientSetup.exe`).

10. Kliknij przycisk **Utwórz**.

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

## Co dalej

Zainstaluj pakiet na klientach.

**Wymagania dotyczące klientów:**

- 1 GB wolnego miejsca na dysku, jeśli jako metodę skanowania pakietu wybrano skanowanie konwencjonalne, 500 MB w przypadku Smart Scan.
- Instalator Windows 4.5 lub nowszy (aby uruchomić pakiet MSI)

**Wytyczne dotyczące instalacji pakietu:**

- Wyślij pakiet do użytkowników i poleć im, aby uruchomili pakiet, klikając dwukrotnie plik (`.msi` lub `.exe`).

  **Uwaga**

  Wyślij pakiet tylko do użytkowników, których programy Security Agent podlegają serwerowi, na którym utworzono pakiet.

- Poinstruuj użytkowników, aby kliknęli plik pakietu prawym przyciskiem myszy i wybrali opcję **Uruchom jako administrator**.
- Używając usługi Active Directory, można automatycznie zainstalować program Security Agent na wszystkich klientach jednocześnie za pomocą pliku `.msi`. Nie jest wówczas konieczne, aby każdy użytkownik instalował program Security Agent samodzielnie. Aby można było zainstalować program Security Agent niezależnie od tego, który użytkownik zaloguje się na kliencie, zamiast opcji **Konfiguracja użytkownika** użyj opcji **Konfiguracja komputera**.

- Jeśli nowo zainstalowany program Security Agent nie może połączyć się z serwerem Security Server, zachowa ustawienia domyślne. Po połączeniu się z serwerem Security Server program Security Agent uzyska ustawienia dla swojej grupy w konsoli internetowej.
- Jeżeli występują problemy z uaktualnianiem programu Security Agent przy użyciu programu Client Packager, firma Trend Micro zaleca odinstalowanie poprzedniej wersji programu Security Agent, a następnie zainstalowanie nowej. Instrukcje odinstalowania programu zawiera sekcja *Usuwanie agentów na stronie 3-41*.

## Instalowanie za pomocą instalacji zdalnej

### Przed rozpoczęciem

Program Security Agent można zainstalować zdalnie na jednym lub wielu punktach końcowych podłączonych do sieci.

Aby zainstalować program zdalnie, muszą być spełnione następujące wymagania:

| ELEMENT DO SPRAWDZENIA | WYMAGANIE |
|---|---|
| Docelowy punkt końcowy | • Do logowania na każdym docelowym punkcie końcowym należy używać konta administratora.<br><br>**Uwaga**<br>• Jeśli na docelowym punkcie końcowym zainstalowany jest system Windows 7, należy najpierw włączyć wbudowane konto administratora. System Windows 7 domyślnie wyłącza wbudowane konto administratora.<br><br>Więcej informacji znajduje się na stronie pomocy firmy Microsoft (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx).<br>• Podczas wykonywania zdalnej instalacji w systemie Windows 8/8.1 lub 10 nie można użyć konta Microsoft w celu zalogowania na kliencie docelowym.<br><br>• Na docelowym punkcie końcowym nie może być zainstalowany program Security Server. Na punkcie końcowym, na którym jest |

<table>
<tr><th>Element do sprawdzenia</th><th>Wymaganie</th></tr>
<tr><td></td><td>już zainstalowany program Security Server, nie da się zainstalować zdalnie programu Security Agent.</td></tr>
<tr><td>Udostępnianie plików i drukarek</td><td>Na punkcie końcowym włącz tymczasowo usługę Udostępnianie plików i drukarek.<br><br>Uwaga<br>Jeśli firmowa reguła bezpieczeństwa wymaga wyłączenia Zapory systemu Windows, przejdź od razu do sekcji Rejestr zdalny.<br><br>1. Uruchom zaporę systemu Windows w Panelu sterowania.<br>2. Kliknij polecenie Zezwalaj programowi na dostęp przez Zaporę systemu Windows. Jeśli zostanie wyświetlony monit o wpisanie hasła administratora lub potwierdzenie, wpisz hasło lub potwierdź. Zostanie wyświetlone okno ustawień Zapory systemu Windows.<br>3. Sprawdź, czy zaznaczone jest pole wyboru Udostępnianie plików i drukarek na karcie Wyjątki w obszarze Lista programów lub portów.<br>4. Kliknij przycisk OK.<br>5. W razie potrzeby po zainstalowaniu agentów Security Agent przywróć oryginalne ustawienia.</td></tr>
<tr><td>Kontrola konta użytkownika</td><td>Wyłącz kontrolę konta użytkownika.<br><br>Uwaga<br>Zmodyfikuj następujący klucz rejestru, aby wyłączyć kontrolę konta użytkownika: <code>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] “EnableLUA”=dword:00000000.</code><br><br>W razie potrzeby po zainstalowaniu agentów Security Agent przywróć oryginalne ustawienia.</td></tr>
</table>

| ELEMENT DO SPRAWDZENIA | WYMAGANIE |
|---|---|
| Rejestr zdalny | Uruchom tymczasowo usługę Rejestr zdalny.<br>1. **Uwaga**<br>W oknie Uruchom wpisz ciąg `services.msc`, aby uruchomić konsolę Microsoft Management Console.<br>2. Kliknij prawym przyciskiem myszy pozycję **Rejestr zdalny** i wybierz opcję **Uruchom**.<br>3. W razie potrzeby po zainstalowaniu agentów Security Agent przywróć oryginalne ustawienia. |
| IPv6 | Za pomocą programu Security Server z dwoma stosami można zainstalować program Security Agent na dowolnym punkcie końcowym. Za pomocą programu Security Server wykorzystującego tylko protokół IPv6 można zainstalować program Security Agent wyłącznie na punktach końcowych wykorzystujących tylko protokół IPv6 lub dwa stosy. |

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Kliknij pozycję **Dodaj urządzenia**.
3. W obszarze **Typ komputera** wybierz pozycję **Komputer lub serwer**.
4. W obszarze **Metoda** wybierz opcję **Zdalna instalacja**.
5. Kliknij przycisk **Dalej**.

   Zostanie wyświetlony nowy ekran.
6. Wybierz klienta z listy klientów w oknie **Grupy i komputery** i kliknij przycisk **Dodaj**. Zostanie wyświetlony monit o podanie nazwy użytkownika i hasła dla klienta.
7. Wpisz nazwę użytkownika i hasło, a następnie kliknij przycisk **Zaloguj**. Klient pojawi się na liście **Wybrane komputery**.

8. Powtarzaj te etapy, aż lista w oknie **Wybrane komputery** będzie zawierać wszystkie klienty.

9. Kliknij opcję **Instaluj**.

   Zostanie wyświetlone okno potwierdzenia.

10. Kliknij przycisk **Tak**, aby potwierdzić chęć instalacji agenta na klientach.

    Podczas kopiowania plików programu Security Agent na każdego klienta zostanie wyświetlony ekran postępu.

    Gdy program Security Server zakończy instalację na kliencie, informacje o stanie instalacji zostaną wyświetlone w polu **Status** na liście **Wybrane komputery**, a obok nazwy klienta pojawi się zielony symbol wyboru.

### Co dalej

Jeśli instalacja zdalna się nie powiedzie, wykonaj następujące czynności:

- Sprawdź, używając polecenia ping lub telnet, czy istnieje komunikacja między klientem a serwerem.
- Sprawdź, czy na kliencie włączono i poprawnie skonfigurowano protokół TCP/IP.
- Jeżeli do komunikacji klient-serwer używany jest serwer proxy, sprawdź, czy jego ustawienia są prawidłowe.
- W przeglądarce internetowej usuń dodatki firmy Trend Micro i historię przeglądania.

## Instalowanie za pomocą narzędzia Vulnerability Scanner

### Przed rozpoczęciem

Narzędzie Vulnerability Scanner służy do wykrywania zainstalowanych rozwiązań antywirusowych, wyszukiwania w sieci niechronionych klientów oraz instalowania na nich programów Security Agent.

Aby zainstalować narzędzie Vulnerability Scanner, muszą być spełnione następujące wymagania:

| ELEMENT DO SPRAWDZENIA | WYMAGANIE |
|---|---|
| Miejsce uruchamiania narzędzia Vulnerability Scanner | Narzędzie Vulnerability Scanner można uruchomić na serwerze Security Server albo na dowolnym kliencie w sieci. Na kliencie nie powinien działać program Terminal Server. |
| Klient docelowy | • Na kliencie docelowym nie może być zainstalowany program Security Server. Narzędzie Vulnerability Scanner nie zainstaluje programu Security Agent na kliencie, na którym działa już program Security Server.<br>• Aby móc zalogować się na kliencie, użytkownicy muszą korzystać z konta administratora.<br><br>**Uwaga**<br>Jeśli na kliencie docelowym zainstalowany jest system Windows 7, należy najpierw włączyć wbudowane konto administratora. System Windows 7 domyślnie wyłącza wbudowane konto administratora. Więcej informacji znajduje się na stronie pomocy firmy Microsoft (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx). |

Istnieje kilka sposobów uruchamiania skanowania narażenia na atak.

- *Uruchamianie ręcznego skanowania narażenia na atak na stronie 3-23*
- *Uruchamianie skanowania DHCP na stronie 3-25*
- *Konfigurowanie zaplanowanego skanowania narażenia na atak na stronie 3-28*

## Uruchamianie ręcznego skanowania narażenia na atak

Uruchom skanowanie narażenia na atak na żądanie.

**Procedura**

1. Uruchom narzędzie Vulnerability Scanner.

| Aby włączyć narzędzie Vulnerability Scanner: | Czynności |
|---|---|
| Program Security Server | a. Przejdź do `<folderu instalacji serwera>\PCCSRV\Admin\Utility\TMVS`.<br>b. Kliknij dwukrotnie plik `TMVS.exe`. |
| Klient w sieci | a. W programie Security Server przejdź do `<folderu instalacji serwera>\PCCSRV\Admin\Utility`.<br>b. Skopiuj folder `TMVS` na innego klienta.<br>c. Na innym kliencie otwórz folder `TMVS` i kliknij dwukrotnie plik `TMVS.exe`. |

2. Przejdź do sekcji **Skanowanie ręczne**.
3. Wpisz zakres adresów IP klientów, które mają być skanowane.
   a. Wpisz zakres adresów IPv4.

> **Uwaga**
>
> Narzędzie Vulnerability Scanner umożliwia sprawdzanie zakresu adresów IPv4 tylko w przypadku uruchomienia go na kliencie wykorzystującym wyłącznie protokół IPv4 lub na kliencie 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 kliencie wykorzystującym wyłącznie protokół IPv6 lub na kliencie z dwoma stosami.

4. Kliknij **Ustawienia**.

   Zostanie wyświetlony ekran **Ustawienia**.

5. Skonfiguruj ustawienia skanowania narażenia na atak. Aby uzyskać więcej informacji, zobacz *Ustawienia skanowania narażenia na atak na stronie 3-30*.

6. Kliknij przycisk **OK**.

   Ekran Ustawienia zostanie zamknięty.

7. Kliknij przycisk **Start**.

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

   **Uwaga**

   Jeśli na komputerze jest uruchomiony system operacyjny Windows Server 2008, 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

Uruchom skanowanie narażenia na atak na komputerach uzyskujących adres IP z serwera DHCP.

Narzędzie Vulnerability Scanner nasłuchuje na porcie 67, który stanowi port nasłuchiwania serwera DHCP dla żądań DHCP. Po wykryciu żądania DHCP od klienta 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 lub Windows 7.

**Procedura**

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

**TABELA 3-5. Ustawienia DHCP w pliku `TMVS.ini`**

| USTAWIANIE | OPIS |
|---|---|
| DhcpThreadNum=x | Liczba wątków trybu DHCP. Minimalna wartość to 3, a maksymalna — 100. Domyślna wartość to 3. |
| DhcpDelayScan=x | To wyrażone w sekundach opóźnienie przed sprawdzeniem instalacji programu antywirusowego na komputerze wysyłającym żądanie.<br>Minimalna wartość to 0 (nie czekaj), a maksymalna — 600. Domyślna wartość to 60. |
| LogReport=x | Wartość 0 wyłącza rejestrowanie, 1 — włącza.<br>Narzędzie Vulnerability Scanner wysyła wyniki skanowania do serwera Worry-Free Business Security. Dzienniki są wyświetlane na ekranie **Dzienniki zdarzeń systemowych** w konsoli Web. |
| OsceServer=x | Jest to adres IP lub nazwa DNS serwera Worry-Free Business Security. |
| OsceServerPort=x | Jest to port serwera Web na serwerze Worry-Free Business Security. |

2. Uruchom narzędzie Vulnerability Scanner.

| ABY WŁĄCZYĆ NARZĘDZIE VULNERABILITY SCANNER: | CZYNNOŚCI |
|---|---|
| Program Security Server | a. Przejdź do `<folderu instalacji serwera>\PCCSRV\Admin\Utility\TMVS`.<br>b. Kliknij dwukrotnie plik `TMVS.exe`. |

| ABY WŁĄCZYĆ NARZĘDZIE VULNERABILITY SCANNER: | CZYNNOŚCI |
|---|---|
| Klient w sieci | a. W programie Security Server przejdź do `<folderu instalacji serwera>\PCCSRV\Admin\Utility`.<br>b. Skopiuj folder `TMVS` na innego klienta.<br>c. Na innym kliencie otwórz folder `TMVS` i kliknij dwukrotnie plik `TMVS.exe`. |

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

   Zostanie wyświetlony ekran **Ustawienia**.

4. Skonfiguruj ustawienia skanowania narażenia na atak. Aby uzyskać więcej informacji, zobacz *Ustawienia skanowania narażenia na atak na stronie 3-30*.

5. Kliknij przycisk **OK**.

   Ekran Ustawienia zostanie zamknięty.

6. Na karcie **Wyniki** kliknij kartę **Skanowanie DHCP**.

   **Uwaga**

   Karta **Skanowanie DHCP** jest niedostępna na komputerach z systemem operacyjnym Windows 2008 oraz Windows 7.

7. Kliknij przycisk **Uruchom DHCP**.

   Narzędzie Vulnerability Scanner rozpocznie nasłuchiwanie żądań DHCP i sprawdzi narażenie klientów 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

Skanowania narażenia na atak są uruchamiane zgodnie z harmonogramem.

**Procedura**

1. Uruchom narzędzie Vulnerability Scanner.

| ABY WŁĄCZYĆ NARZĘDZIE VULNERABILITY SCANNER: | CZYNNOŚCI |
|---|---|
| Program Security Server | a. Przejdź do `<folderu instalacji serwera>\PCCSRV\Admin\Utility\TMVS`.<br>b. Kliknij dwukrotnie plik `TMVS.exe`. |
| Klient w sieci | a. W programie Security Server przejdź do `<folderu instalacji serwera>\PCCSRV\Admin\Utility`.<br>b. Skopiuj folder `TMVS` na innego klienta.<br>c. Na innym kliencie otwórz folder `TMVS` i kliknij dwukrotnie plik `TMVS.exe`. |

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 komputerów, 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, który ma dostępny adres IPv4. 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, który ma dostępny adres IPv6.

6. Określ godzinę rozpoczęcia przy użyciu 24-godzinnego formatu czasu, a następnie ustal częstotliwość wykonywania skanowania. codziennie, raz w tygodniu lub raz w miesiącu.

7. 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 3-23*.

   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**. Skonfiguruj ustawienia skanowania i kliknij przycisk **OK**. Aby uzyskać więcej informacji, zobacz *Ustawienia skanowania narażenia na atak na stronie 3-30*.

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 komputerze jest uruchomiony system operacyjny Windows Server 2008, 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**.

11. Aby zatrzymać uruchamianie zaplanowanych skanowań narażenia na atak, przejdź do obszaru **Skanowania zaplanowane**, zaznacz skanowanie zaplanowane i kliknij przycisk **Usuń**.

## Ustawienia skanowania narażenia na atak

Podczas uruchamiania skanowania narażenia na atak należy skonfigurować poniższe ustawienia. Szczegółowe informacje na temat różnych rodzajów skanowania narażenia na atak zawiera część *Instalowanie za pomocą narzędzia Vulnerability Scanner na stronie 3-22*.

| USTAWIENIA | OPIS I INSTRUKCJE |
|---|---|
| Kwerenda dotycząca produktu | Narzędzie Vulnerability Scanner może sprawdzać obecność oprogramowania zabezpieczającego na klientach docelowych.<br>1. Wybierz oprogramowanie zabezpieczające do sprawdzenia.<br>2. Podczas sprawdzania oprogramowania narzędzie Vulnerability Scanner korzysta z domyślnych portów wyświetlanych na ekranie. Jeśli administrator oprogramowania zmienił porty domyślnie, należy wprowadzić niezbędne zmiany, aby umożliwić narzędziu Vulnerability Scanner wykrycie oprogramowania.<br>3. W przypadku narzędzia Norton Antivirus Corporate Edition można zmienić ustawienia limitu czasu za pomocą przycisku **Ustawienia**. |
| | **Ustawienia kwerendy dotyczącej innego produktu**<br>Aby ustawić liczbę klientów, które narzędzie Vulnerability Scanner będzie jednocześnie sprawdzać po kątem oprogramowania zabezpieczającego:<br>1. Przejdź do pozycji `<Folder instalacji serwera>\PCCSRV\Admin\Utility\TMVS` i otwórz plik `TMVS.ini` za pomocą edytora tekstu, np. Notatnika.<br>2. Aby ustawić liczbę sprawdzanych klientów:<br>• W przypadku ręcznego skanowania narażenia na atak zmień wartość `ThreadNumManual`. Określ wartość między 8 a 64.<br>Można na przykład wpisać wartość `ThreadNumManual=60`, aby narzędzie Vulnerability Scanner sprawdzało jednocześnie 60 klientów.<br>• W przypadku zaplanowanego skanowania narażenia na atak zmień wartość `ThreadNumSchedule`. Podaj wartość między 8 a 64.<br>Można na przykład wpisać wartość `ThreadNumSchedule=50`, aby narzędzie Vulnerability Scanner sprawdzało jednocześnie 50 klientów.<br>3. Zapisz plik `TMVS.ini`. |

| Ustawienia | Opis i instrukcje |
|---|---|
| Ustawienia pobierania opisów | Gdy narzędzie Vulnerability Scanner może wysyłać polecenia ping do klientów, możliwe jest uzyskanie dodatkowych informacji o tych klientach. Istnieją dwie metody pobierania informacji:<br>• **Normalne pobieranie**: są pobierane informacje o domenie i komputerze.<br>• **Szybkie pobieranie**: jest pobierana tylko nazwa komputera. |
| Ustawienia ostrzeżeń | Aby automatycznie wysyłać wyniki narzędzia Vulnerability Scan do administratorów w organizacji:<br>1. Wybierz opcję **Wyślij wyniki pocztą e-mail do administratora systemu**.<br>2. Kliknij opcję **Konfiguruj**, aby określić ustawienia poczty e-mail.<br>3. W polu **Do** wpisz adres e-mail odbiorcy.<br>4. W polu **Od** wpisz adres e-mail nadawcy.<br>5. W polu **Serwer SMTP** wpisz adres serwera SMTP.<br>Przykładowy adres to `smtp.firma.com`. Informacja o serwerze SMTP jest wymagana.<br>6. W polu **Temat** wpisz nowy temat wiadomości lub zatwierdź domyślny.<br>7. Kliknij przycisk **OK**.<br>Aby poinformować użytkowników, że na ich komputerach nie jest zainstalowane żadne oprogramowanie zabezpieczające:<br>1. Wybierz opcję **Wyświetl powiadomienie na niechronionych komputerach**.<br>2. Kliknij polecenie **Dostosuj**, aby skonfigurować powiadomienia programu.<br>3. Na ekranie **Powiadomienie programu** wpisz treść nowej wiadomości lub zatwierdź domyślną wiadomość.<br>4. Kliknij przycisk **OK**. |

| USTAWIENIA | OPIS I INSTRUKCJE |
|---|---|
| Zapisywanie jako plik CSV | Wyniki skanowania narażenia na atak można zapisać do pliku rozdzielanego przecinkami (CSV).<br><br>Plik zostanie zapisany na kliencie, na którym uruchomiono narzędzie Vulnerability Scanner. Zaakceptuj domyślną ścieżkę do pliku lub zmień ją zgodnie z preferencjami. |
| Ustawienia polecenia ping | Ustawienia polecenia ping umożliwiają sprawdzenie istnienia klienta i określenie jego systemu operacyjnego. Jeśli ustawienia te są wyłączone, narzędzie Vulnerability Scanner skanuje wszystkie adresy IP w określonym zakresie — nawet te, które nie są używane przez żadnego klienta — przez co skanowanie trwa dłużej, niż powinno.<br><br>1. W polach **Rozmiar pakietu** i **Limit czasu** zaakceptuj lub zmodyfikuj wartości domyślne.<br><br>2. Wybierz opcję **Wykryj typ systemu operacyjnego za pomocą pakietu identyfikacyjnego ICMP OS**.<br><br>Jeśli wybierzesz tę opcję, narzędzie Vulnerability Scanner będzie sprawdzać, czy na kliencie działa system operacyjny Windows lub inny system. W przypadku klientów z systemem Windows narzędzie Vulnerability Scanner może zidentyfikować wersję systemu Windows. |
| | **Inne ustawienia polecenia ping**<br><br>Aby ustawić liczbę klientów, do których narzędzie Vulnerability Scanner będzie jednocześnie wysyłać polecenie ping:<br><br>1. Przejdź do pozycji `<Folder instalacji serwera>\PCCSRV\Admin\Utility\TMVS` i otwórz plik `TMVS.ini` za pomocą edytora tekstu, np. Notatnika.<br><br>2. Zmień wartość opcji `EchoNum`. Podaj wartość między 1 a 64.<br><br>Przykładowo można wpisać wartość `EchoNum=60`, aby narzędzie Vulnerability Scanner wysyłało polecenie ping jednocześnie do 60 klientów.<br><br>3. Zapisz plik `TMVS.ini`. |

| Ustawienia | Opis i instrukcje |
|---|---|
| Ustawienia programu Security Server | 1. Aby zainstalować program Security Agent na klientach, które będą skanowane przez narzędzie Vulnerability Scanner, wybierz opcję **Automatycznie instaluj program Security Agent na niezabezpieczonych komputerach**.<br>2. Wpisz nazwę hosta programu Security Server lub adres IPv4/IPv6 i numer portu. Programy Security Agent zainstalowane przez narzędzie Vulnerability Scanner będą podlegać temu serwerowi.<br>3. Skonfiguruj poświadczenia administracyjne używane podczas logowania na klientach, klikając przycisk **Konto instalacyjne**. Na ekranie **Informacje o koncie** wpisz nazwę użytkownika i hasło, a następnie kliknij przycisk **OK**. |

## Instalowanie za pomocą powiadomienia e-mail

Tej metody instalacji należy użyć, aby wysłać wiadomość e-mail zawierającą łącze do programu instalacyjnego.

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Kliknij pozycję **Dodaj urządzenia**.
3. W obszarze **Typ komputera** wybierz pozycję **Komputer lub serwer**.
4. W sekcji **Metoda** wybierz opcję **Instalacja za pomocą powiadomienia e-mail**.
5. Kliknij przycisk **Dalej**.

   Zostanie wyświetlony nowy ekran.
6. Wprowadź temat wiadomości e-mail i odbiorców.
7. Kliknij przycisk **Zastosuj**. Zostanie otwarte okno domyślnego programu do obsługi poczty elektronicznej z wprowadzonymi odbiorcami, tematem oraz łączem do programu instalacyjnego produktu.

# Migracja do programu Security Agent

Podczas instalowania programu Security Agent program instalacyjny sprawdza, czy na kliencie jest zainstalowane oprogramowanie zabezpieczające punkt końcowy firmy Trend Micro lub innego producenta.

Program instalacyjny może wykonać następujące operacje:

- Usunąć inne oprogramowanie zabezpieczające punkt końcowy zainstalowane obecnie na kliencie i zastąpić je programem Security Agent.
- Wykryć inne oprogramowanie zabezpieczające punkt końcowy, ale nie usuwać go.

Lista oprogramowania zabezpieczającego punkt końcowy jest dostępna pod adresem:

http://esupport.trendmicro.com/solution/en-US/1060980.aspx

Jeśli oprogramowania zainstalowanego na kliencie nie można usunąć automatycznie lub da się je tylko wykryć, ale nie można go usunąć, należy je najpierw odinstalować ręcznie. W zależności od procesu dezinstalacji oprogramowania klient może wymagać ponownego uruchomienia.

## Problemy z migracją i możliwe rozwiązania

Automatyczna dezinstalacja oprogramowania zabezpieczającego punkt końcowy dostarczonego przez inną firmę może się nie powieść z następujących powodów:

- Numer wersji lub klucz produktu oprogramowania innej firmy jest nieprawidłowy.
- Dezinstalator oprogramowania innej firmy nie działa.
- Niektóre pliki wchodzące w skład oprogramowania innej firmy są uszkodzone lub ich brakuje.
- Klucz rejestru oprogramowania innej firmy nie może zostać usunięty.
- Oprogramowanie innej firmy nie ma dezinstalatora.

Możliwe rozwiązania tych problemów:

- Usuń oprogramowanie innej firmy ręcznie.
- Zatrzymać usługę oprogramowania innej firmy.

- Usunąć z pamięci usługę lub proces oprogramowania innej firmy.

## Wykonywanie zadań po instalacji w programach Security Agent

**Procedura**

1. Sprawdź następujące elementy:
   - Skróty programu Security Agent są dostępne w menu Start systemu Windows na punkcie końcowym.
   - Program **Trend Micro Worry-Free Business Security Agent** znajduje się na liście Dodaj/usuń programy w Panelu sterowania klienta na punkcie końcowym.
   - Program Security Agent jest widoczny na ekranie **Urządzenia** w konsoli internetowej i należy do grupy **Serwery (domyślne)** lub **Komputery (domyślne)** zależnie od typu systemu operacyjnego na punkcie końcowym.

     **Uwaga**

     Jeśli nie widzisz programu Security Agent, uruchom zadanie sprawdzenia połączenia, używając pozycji **Administracja** > **Ustawienia globalne** > **karta System** > **Sprawdzanie połączenia agenta**.

   - W konsoli **Microsoft Management Console** są wyświetlane następujące usługi programu Security Agent:
     - Trend Micro Security Agent Listener (`tmlisten.exe`).
     - Trend Micro Security Agent RealTime Scan (`ntrtscan.exe`).
     - Trend Micro Security Agent NT Proxy (`TmProxy.exe`).

       **Uwaga**

       Ta usługa jest dostępna tylko w systemie Windows 2008.

- Trend Micro Security Agent Firewall (`TmPfw.exe`), jeśli została włączona podczas instalacji
- Trend Micro Unauthorized Change Prevention (`TMBMSRV.exe`), jeśli podczas instalacji włączono funkcję monitorowania zachowania lub kontroli urządzeń
- Trend Micro Common Client Solution Framework (`TmCCSF.exe`)

2. Jeśli program Security Agent nie jest widoczny w konsoli internetowej, być może nie był w stanie przesłać swojego stanu do serwera. Wykonaj jedną z następujących operacji:

   - Otwórz przeglądarkę internetową na kliencie, w polu adresu wpisz `https://{nazwa_serwera_Trend Micro Security Server}:{numer portu}/SMB/cgi/cgionstart.exe`, a następnie naciśnij klawisz ENTER.

     Jeżeli na następnym ekranie zostanie wyświetlona wartość -2, oznacza to, że agent może komunikować się z serwerem. Wskazuje to też na możliwość występowania problemu w bazie danych serwera — może brakować rekordu agenta.

   - Sprawdź, używając polecenia ping lub telnet, czy istnieje komunikacja między klientem a serwerem.
   - Jeżeli masz ograniczoną przepustowość, sprawdź, czy nie jest to powodem przekroczenia limitu czasu połączenia między serwerem a klientem.
   - Sprawdź, czy folder `\PCCSRV` na serwerze ma uprawnienia udostępniania i czy wszystkim użytkownikom zostały przyznane pełne uprawnienia do kontroli tego folderu.
   - Sprawdź, czy ustawienia proxy programu Trend Micro Security Server są prawidłowe.

3. Sprawdź działanie programu Security Agent za pomocą skryptu testowego EICAR.

   Europejski Instytut Badań Nad Wirusami Komputerowymi (European Institute for Computer Antivirus Research, EICAR) opracował testowego „wirusa", którego można używać do sprawdzenia instalacji i konfiguracji. Plik ten jest plikiem tekstowym, którego sygnatura binarna jest zawarta w pliku sygnatur wirusów

dostarczanym przez większość producentów oprogramowania antywirusowego. Nie jest on wirusem i nie zawiera żadnego kodu programowego.

Wirusa testowego instytutu EICAR można pobrać z witryny dostępnej pod następującym adresem URL:

http://www.eicar.org/anti_virus_test_file.htm

Można także utworzyć własnego wirusa testowego EICAR, wpisując następujący ciąg w pliku tekstowym, a następnie nadając mu nazwę „eicar.com":

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
```

**Uwaga**

Przed rozpoczęciem testów należy oczyścić pamięć podręczną serwera i lokalnej przeglądarki internetowej.

# Instalacja programu Messaging Security Agent

Programy Messaging Security Agent można zainstalować tylko w razie korzystania z programu Worry-Free Business Security w wersji Advanced.

Zainstaluj od nowa program Messaging Security Agent na serwerach Microsoft Exchange.

**Uwaga**

Informacje o uaktualnianiu programów Messaging Security Agent do tej wersji zawiera Podręcznik instalacji i uaktualniania.

## Wymagania dotyczące instalacji programu Messaging Security Agent

Pełna lista wymagań dotyczących instalacji jest dostępna pod adresem:

http://docs.trendmicro.com/pl-pl/smb/worry-free-business-security.aspx

# Instalowanie programu Messaging Security Agent (tylko w wersji Advanced)

## Przed rozpoczęciem

Uwagi i wymagania dotyczące instalacji:

- Nie ma konieczności zatrzymywania lub uruchamiania usług Microsoft Exchange przed rozpoczęciem lub zakończeniem instalacji.
- Jeżeli na punkcie końcowym zapisane są informacje z poprzedniej instalacji programu Messaging Security Agent, instalacja nowej wersji programu nie będzie możliwa. Użyj Panelu sterowania Windows do usunięcia pozostałości z poprzedniej instalacji.

  Patrz *Odinstalowywanie programu Messaging Security Agent z serwera Microsoft Exchange (tylko w wersji Advanced) na stronie 3-46*, aby uzyskać więcej informacji.
- W przypadku instalowania programu Messaging Security Agent na serwerze, na którym uruchomione są narzędzia blokowania, należy te narzędzia usunąć, aby nie wyłączały usługi IIS, bez której instalacja nie powiodłaby się.
- Program Messaging Security Agent można także zainstalować podczas instalacji programu Security Server. Szczegółowe informacje zawiera Podręcznik instalacji i uaktualniania.
- Program Messaging Security Agent nie obsługuje niektórych funkcji serwera Microsoft Exchange Server Enterprise, takich jak grupa dostępności danych.

---

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Kliknij pozycję **Dodaj urządzenia**.
3. Wybierz pozycję **Serwer Exchange**.
4. W obszarze **Informacje o serwerze Exchange** wpisz następujące informacje:

- **Nazwa serwera**: Nazwa serwera Microsoft Exchange, na którym chcesz zainstalować agenta.
- **Konto**: Nazwa użytkownika wbudowanego konta administratora domeny.
- **Hasło**: Hasło wbudowanego konta administratora domeny.

5. Kliknij przycisk **Dalej**.

   W kreatorze instalacji wyświetlony zostanie ekran, którego zawartość zależy od typu wykonywanej instalacji.

   - **Nowa instalacja**: Na serwerze Microsoft Exchange nie ma agenta, zostanie on dopiero zainstalowany.
   - **Uaktualnianie**: Na serwerze Microsoft Exchange jest zainstalowana poprzednia wersja agenta, która zostanie uaktualniona do bieżącej wersji.
   - **Instalacja nie jest wymagana**: Na serwerze Microsoft Exchange jest zainstalowana bieżąca wersja agenta. Jeśli agent nie jest obecnie widoczny w drzewie grup zabezpieczeń, zostanie automatycznie dodany.
   - **Nieprawidłowa instalacja**: Wystąpił problem z instalacją agenta.

   **Uwaga**

   W przypadku opcji **Typ zarządzania spamem** będzie używane narzędzie **End User Quarantine**.

6. W obszarze **Katalogi** zmień lub zaakceptuj domyślne katalogi docelowe i udostępnione do instalacji programu Messaging Security Agent. Domyślne katalogi docelowe i udostępniane to odpowiednio `C:\Program Files\Trend Micro\Messaging Security Agent` i `C$`.

7. Kliknij przycisk **Dalej**.

   Zostanie wyświetlony nowy ekran.

8. Sprawdź, czy ustawienia serwera Microsoft Exchange określone na poprzednich ekranach są poprawne, a następnie kliknij przycisk **Dalej**, aby rozpocząć instalację programu.

9. Aby wyświetlić stan instalacji programu, kliknij kartę **Stan aktywności**.

# Usuwanie agentów

Polecenie **Odinstaluj agenta** udostępnia następujące sposoby usuwania programów Security Agent i Messaging Security Agent (tylko w wersji Advanced):

- *Usuwanie agentów z konsoli internetowej na stronie 3-42*

  Użyj tej opcji w przypadku nieaktywnych agentów. Jeśli nieaktywny agent jest w konsoli internetowej stale widoczny jako znajdujący się w trybie offline, ponieważ klient, na którym go zainstalowano, został wyłączony na dłuższy czas lub sformatowany ponownie, można takiego agenta odinstalować.

  Podczas usuwania agentów z konsoli internetowej:

  - Jeśli agent nadal istnieje na kliencie, nie zostanie odinstalowany.
  - Serwer przestanie zarządzać agentem.
  - Jeśli agent ponownie zacznie komunikować się z serwerem (np. po włączeniu klienta), zostanie z powrotem dodany do konsoli. Program Security Agent zastosuje do niego ustawienia oryginalnej grupy. Jeśli grupa ta już nie istnieje, agent zostanie dodany do grupy **Serwery (domyślne)** lub **Komputery (domyślne)**, zależnie od systemu operacyjnego klienta, i zostaną do niego zastosowane ustawienia tej grupy.

  **Porada**

  Program WFBS udostępnia jeszcze jedną funkcję, która wykrywa nieaktywne agenty i usuwa je z konsoli internetowej. Funkcja ta pozwala zautomatyzować zadanie usuwania agentów. Aby użyć tej funkcji, przejdź do karty **Administracja** > **Ustawienia globalne** > **System**, a następnie do sekcji Usuwanie nieaktywnych programów Security Agent.

- *Odinstalowywanie agentów z konsoli internetowej na stronie 3-42*

  W przypadku wystąpienia problemów z programem agenta można go odinstalować (co spowoduje jego usunięcie z konsoli internetowej). Firma Trend Micro zaleca,

aby natychmiast zainstalować agenta ponownie w celu utrzymania ochrony klienta przed zagrożeniami.

## Usuwanie agentów z konsoli internetowej

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Aby usunąć programy Security Agent, wybierz grupę, a następnie wybierz agenty. Aby usunąć program Messaging Security Agent, wybierz go.

   **Porada**

   Aby wybrać wiele sąsiadujących programów Security Agent, kliknij pierwszego agenta w zakresie, przytrzymaj klawisz SHIFT i kliknij ostatniego agenta w zakresie. Aby wybrać nieciągły zakres agentów, kliknij pierwszego agenta w zakresie, przytrzymaj klawisz CTRL, a następnie klikaj agenty, które chcesz zaznaczyć.

3. Kliknij pozycję **Więcej** > **Odinstaluj agenta**.

   Zostanie wyświetlony nowy ekran.

4. Kliknij polecenie **Usuń wybrane agenty**.
5. Kliknij przycisk **Zastosuj**.

## Odinstalowywanie agentów z konsoli internetowej

Podczas odinstalowywania programu Messaging Security Agent usługa IIS Admin/serwer Apache i wszystkie usługi pokrewne zostaną automatycznie zatrzymane, a następnie uruchomione ponownie.

**Procedura**

1. Przejdź do menu **Urządzenia**.

2. Aby odinstalować programy Security Agent, wybierz grupę, a następnie wybierz agenty. Aby odinstalować program Messaging Security Agent, wybierz go.

**Porada**

Aby wybrać wiele sąsiadujących programów Security Agent, kliknij pierwszego agenta w zakresie, przytrzymaj klawisz SHIFT i kliknij ostatniego agenta w zakresie. Aby wybrać nieciągły zakres agentów, kliknij pierwszego agenta w zakresie, przytrzymaj klawisz CTRL, a następnie klikaj agenty, które chcesz zaznaczyć.

3. Kliknij pozycję **Więcej** > **Odinstaluj agenta**.

   Zostanie wyświetlony nowy ekran.

4. Kliknij polecenie **Odinstaluj wybrane agenty**.

5. Kliknij przycisk **Zastosuj**.

   Zostanie wyświetlony ekran zawierający informacje o liczbie powiadomień o odinstalowaniu wysłanych przez serwer oraz o liczbie agentów, które otrzymały powiadomienie.

**Uwaga**

W przypadku programu Messaging Security Agent po wyświetleniu monitu wpisz nazwę i hasło konta na serwerze Microsoft Exchange.

6. Kliknij przycisk **OK**.

7. Aby sprawdzić, czy agent został odinstalowany, odśwież ekran Ustawienia zabezpieczeń. Agent nie powinien już być widoczny w drzewie grup zabezpieczeń.

   Jeśli odinstalowanie programu Security Agent nie powiedzie się, zapoznaj się z częścią *Używanie narzędzia SA Uninstall na stronie 3-44*.

## Odinstalowywanie programu Security Agent z punktu końcowego

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.

Hasło można ustawić lub wyłączyć w obszarze **Administracja** > **Ustawienia globalne** > **karta Komputer/serwer** > **Hasło dezinstalacji programu Security Agent**.

---

**Procedura**

1. Kliknij **Panel sterowania** > **Dodaj lub usuń programy**.
2. Zlokalizuj program **Trend Micro Worry-Free Business Security Agent** i kliknij przycisk **Zmień** lub **Odinstaluj**, zależnie od tego, który z nich jest dostępny.
3. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Po wyświetleniu monitu wprowadź hasło dezinstalacji.

   Program Security Server powiadomi użytkownika o postępie odinstalowywania i jego zakończeniu. Użytkownik nie musi ponownie uruchamiać klienta w celu zakończenia odinstalowywania.

   Jeśli wykonanie tej procedury nie powiedzie się, zapoznaj się z częścią *Używanie narzędzia SA Uninstall na stronie 3-44*.

---

## Używanie narzędzia SA Uninstall

Użyj narzędzia SA Uninstall:

- Jeśli instalacja nie powiedzie się lub jeśli niezbędne jest całkowite odinstalowanie programu. Narzędzie automatycznie usuwa wszystkie składniki programu Security Agent z klienta.
- Aby odinstalować program Security Agent

---

**Procedura**

1. W programie Security Server przejdź do `<folderu instalacji serwera>\PCCSRV\Private`.

2. Skopiuj plik `SA_Uninstall.exe` na docelowy komputer kliencki.
3. Uruchom program `SA_Uninstall.exe` na kliencie docelowym.
4. Zaloguj się w systemie Windows jako administrator (lub za pomocą konta z uprawnieniami administratora).
5. Wykonuj kolejne czynności zadania, które zamierzasz zrealizować.

| ZADANIE | CZYNNOŚCI |
|---|---|
| Dezinstalacja programu Security Agent | a. Przejdź do katalogu narzędzia, kliknij prawym przyciskiem myszy plik **Uninstall.bat** i wybierz polecenie **Uruchom jako administrator**. Na ekranie **Kontrola konta użytkownika** wybierz opcję **Zgoda**.<br>b. Kiedy pojawi się komunikat **Czy chcesz teraz ponownie uruchomić komputer? (T/N)** wybierz jedną z opcji:<br>• **N [Enter]**: niektóre sterowniki zostaną odinstalowane dopiero po ponownym uruchomieniu komputera.<br>• **T [Enter]**: po 30-sekundowym odliczaniu nastąpi ponowne uruchomienie komputera.<br>Narzędzie SA Uninstall automatycznie zatrzyma agenta. |
| Zamykanie programu Security Agent | a. Przejdź do katalogu narzędzia, kliknij prawym przyciskiem myszy plik **Stop.bat** i wybierz polecenie **Uruchom jako administrator**. Na ekranie **Kontrola konta użytkownika** wybierz opcję **Zgoda**.<br>b. Upewnij się, że program zakończy działanie po zatrzymaniu klienta. |

## Odinstalowywanie programu Messaging Security Agent z serwera Microsoft Exchange (tylko w wersji Advanced)

Podczas odinstalowywania programu Messaging Security Agent usługa IIS Admin/ serwer Apache i wszystkie usługi pokrewne zostaną automatycznie zatrzymane, a następnie uruchomione ponownie.

**Procedura**

1. Zaloguj się na serwerze Microsoft Exchange z uprawnieniami administratora.
2. Kliknij pozycje **Panel sterowania** > **Odinstaluj program**.
3. Zlokalizuj program **Trend Micro Messaging Security Agent** i kliknij przycisk **Zmień**.
4. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

# Rozdział 4

# Zarządzanie urządzeniami

W programie Worry-Free Business Security ekran **Urządzenia** jest podzielony na dwie główne części.

- Drzewo urządzeń

  Drzewo urządzeń jest rozszerzalną listą grup logicznych. Grupami można ręcznie zarządzać na podstawie typu punktu końcowego lub można ręcznie konfigurować grupy i organizować programy Security Agent zgodnie z wymaganiami.

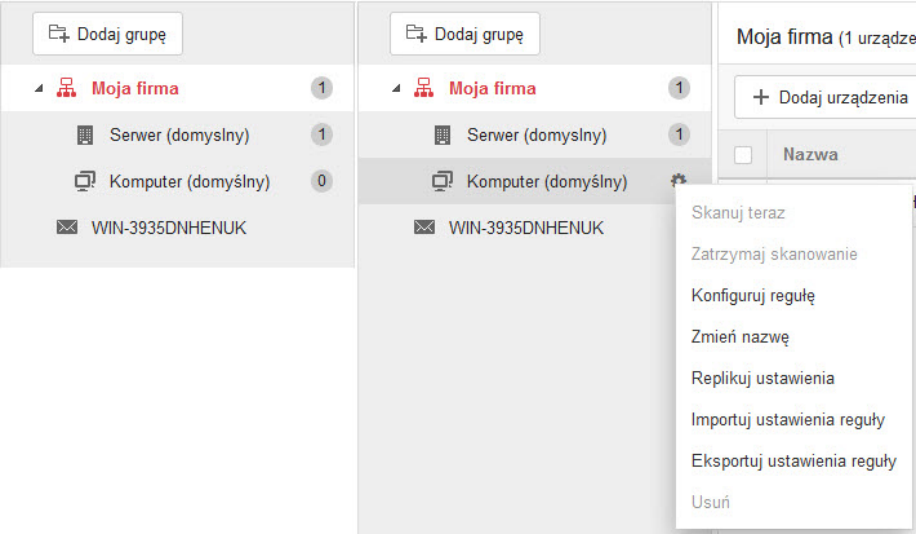
  Patrz *Korzystanie z drzewa urządzeń na stronie 4-2*, aby uzyskać więcej informacji.

- Tabela informacji o grupie

  Po wybraniu grupy z drzewa urządzeń po prawej stronie pojawi się lista programów Security Agent należących do grupy.

  Patrz *Używanie poleceń urządzenia na stronie 4-4*, aby uzyskać więcej informacji.

# Korzystanie z drzewa urządzeń




**ILUSTRACJA 4-1. Korzystanie z menu poleceń Drzewa urządzeń**

Aby otworzyć menu Drzewo urządzeń, wykonaj następujące czynności:

- Wybierz grupę z Drzewa urządzeń i kliknij ikonę koła zębatego obok nazwy grupy.
- Wybierz program Messaging Security Agent i kliknij ikonę koła zębatego obok nazwy grupy.

W zależności od wybranego rodzaju grupy niektóre polecenia są dostępne tylko w określonych typach grup lub mogą być wyłączone.

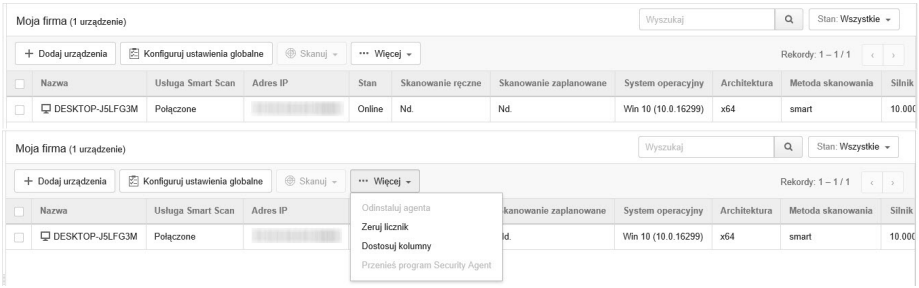
**TABELA 4-1. Polecenia Drzewa urządzeń**

| POLECENIE | OPIS |
|---|---|
| Dodaj grupę | Dodaje nową grupę do Drzewa urządzeń<br><br>Patrz *Dodawanie grup na stronie 4-8*, aby uzyskać więcej informacji. |

| POLECENIE | OPIS |
|---|---|
| **Skanuj teraz** | • Rozpoczyna skanowanie wszystkich punktów końcowych w wybranej grupie<br>• Rozpoczyna skanowanie serwera Exchange |
| **Zatrzymaj skanowanie** | • Kończy skanowanie wszystkich punktów końcowych w wybranej grupie<br>• Kończy skanowanie serwera Exchange |
| Skonfiguruj ustawienia globalne | Umożliwia skonfigurowanie ogólnych ustawień programu Security Agent w zakresie skanowania zabezpieczeń, listy zatwierdzonych/zablokowanych adresów URL, kontroli programu Security Agent oraz zarządzania urządzeniem.<br>Patrz *Ustawienia globalne na stronie 11-2*, aby uzyskać więcej informacji. |
| **Konfiguruj regułę** | • Konfiguruje następujące podstawowe ustawienia zabezpieczeń dla wszystkich programów Security Agent należących do wybranej grupy<br>Patrz *Zestawienie podstawowych ustawień zabezpieczeń w programach Security Agent na stronie 5-2*, aby uzyskać więcej informacji.<br>• Konfiguruje następujące podstawowe ustawienia zabezpieczeń dla wybranego programu Messaging Security Agent<br>Patrz *Zarządzanie podstawowymi ustawieniami zabezpieczeń w programach Messaging Security Agent (tylko w wersji Advanced) na stronie 6-1*, aby uzyskać więcej informacji. |
| Zmień nazwę | Zmienia nazwę wybranej grupy |
| Replikuj ustawienia | Kopiuje ustawienia z jednej grupy do drugiej. Programy Security Agent w grupie docelowej przyjmują te same ustawienia, co grupa źródłowa<br>Patrz *Replikowanie ustawień na stronie 4-16*, aby uzyskać więcej informacji. |

| POLECENIE | OPIS |
|---|---|
| Importuj ustawienia reguły | Importuje ustawienia uzyskane z innej grupy<br>Patrz *Importowanie i eksportowanie ustawień grup Security Agent na stronie 4-18*, aby uzyskać więcej informacji. |
| Eksportuj ustawienia reguły | Eksportuje ustawienia wybranej grupy<br>Patrz *Importowanie i eksportowanie ustawień grup Security Agent na stronie 4-18*, aby uzyskać więcej informacji. |
| Usuń | Usuwa grupę z Drzewa urządzeń |

# Używanie poleceń urządzenia




**ILUSTRACJA 4-2. Korzystanie z menu poleceń urządzenia**

Po wybraniu grupy z drzewa urządzeń po prawej stronie w tabeli pojawi się lista programów Security Agents w grupie. Pasek menu u góry tabeli zawiera polecenia, których można użyć do zarządzania programami Security Agent. W zależności od wybranego rodzaju grupy niektóre polecenia są dostępne tylko w określonych typach grup lub mogą być wyłączone.

Użyj paska wyszukiwania na górze ekranu **Urządzenia**, aby wyszukać punkty końcowe za pomocą nazw, etykiet lub adresów IP.

**Porada**

Aby wyszukać punkty końcowe w sieci, możesz wpisać fragment adresu IP. Na przykład wpisanie liczby „192” spowoduje zwrócenie wszystkich adresów IP z liczbą „192”, a wpisanie „192.” zwróci tylko adresy IP zaczynające się od „192”. Do wyszukiwania nazw punktów końcowych nie można jednak używać symboli wieloznacznych ani znaków specjalnych (*, +, (,), -, i).

**TABELA 4-2. Polecenia dotyczące urządzeń**

| POLECENIE | OPIS |
|---|---|
| **Dodaj urządzenia** | Instalowanie jednego z poniższych programów:<br>• Program **Security Agent** na punkcie końcowym (komputerze lub serwerze)<br>• Programu **Messaging Security Agent** na serwerze Microsoft Exchange (tylko w wersji Advanced)<br>Patrz *Dodawanie agentów do grup na stronie 4-6*, aby uzyskać więcej informacji. |
| **Konfiguruj regułę** | Konfiguruje następujące podstawowe ustawienia zabezpieczeń dla wszystkich programów Security Agent należących do wybranej grupy<br>Patrz *Zestawienie podstawowych ustawień zabezpieczeń w programach Security Agent na stronie 5-2*, aby uzyskać więcej informacji. |
| **Skanuj teraz** | • Rozpoczyna skanowanie wszystkich punktów końcowych w wybranej grupie<br>• Rozpoczyna skanowanie wybranych punktów końcowych |
| **Zatrzymaj skanowanie** | • Kończy skanowanie wszystkich punktów końcowych w wybranej grupie<br>• Kończy skanowanie wybranych punktów końcowych |

| POLECENIE | OPIS |
|---|---|
| **Odinstaluj agenta** | Umożliwia usunięcie programu Security Agent z wybranych punktów końcowych.<br><br>Patrz *Usuwanie agentów na stronie 3-41*, aby uzyskać więcej informacji. |
| **Zeruj licznik** | Resetuje liczniki wykrywania zagrożeń bezpieczeństwa dla wszystkich programów Security Agent w sieci. Powiązane dane dziennika są nadal dostępne za pośrednictwem Kwerendy dziennika. |
| **Dostosuj kolumny** | Wybiera kolumny do wyświetlenia w tabeli<br><br>Patrz *Dostosowanie kolumn listy urządzeń na stronie 4-9*, aby uzyskać więcej informacji. |
| **Przenieś program Security Agent** | Przeniesienie wybranych programów Security Agent do innej grupy albo do innego serwera Security Server.<br><br>Patrz *Przenoszenie agentów na stronie 4-11*, aby uzyskać więcej informacji. |

# Dodawanie agentów do grup

Jeśli agent zostanie zainstalowany i podlega programowi Security Server, jest przez serwer dodawany do grupy.

- Agenty Security Agent zainstalowane na platformach serwerowych są dodawane do grupy **Serwery (domyślne)**.
- Agenty Security Agent zainstalowane na platformach komputerowych są dodawane do grupy **Komputery (domyślne)**.

**Uwaga**

Programy Security Agent można przypisywać do innych grup, przenosząc je. Aby uzyskać więcej informacji, zobacz *Przenoszenie agentów na stronie 4-11*.

- Każdy program Messaging Security Agent (tylko w wersji Advanced) stanowi odrębną grupę. Nie można połączyć kliku programów Messaging Security Agent w jedną grupę.

Jeśli liczba agentów widoczna w grupie drzew zabezpieczeń jest nieprawidłowa, być może agenty zostały usunięte bez powiadamiania o tym serwera (np. jeśli w momencie usuwania agenta nastąpiła przerwa w komunikacji klienta z serwerem). Serwer zachowuje wówczas informacje o agencie w swojej bazie danych, a w konsoli internetowej agent widoczny jest jako offline. Po ponownym zainstalowaniu agenta serwer tworzy nowy rekord w bazie danych i traktuje agenta jako nowego. W drzewie grup zabezpieczeń agenty są wówczas zduplikowane. Aby wyszukać zduplikowane rekordy dotyczące agentów, należy użyć funkcji sprawdzania połączenia agenta, korzystając z opcji **Administracja** > **Ustawienia globalne** > **System**.

### Instalowanie programów Security Agent

Zobacz następujące tematy:


- *Wymagania dotyczące instalacji programu Security Agent na stronie 3-2*
- *Uwagi dotyczące instalacji programu Security Agent na stronie 3-2*
- *Metody instalacji programu Security Agent na stronie 3-7*
    - *Instalowanie z wewnętrznej strony internetowej na stronie 3-11*
    - *Instalowanie za pomocą skryptu logowania na stronie 3-13*
    - *Instalowanie za pomocą narzędzia Client Packager na stronie 3-15*
    - *Instalowanie za pomocą instalacji zdalnej na stronie 3-19*
    - *Instalowanie za pomocą narzędzia Vulnerability Scanner na stronie 3-22*
    - *Instalowanie za pomocą powiadomienia e-mail na stronie 3-34*
- *Wykonywanie zadań po instalacji w programach Security Agent na stronie 3-36*


### Instalowanie programów Messaging Security Agent (tylko w wersji Advanced)

Zobacz następujące tematy:

- *Wymagania dotyczące instalacji programu Messaging Security Agent na stronie 3-38*
- *Instalowanie programu Messaging Security Agent (tylko w wersji Advanced) na stronie 3-39*


# Dodawanie grup

Istnieje możliwość dodania grupy serwerów lub komputerów zawierającej co najmniej jeden program Security Agent.

Nie można dodać grupy zawierającej programy Messaging Security Agent. Po zainstalowaniu program Messaging Security Agent podlega programowi Security Server i automatycznie staje się odrębną grupą w **drzewie grup zabezpieczeń**.

---

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Kliknij przycisk **Dodaj grupę**.

   Zostanie wyświetlony nowy ekran.
3. Wybierz typ grupy:
   - **Komputery**
   - **Serwery**
4. Wpisz nazwę grupy.
5. Aby do dodawanej grupy zastosować ustawienia istniejącej grupy, kliknij polecenie **Importuj ustawienia z grupy** i wybierz ją. Widoczne będą tylko grupy wybranego typu.
6. Kliknij przycisk **Zapisz**.

---

# Dostosowanie kolumn listy urządzeń

Możesz wybrać kolumny do wyświetlenia, klikając pozycje **Więcej** > **Dostosuj kolumny** u góry listy urządzeń.

| KOLUMNA | PRZEDSTAWIONE INFORMACJE |
|---|---|
| **Programy Security Agent** | |
| Nazwa | Nazwa hosta klienta, na którym agent jest zainstalowany |
| Adres IP | Adres IP klienta, na którym agent jest zainstalowany |
| Online/offline | • **Online**:agent jest połączony z serwerem Security Server<br>• **Offline**:agent jest odłączony od serwera Security Server |
| Skanowanie zaplanowane | Data i godzina ostatniego skanowania zaplanowanego |
| Skanowanie ręczne | Data i godzina ostatniego skanowania ręcznego |
| Platforma | System operacyjny klienta, na którym agent jest zainstalowany |
| Architektura | • **x64**:64-bitowy system operacyjny<br>• **x86**:32-bitowy system operacyjny |
| Metoda skanowania | • **Inteligentne**:skanowanie lokalne i w chmurze<br>• **Standardowe**:tylko skanowanie lokalne<br>Aby uzyskać więcej informacji, zobacz *Metody skanowania na stronie 5-3*. |
| Mechanizm antywirusowy | Wersja silnika skanowania antywirusowego |

| KOLUMNA | PRZEDSTAWIONE INFORMACJE |
|---|---|
| Sygnatura agenta usługi Smart Scan<br><br>**Uwaga**<br>Ta kolumna jest widoczna tylko wtedy, jeśli metodą skanowania jest Smart Scan. | Wersja sygnatura agenta usługi Smart Scan |
| Usługa Smart Scan<br><br>**Uwaga**<br>Ta kolumna jest widoczna tylko wtedy, jeśli metodą skanowania jest Smart Scan. | • **Połączony**: agent jest połączony z usługą Smart Scan<br>• **Odłączony**: agent jest odłączony od usługi Smart Scan<br><br>**Uwaga**<br>Usługa skanowania inteligentnego jest uruchamiana na serwerze Security Server. Jeśli agent jest odłączony, oznacza to, że nie może się połączyć z serwerem Security Server lub że usługa Smart Scan nie działa (np. została zatrzymana). |
| Sygnatura wirusów<br><br>**Uwaga**<br>Ta kolumna jest widoczna tylko wtedy, jeśli metodą skanowania jest skanowanie standardowe. | Wersja sygnatur wirusów |
| Wykryto wirusy | Liczba znalezionych wirusów/złośliwego oprogramowania |
| Wykryto oprogramowanie spyware | Liczba wykrytych programów spyware/grayware, |

| Kolumna | Przedstawione informacje |
|---|---|
| Wersja agenta | Wersja agenta |
| Naruszenia dot. adresów URL | Liczba przypadków uzyskiwania dostępu do zablokowanych adresów URL |
| Wykryty spam | Liczba wiadomości e-mail zawierających spam |
| Skanowanie POP3 | • **Włączone**<br>• **Wyłączone** |
| **Programy Messaging Security Agent (tylko w wersji Advanced)** | |
| Nazwa | Nazwa hosta klienta, na którym agent jest zainstalowany |
| Adres IP | Adres IP klienta, na którym agent jest zainstalowany |
| Online/offline | • **Online**:agent jest połączony z serwerem Security Server<br>• **Offline**:agent jest odłączony od serwera Security Server |
| Platforma | System operacyjny klienta, na którym agent jest zainstalowany |
| Architektura | • **x64**:64-bitowy system operacyjny<br>• **x86**:32-bitowy system operacyjny |
| Wersja Exchange | Wersja serwera Microsoft Exchange |
| Sygnatura wirusów | Wersja sygnatur wirusów |
| Mechanizm antywirusowy | Wersja silnika skanowania antywirusowego |
| Wersja agenta | Wersja agenta |

# Przenoszenie agentów

Istnieje kilka sposobów przenoszenia agentów.

| Przenoszony agent | Szczegóły | Sposób przenoszenia agentów |
|---|---|---|
| Security Agent | Możesz przenosić programy Security Agent między grupami. Po przeniesieniu agenty odziedziczą ustawienia nowej grupy. | Użyj konsoli internetowej do przeniesienia jednego lub więcej agentów. Patrz sekcja *Przenoszenie programów Security Agent między grupami na stronie 4-13*. |
| | Jeśli dysponujesz co najmniej dwoma serwerami Security Server, możesz przenosić programy Security Agent między serwerami.<br><br>Po przeniesieniu agenty zostaną na drugim serwerze Security Server połączone w grupę **Komputery (domyślne)** lub **Serwery (domyślne)**, zależnie od systemu operacyjnego klienta. Agent dziedziczy ustawienia swojej nowej grupy. | • Użyj konsoli internetowej do przeniesienia jednego lub więcej agentów. Patrz sekcja *Przenoszenie agentów między serwerami Security Server za pomocą konsoli internetowej na stronie 4-13*.<br><br>• Aby przenieść agenta zainstalowanego na kliencie, uruchom na tym kliencie narzędzie Client Mover. Patrz sekcja *Przenoszenie programu Security Agent między serwerami Security Server za pomocą narzędzia Client Mover na stronie 4-14*. |
| Programy Messaging Security Agent (tylko w wersji Advanced) | Jeśli dysponujesz co najmniej dwoma serwerami Security Server, możesz przenosić programy Messaging Security Agent między serwerami.<br><br>Po przeniesieniu agent będzie stanowił własną grupę na drugim serwerze Security Server i zachowa swoje ustawienia. | Użyj konsoli internetowej do przenoszenia agentów pojedynczo. Patrz sekcja *Przenoszenie agentów między serwerami Security Server za pomocą konsoli internetowej na stronie 4-13*. |

## Przenoszenie programów Security Agent między grupami

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Wybierz agenty do przeniesienia.

**Porada**

Aby wybrać wiele sąsiadujących programów Security Agent, kliknij pierwszego agenta w zakresie, przytrzymaj klawisz SHIFT i kliknij ostatniego agenta w zakresie. Aby wybrać nieciągły zakres agentów, kliknij pierwszego agenta w zakresie, przytrzymaj klawisz CTRL, a następnie klikaj agenty, które chcesz zaznaczyć.

4. Przeciągnij agenty do nowej grupy.

## Przenoszenie agentów między serwerami Security Server za pomocą konsoli internetowej

### Przed rozpoczęciem

Podczas przenoszenia agenta między serwerami Security Server:

- Jeśli agent we wcześniejszej wersji zostanie przeniesiony na serwer Security Server, na którym działa wersja bieżąca, zostanie automatycznie zaktualizowany.
- Nie należy przenosić agenta w bieżącej wersji na serwer Security Server, na którym działa poprzednia wersja, ponieważ spowoduje to wyłączenie agenta z zakresu zarządzania (agent zostanie wyrejestrowany z poprzedniego serwera, ale nie uda się zarejestrować go na nowym serwerze, nie będzie go więc widać w żadnej konsoli internetowej). Zostanie zachowana bieżąca wersja agenta (bez zmiany wersji na wcześniejszą).
- Serwery Security Server muszą być w tej samej wersji językowej.

- Zarejestruj nazwę hosta i port nasłuchiwania serwera Security Server, na który agent zostanie przeniesiony. Nazwę hosta i port nasłuchiwania można znaleźć na ekranie Ustawienia zabezpieczeń serwera Security Server, nad panelem Zadania.

**Procedura**

1. W konsoli internetowej serwera Security Server, który obecnie zarządza agentami, przejdź do pozycji **Urządzenia**.
2. Aby przenieść programy Security Agent, zaznacz grupę, a następnie zaznacz agenty. Aby przenieść program Messaging Security Agent, wybierz go.
3. Kliknij pozycję **Więcej** > **Przenieś program Security Agent**.

   Zostanie wyświetlony nowy ekran.
4. Zarejestruj nazwę hosta i port nasłuchiwania serwera Security Server, na który agenty zostaną przeniesione.
5. Kliknij opcję **Przenieś**.
6. Aby sprawdzić, czy agenty podlegają teraz drugiemu serwerowi Security Server, otwórz konsolę internetową tego serwera i zlokalizuj je w drzewie grup zabezpieczeń.

**Uwaga**

Jeśli program Security Agent nie jest wyświetlany w drzewie grup zabezpieczeń, uruchom ponownie usługę Trend Micro Security Server Master Service.

## Przenoszenie programu Security Agent między serwerami Security Server za pomocą narzędzia Client Mover

### Przed rozpoczęciem

Podczas przenoszenia agenta między serwerami Security Server:

- Jeśli agent we wcześniejszej wersji zostanie przeniesiony na serwer Security Server, na którym działa wersja bieżąca, zostanie automatycznie zaktualizowany.

- Nie należy przenosić agenta w bieżącej wersji na serwer Security Server, na którym działa poprzednia wersja, ponieważ spowoduje to wyłączenie agenta z zakresu zarządzania (agent zostanie wyrejestrowany z poprzedniego serwera, ale nie uda się zarejestrować go na nowym serwerze, nie będzie go więc widać w żadnej konsoli internetowej). Zostanie zachowana bieżąca wersja agenta (bez zmiany wersji na wcześniejszą).
- Serwery Security Server muszą być w tej samej wersji językowej.
- Zarejestruj nazwę hosta i port nasłuchiwania serwera Security Server, na który agent zostanie przeniesiony. Nazwę hosta i port nasłuchiwania można znaleźć na ekranie Ustawienia zabezpieczeń serwera Security Server, nad panelem Zadania.
- Zaloguj się na kliencie, używając konta administratora.

**Procedura**

1. Na kliencie otwórz wiersz polecenia.

   **Uwaga**

   Należy otworzyć wiersz polecenia jako administrator.

2. Wpisz `cd` i ścieżkę do folderu instalacji programu Security Agent. Na przykład: `cd C:\Program Files\Trend Micro\Security Agent`
3. Uruchom narzędzie Client Mover, używając następującej składni:

   ```
   <nazwa pliku wykonywalnego> -s <nazwa serwera> -p <port nasłuchiwania serwera> -c <port nasłuchiwania klienta>
   ```

**TABELA 4-3. Parametry narzędzia Client Mover**

| PARAMETR | WYJAŚNIENIE |
|---|---|
| `<nazwa pliku wykonywalnego>` | `IpXfer.exe` (32-bitowy)<br>`IpXfer_x64.exe` (64-bitowy) |
| `<nazwa serwera>` | Nazwa docelowego serwera Worry-Free Business Security (serwera, na który zostanie przeniesiony agent). |

| PARAMETR | WYJAŚNIENIE |
|---|---|
| `<port nasłuchiwania serwera>` | Port nasłuchiwania (lub zaufany port) docelowego serwera Security Server. |
| `<port nasłuchiwania klienta>` | Numer portu używany przez program Security Agent do komunikowania się z serwerem. |

Przykład:

```
ipXfer.exe -s Server01 -p 8080 -c 21112
```

4. Aby sprawdzić, czy program Security Agent podlega teraz drugiemu serwerowi Security Server, otwórz konsolę internetową tego serwera i zlokalizuj agenta w drzewie grup zabezpieczeń.

**Uwaga**

Jeśli program Security Agent nie jest wyświetlany w drzewie grup zabezpieczeń, uruchom ponownie usługę Trend Micro Security Server Master Service.

# Replikowanie ustawień

Replikowanie ustawień między grupami programów Security Agent albo programami Messaging Security Agent (tylko w wersji Advanced).

## Replikowanie ustawień grupy programów Security Agent

Funkcja ta pozwala zastosować ustawienia konkretnej grupy komputerów lub serwerów do innej grupy tego samego typu. Nie można replikować ustawień grupy serwerów do grupy komputerów ani odwrotnie.

Jeśli istnieje tylko jedna grupa danego typu, funkcja ta zostanie wyłączona.

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij ikonę koła zębatego obok nazwy grupy.
4. Kliknij pozycję **Replikuj ustawienia**.

   Zostanie wyświetlony nowy ekran.
5. Wybierz grupy docelowe, które odziedziczą ustawienia.
6. Kliknij przycisk **Zastosuj**.

## Replikowanie ustawień programu Messaging Security Agent (tylko w wersji Advanced)

Ustawienia programów Messaging Security Agent można replikować tylko wtedy, jeśli współdzielą one tę samą domenę.

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij ikonę koła zębatego obok programu Messaging Security Agent.
4. Kliknij pozycję **Replikuj ustawienia**.

   Zostanie wyświetlony nowy ekran.
5. Wybierz program Messaging Security Agent, który odziedziczy ustawienia.
6. Kliknij przycisk **Zastosuj**.
7. Jeśli replikacja się nie powiodła:

   a. Uruchom edytor rejestru (polecenie regedit).

b. Przejdź do wpisu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`.

c. Prawym przyciskiem myszy kliknij kolejno pozycje **winreg** > **Uprawnienia**

d. Dodaj pozycję **Smex Admin Group** dotyczącą domeny docelowej, a następnie włącz opcję **Allow Read**.

# Importowanie i eksportowanie ustawień grup Security Agent

Ustawienia grupy komputerów lub serwerów można wyeksportować do pliku `.dat`, aby utworzyć kopię zapasową ustawień. Plik `.dat` można także wykorzystać do zaimportowania ustawień do innej grupy.

**Uwaga**

Ustawienia można importować/eksportować z/do komputerów i grup serwerów. Ustawienia są niezależne od typu grupy. Można też użyć funkcji **Replikuj ustawienia**, choć zależy ona od typu grupy. Szczegółowe informacje o funkcji **Replikuj ustawienia** zawiera część *Replikowanie ustawień na stronie 4-16*.

**TABELA 4-4. Ustawienia, które można importować i eksportować**

| WYBÓR | EKRAN ZAWIERAJĄCY USTAWIENIA | USTAWIENIA, KTÓRE MOŻNA EKSPORTOWAĆ/IMPORTOWAĆ |
|---|---|---|
| Grupa komputerów ( ) lub grupa serwerów ( ) | Urządzenia (**Urządzenia** > **Konfiguruj regułę**) | • Oprogramowanie antywirusowe/anty-spyware (skanowanie w czasie rzeczywistym)<br>• Przewidujące uczenie maszynowe<br>• Monitorowanie zachowania<br>• Zaufany program<br>• Kwarantanna<br>• Usługa Web Reputation<br>• Filtrowanie adresów URL<br>• Zapora<br>• Kontrola urządzeń<br>• Narzędzia użytkownika (dostępne tylko w przypadku grup komputerów)<br>• Uprawnienia agenta |
| | Skanowanie ręczne (**Skanowanie** > **Skanowanie ręczne**) | Wszystkie ustawienia |
| | Zaplanowane skanowanie (**Skanowanie** > **Skanowanie zaplanowane**) | Wszystkie ustawienia |

## Eksportowanie ustawień

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij ikonę koła zębatego obok nazwy grupy.
4. Kliknij pozycję **Eksportuj ustawienia reguły**.

   Zostanie wyświetlony nowy ekran.
5. Kliknij przycisk **Eksportuj**.

   Zostanie wyświetlone okno dialogowe.
6. Kliknij przycisk **Zapisz**, przejdź do wybranej lokalizacji, a następnie kliknij przycisk **Zapisz** ponownie.

## Importowanie ustawień

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Importuj ustawienia reguły**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij przycisk **Przeglądaj**, znajdź plik, a następnie kliknij przycisk **Importuj**.

# Rozdział 5

# Zarządzanie podstawowymi ustawieniami zabezpieczeń w programach Security Agent

W tym rozdziale wyjaśniono, jak skonfigurować podstawowe ustawienia zabezpieczeń agentów Security Agent.

# Zestawienie podstawowych ustawień zabezpieczeń w programach Security Agent

**TABELA 5-1. Zestawienie podstawowych ustawień zabezpieczeń w programach Security Agent**

| OPCJA | OPIS | DOMYŚLNE |
|---|---|---|
| Metoda skanowania | Włączenie lub wyłączenie skanowania Smart Scan. | Włączenie lub wyłączenie wybiera się podczas instalacji. |
| Oprogramowanie antywirusowe/anty-spyware | Konfigurowanie opcji skanowania w czasie rzeczywistym, ochrony antywirusowej i ochrony antyszpiegowskiej | Włączone (skanowanie w czasie rzeczywistym) |
| Przewidujące uczenie maszynowe | Konfigurowanie opcji Przewidującego uczenia maszynowego | Wyłączone |
| Monitorowanie zachowania | Konfigurowanie opcji monitorowania zachowania | Włączone dla grup komputerów<br>Wyłączone dla grup serwerów |
| Zaufany program | Określanie, w przypadku których programów nie trzeba monitorować podejrzanych zachowań | nd. |
| Kwarantanna | Należy określić katalog kwarantanny | http://<Nazwa serwera Security Server lub adres IP> |
| Usługa Web Reputation | Konfigurowanie opcji W biurze i Poza biurem usługi Web Reputation | W biurze: Włączone, Niski<br>Poza biurem: Włączone, Średni |

| Opcja | Opis | Domyślne |
|---|---|---|
| Filtrowanie adresów URL | Filtrowanie adresów URL blokuje witryny sieci web naruszające skonfigurowane zasady. | Włączone, Niski |
| Dozwolone/zablokowane adresy URL | Konfigurowanie globalnych list dozwolonych/ zablokowanych elementów | Wyłączone |
| Zapora | Konfigurowanie opcji zapory | Wyłączone |
| Kontrola urządzeń | Konfigurowanie opcji automatycznego uruchamiania, dostępu do urządzeń USB i zasobów sieciowych | Wyłączone |
| Narzędzia użytkownika | Konfiguracja narzędzie Wi-Fi Advisor i Trend Micro Anti-Spam Toolbar | Wyłączone: Narzędzie Wi-Fi Advisor<br>Wyłączone: Pasek narzędzi Anti-spam Toolbar w zgodnych klientach poczty e-mail |
| Uprawnienia agenta | Konfigurowanie dostępu do ustawień z konsoli agenta<br>Wyłącz aktualizację i instalację poprawek hot fix programu Security Agent | nd. |

# Metody skanowania

Podczas skanowania zagrożeń bezpieczeństwa programy Security Agent mogą korzystać z dwóch metod skanowania.

- **Smart Scan**: Programy Security Agent, które używają skanowania Smart Scan, są w tym dokumencie nazywane **agentami Smart Scan**. Agenty Smart Scan

korzystają z funkcji skanowania lokalnego i zapytań w chmurze obsługiwanych przez usługi File Reputation Services.

- **Skanowanie standardowe**: Programy Security Agent, które nie używają skanowania Smart Scan, są w tym dokumencie nazywane **agentami skanowania standardowego**. Podczas skanowania agent skanowania standardowego zapisuje wszystkie składniki na klient i skanuje wszystkie pliki lokalnie.

Poniższa tabela przedstawia porównanie tych dwóch metod skanowania.

**TABELA 5-2. Porównanie skanowania standardowego i skanowania Smart Scan**

| PODSTAWA PORÓWNANIA | SKANOWANIE STANDARDOWE | SMART SCAN |
|---|---|---|
| Zachowanie skanowania | Security Agent skanowania standardowego przeprowadza skanowanie na klient. | • Agent usługi Smart Scan przeprowadza skanowanie na klient.<br>• Jeśli podczas skanowania Security Agent nie jest w stanie ustalić zagrożeń związanych z danym plikiem, Security Agent weryfikuje zagrożenie, wysyłając zapytanie do serwera skanowania (w przypadku Security Agent połączonych z Smart Scan Server) lub do usługi Trend Micro Smart Protection Network (w przypadku Security Agent odłączonych od Smart Scan Server).<br>**Uwaga**<br>Serwer skanowania to usługa uruchamiana na Smart Scan Server.<br>• Security Agent „buforuje” wynik zapytania o skanowanie, aby zwiększyć skuteczność skanowania. |

| PODSTAWA PORÓWNANIA | SKANOWANIE STANDARDOWE | SMART SCAN |
|---|---|---|
| Używane i aktualizowane składniki | Wszystkie elementy Security Agent dostępne w źródle aktualizacji poza sygnaturą agenta usługi Smart Scan. | Wszystkie składniki poza sygnaturą wirusów dostępne w źródle aktualizacji |
| Typowe źródło aktualizacji | Serwer ActiveUpdate | Serwer ActiveUpdate |

## Konfiguracja metod skanowania

### Przed rozpoczęciem

Po zainstalowaniu serwera Security Server dostępna jest możliwość włączenia opcji Smart Scan. Jeśli ta opcja jest włączona, domyślną metodą skanowania jest Smart Scan, co oznacza, że wszystkie programy Security Agent będą korzystać z opcji Smart Scan. W przeciwnym razie domyślną metodą jest skanowanie standardowe. W zależności od bieżących wymagań można przełączać te dwie metody skanowania w odniesieniu do agentów. Na przykład:

- Jeśli agenty korzystają aktualnie ze skanowania standardowego i jego ukończenie zajmuje dużo czasu, można zmienić ustawienie na Smart Scan, czyli metodę opracowaną w celu przyspieszenia i zwiększenia wydajności skanowania Innym przykładem sytuacji, w której warto zmienić metodę na Smart Scan, jest wyczerpywanie się miejsca na dysku agenta, ponieważ agenty Smart Scan pobierają mniejsze pliki sygnatur, zajmujące mniej miejsca na dysku.

  Przed przełączeniem metody na Smart Scan należy przejść do karty **Administracja** > **Ustawienia globalne**, kliknąć kartę **Komputer/serwer**, a następnie przejść do sekcji **Ogólne ustawienia skanowania**. Należy upewnić się, że opcja **Wyłącz usługę skanowania Smart Scan** została wyłączona.

- W razie zauważenia spadku wydajności serwera Security Server, co może sygnalizować, że nie jest on w stanie przetworzyć wszystkich żądań skanowania od agentów we właściwym czasie, należy zmienić metodę na skanowanie standardowe.

W poniższej tabeli wyszczególniono, co należy brać pod uwagę przy zmianie metod skanowania:

**TABELA 5-3. Czynniki dotyczące przełączania metod skanowania**

| UWAGA | SZCZEGÓŁY |
|---|---|
| Połączenie z serwerem Security Server | Upewnij się, że programy Security Agent są w stanie połączyć się z serwerem Security Server. O zmianie metody skanowania są powiadamiane wyłącznie agenty online. Agenty offline otrzymają powiadomienie po przejściu do trybu online.<br><br>Należy również sprawdzić, czy serwer Security Server zawiera najnowsze składniki, ponieważ agenty muszą pobierać z serwera Security Server nowe składniki, a mianowicie sygnaturę agenta usługi Smart Scan w przypadku przełączania agentów na korzystanie z metody Smart Scan oraz sygnaturę wirusów w przypadku przełączania agentów na korzystanie ze skanowania standardowego. |
| Liczba programów Security Agent do przełączenia | W celu zapewnienia optymalnego wykorzystania zasobów serwera Security Server jednorazowo należy przełączać względnie małą liczbę programów Security Agent. Podczas przełączania metody skanowania serwer Security Server może wykonywać inne ważne zadania. |
| Synchronizacja | Przy pierwszym przełączeniu programy Security Agent muszą pobrać **pełną wersję** sygnatury agenta usługi Smart Scan (w przypadku przełączania agentów na metodę Smart Scan) lub sygnatury wirusów (w przypadku przełączania agentów na skanowanie standardowe).<br><br>Należy wziąć pod uwagę, że pobieranie będzie trwać krócej, jeśli zostanie wykonane poza godzinami największego ruchu w sieci. Należy również tymczasowo wyłączyć w odniesieniu do agentów funkcję „Aktualizuj teraz”, aby uniemożliwić aktualizacje inicjowane przez użytkownika, i włączyć ją ponownie po przełączeniu metody skanowania dla agentów.<br><br>**Uwaga**<br>Dzięki temu agenty będą pobierać **mniejsze, przyrostowe** wersje sygnatury agenta usługi Smart Scan lub sygnatury wirusów, jeśli tylko będą często aktualizowane. |

| Uwaga | Szczegóły |
|---|---|
| Obsługa IPv6 | Będący w trybie offline agent Smart Scan, korzystający wyłącznie z protokołu IPv6, nie może wysyłać żądań bezpośrednio do sieci Trend Micro Smart Protection Network.<br><br>Aby umożliwić takiemu agentowi Smart Scan wysyłanie żądań, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP, taki jak DeleGate. |

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

   Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.
4. Przejdź do menu **Metoda skanowania**.
5. Wybierz preferowaną metodę skanowania.
6. Kliknij przycisk **Zapisz**.

# Skanowanie w czasie rzeczywistym w programach Security Agent

Skanowanie w czasie rzeczywistym zapewnia stałą ochronę. Za każdym razem, gdy plik zostaje otwarty, pobrany, skopiowany lub zmodyfikowany, funkcja skanowania w czasie rzeczywistym programu **Security Agent** sprawdza ten plik w poszukiwaniu zagrożeń.

## Konfigurowanie skanowania w czasie rzeczywistym w programach Security Agent

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

   Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.
4. Kliknij pozycję **Oprogramowanie antywirusowe/anty-spyware**.

   Zostanie wyświetlony nowy ekran.
5. Zaznacz opcję **Włącz oprogramowanie antywirusowe/anty-spyware działające w czasie rzeczywistym**.
6. Skonfiguruj ustawienia skanowania. Szczegółowe informacje zawiera część *Cele skanowania i operacje dotyczące programów Security Agent na stronie 7-11*:

   **Uwaga**

   Jeśli przydzielisz użytkownikom uprawnienia do konfigurowania własnych ustawień skanowania, podczas skanowania zostaną wykorzystane ustawienia skonfigurowane przez użytkownika.
7. Kliknij przycisk **Zapisz**.

# Przewidujące uczenie maszynowe

Przewidujące uczenie maszynowe Trend Micro wykorzystuje zaawansowaną technologię uczenia maszynowego w celu kojarzenia informacji o zagrożeniach i wykonywania szczegółowej analizy plików, aby wykrywać pojawiające się nieznane zagrożenia bezpieczeństwa przy użyciu badania cyfrowych odcisków linii papilarnych DNA, mapowania API i innych cech plików. Przewidujące uczenie maszynowe przeprowadza

także analizę behawioralną nieznanych lub rzadko spotykanych procesów celem określenia, czy pojawiające się lub nieznane zagrożenie podejmuje próbę zarażenia sieci.

Przewidujące uczenie maszynowe to skuteczne narzędzie pomagające chronić środowisko przed nieznanymi zagrożeniami lub atakami typu zero-day.

| Typ wykrycia | Opis |
|---|---|
| Plik | Po wykryciu nieznanego lub rzadko spotykanego pliku program Security Agent skanuje plik przy użyciu mechanizmu skanowania zaawansowanych zagrożeń (ATSE) w celu wyodrębnienia funkcji pliku i wysyła raport do silnika przewidującego uczenia maszynowego, obsługiwanego w sieci Trend Micro Smart Protection Network. Przy użyciu modelowania złośliwego oprogramowania przewidujące uczenie maszynowe porównuje próbkę z modelem złośliwego oprogramowania, przydziela wynik prawdopodobieństwa i określa prawdopodobny typ złośliwego oprogramowania zawartego w pliku.<br><br>W zależności od sposobu konfiguracji przewidującego uczenia maszynowego program Security Agent może podjąć próbę “Przeprowadzenia kwarantanny” narażonego pliku, aby uniemożliwić dalsze rozprzestrzenianie się zagrożenia w sieci. |
| Proces | Po wykryciu nieznanego lub rzadko spotykanego pliku program Security Agent monitoruje proces przy użyciu mechanizmu analiz kontekstowych i wysyła raport o zachowaniu do silnika przewidującego uczenia maszynowego. Przy użyciu modelowania złośliwego oprogramowania przewidujące uczenie maszynowe porównuje zachowanie procesu z modelem, przydziela wynik prawdopodobieństwa i określa prawdopodobny typ złośliwego oprogramowania wykonywanego przez proces.<br><br>W zależności od sposobu skonfigurowania przewidującego uczenia maszynowego program Security Agent może “Przerwać” narażony proces lub skrypt albo podjąć próbę wyczyszczenia pliku, który wykonał dany proces lub skrypt. |

# Konfigurowanie przewidującego uczenia maszynowego

**Uwaga**

Wymagania przewidującego uczenia maszynowego:

- Włącz monitorowanie zachowania przy użyciu opcji **Konfiguruj regułę** > **Monitorowanie zachowania**
- Działające połączenie z Internetem w celu połączenia się w siecią Smart Protection Network

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

   Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.
4. Kliknij opcję **Przewidujące uczenie maszynowe**.
5. Wybierz opcję **Włącz predykcyjne uczenie maszynowe**.
6. Wybierz typ na potrzeby wykrywania i powiązaną operację podejmowaną przez mechanizm Przewidujące uczenie maszynowe.

| 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<br>• **Tylko rejestruj w dzienniku**: Wybierz tę opcję, aby skanować nieznane pliki i zapisywać analizę przewidującego uczenia maszynowego w dzienniku w celu dalszego zbadania zagrożenia w firmie |

| Typ wykrytego zagrożenia | Operacje |
|---|---|
| **Proces** | • **Przerwij**: wybierz tę opcję, aby automatycznie przerywać wszystkie procesy lub skrypty, które zachowują się podobnie do złośliwego oprogramowania na podstawie analizy przewidującego uczenia maszynowego<br><br>**Ważne**<br>Funkcja przewidującego uczenia maszynowego podejmie próbę wyczyszczenia plików, które uruchomiły złośliwe procesy lub skrypty. Jeśli operacja czyszczenia nie powiedzie się, funkcja przewidującego uczenia maszynowego podda odpowiednie pliki kwarantannie.<br><br>• **Tylko rejestruj w dzienniku**: wybierz tę opcję, aby skanować nieznane procesy lub skrypty i rejestrować analizę przewidującego uczenia maszynowego na potrzeby dalszego lokalnego zbadania zagrożenia |

7. Kliknij przycisk **Zapisz**.

# Monitorowanie zachowania

Agenty Security Agent stale monitorują klienty pod kątem nietypowych modyfikacji systemu operacyjnego lub zainstalowanego oprogramowania. Administratorzy (lub użytkownicy) mogą tworzyć listy wyjątków umożliwiające działanie niektórych programów z naruszeniem monitorowanej zmiany, bądź całkowicie zablokować określone programy. Ponadto zawsze jest możliwe uruchomienie programów z prawidłowymi podpisami cyfrowymi.

Inną opcją funkcji Monitorowanie zachowania jest ochrona plików EXE i DLL przed usunięciem lub modyfikacją. Po włączeniu funkcji Monitorowanie zachowania

użytkownicy mogą tworzyć wyjątki umożliwiające zatwierdzanie lub blokowanie określonych programów. Ponadto użytkownicy mogą wybrać wspólną ochronę wszystkich programów Intuit QuickBooks.

## Konfigurowanie monitorowania zachowania

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

   Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.
4. Kliknij pozycję **Monitorowanie zachowania**.
5. Zmień odpowiednio następujące ustawienia:

   - **Włącz monitorowanie zachowania**

     **Uwaga**

     Aby umożliwić użytkownikom dostosowywanie własnych ustawień monitorowania zachowania, przejdź do ekranu **Urządzenia** > **{grupa}** > **Konfiguruj regułę** > **Uprawnienia agenta** > **Monitorowanie zachowania** i wybierz **Pozwalaj użytkownikom modyfikować ustawienia monitorowania zachowania**.

   - **Włącz blokowanie zachowania złośliwego oprogramowania dotyczące znanych i potencjalnych zagrożeń**: Blokowanie działania złośliwego oprogramowania jest osiągane poprzez wykorzystanie zestawu wewnętrznych reguł określonych w **plikach sygnatur**. Reguły te rozpoznają znane i podejrzane groźne zachowanie, często spotykane w złośliwym oprogramowaniu. Przykładem podejrzanego zachowania może być nagłe lub niewyjaśnione uruchamianie usług, zmiana ustawień zapory, modyfikacja systemu plików itp.

     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

- **Monituj użytkowników przed uruchamianiem nowo napotkanych programów pobranych przez HTTP (z wykluczeniem platform serwerowych)**: Funkcja monitorowania zachowania działa w połączeniu z usługą Web Reputation celem sprawdzania większości plików pobieranych kanałami HTTP lub przy użyciu aplikacji pocztowych. Po wykryciu „nowo napotkanego" pliku administratorzy mogą wybrać opcję monitowania użytkowników przed jego uruchomieniem. Firma Trend Micro klasyfikuje program jako nowo napotkany na podstawie liczby wykrytych plików lub wieku historycznego pliku zgodnie z definicją sieci Smart Protection Network.

**Uwaga**

W przypadku kanałów HTTP skanowane są pliki wykonywalne (.exe).
W przypadku aplikacji e-mail (tylko Outlook i Windows Live Mail) skanowane są pliki wykonywalne (.exe) znajdujące się w niezabezpieczonych hasłem plikach archiwów (zip/rar).

- **Włącz ochronę oprogramowania Intuit QuickBooks**: Ochrona plików i folderów oprogramowania Intuit QuickBooks przed nieautoryzowanymi zmianami przez inne programy. Włączenie tej funkcji nie wpłynie na zmiany dokonywane z poziomu programów Intuit QuickBooks, ale uniemożliwi dokonanie zmian w plikach poprzez inne nieautoryzowane aplikacje.

  Obsługiwane są następujące produkty:

  - QuickBooks Simple Start
  - QuickBooks Pro
  - QuickBooks Premier
  - QuickBooks Online

**Uwaga**

Wszystkie pliki wykonywalne Intuit są podpisane cyfrowo i ich aktualizacje nie będą blokowane. Jeśli inne programy będą usiłowały zmienić plik binarny Intuit, w oknie agenta zostanie wyświetlony komunikat zawierający nazwę tego programu. Można zezwolić na aktualizowanie plików Intuit przez inne programy. W tym celu należy dodać określony program do listy wyjątków monitorowania zachowania w agencie. Należy pamiętać o usunięciu tego programu z listy po zakończeniu aktualizacji.

- **Ochrona przed oprogramowaniem typu ransomware**: Chroni przed nieautoryzowanym zmodyfikowaniem lub zaszyfrowaniem plików na komputerze przez zagrożenia typu "ransomware". Ransomware to typ złośliwego oprogramowania, które ogranicza dostęp do plików i domaga się dokonania płatności w celu przywrócenia tych plików.
  - **Włącz ochronę dokumentów przed nieautoryzowanym szyfrowaniem lub modyfikacją**: Ochrona dokumentów przed nieuprawnionymi zmianami.
    - **Automatycznie wykonuj kopię zapasową plików zmienionych przez podejrzane programy**: Automatycznie wykonuje kopie zapasowe plików zmienionych przez podejrzane programy, jeśli włączono ochronę dokumentu.
  - **Włącz blokowanie procesów często powiązanych z oprogramowaniem typu ransomware**: Ochrona punktów końcowych przed atakami ze strony oprogramowania ransomware przez zablokowanie procesów utożsamianych zazwyczaj z próbami przejęcia urządzenia.
  - **Włącz inspekcję programów, aby wykryć i zablokować zaatakowane pliki wykonywalne**: zwiększa prawdopodobieństwo wykrycia zagrożeń poprzez monitorowanie procesów pod kątem zachowania przypominającego oprogramowanie typu ransomware.
  - **Przerywaj działanie programów przejawiających nieprawidłowe zachowania w wyniku ataku programów wykorzystujących luki**: Ochrona przed programami wykorzystującymi luki działa w połączeniu z inspekcją programu w celu monitorowania zachowania programów i wykrycia nietypowego zachowania, które może wskazywać, że atakujący

wykorzystał lukę w zabezpieczeniach programu. Po wykryciu, Monitorowanie zachowania zamyka procesy programu.

**Uwaga**

Ochrona przed programami wykorzystującymi luki wymaga wybrania opcji **Włącz inspekcję programów, aby wykrywać i blokować zaatakowane pliki wykonywalne**.

**Uwaga**

Aby zredukować prawdopodobieństwo wykrycia przez program Worry-Free Business Security bezpiecznego procesu jako złośliwego, należy upewnić się, że komputer ma dostęp do Internetu w celu wykonania dodatkowych procesów weryfikacji przy użyciu serwerów firmy Trend Micro.

- **Wyjątki**: Wyjątki obejmują listę dozwolonych programów i listę zablokowanych programów. Programy umieszczone na liście dozwolonych programów można uruchamiać, nawet jeśli naruszą zasadę dotyczącą monitorowania zmian. Programów na liście zablokowanych programów nie można uruchamiać w żadnej sytuacji.

  - **Wprowadź pełną ścieżkę programu**: Wpisz pełną ścieżkę programu w formacie Windows lub UNC. Poszczególne wpisy należy oddzielać średnikami. Kliknij przycisk **Dodaj do listy dozwolonych** lub **Dodaj do listy zablokowanych**. W razie potrzeby użyj zmiennych środowiskowych do określenia ścieżek.

  - **Lista dozwolonych programów**: programy z tej listy mogą być uruchamiane. Aby usunąć wpis, kliknij odpowiadającą mu ikonę.

    Lista dozwolonych programów obsługuje symbole wieloznaczne i zmienne środowiskowe.

    Listę obsługiwanych zmiennych środowiskowych można znaleźć w tym miejscu *Obsługiwane zmienne środowiskowe na stronie 5-16*.

  - **Lista zablokowanych programów**: programy z tej listy nie mogą być uruchamiane. Aby usunąć wpis, kliknij odpowiadającą mu ikonę.

    Lista zablokowanych programów obsługuje tylko znaki wieloznaczne.

6. Kliknij przycisk **Zapisz**.

## Obsługiwane zmienne środowiskowe

W poniższej tabeli wyszczególniono zmienne środowiskowe, których można użyć podczas dodawania pliku lub ścieżki folderu do listy.

| Zmienna środowiskowa | Przykład | Równoważna ścieżka |
|---|---|---|
| $allappdata$ | $allappdata$\test\sample.exe | C:\ProgramData\test\sample.exe |
| $allprograms$ | $allprograms$\test\sample.exe | C:\ProgramData\Microsoft\Windows\Start Menu\Programs\test\sample.exe |
| $programdir$ | $programdir$\test\sample.exe | C:\Program Files\test\sample.exe |
| $programdirx86$ | $programdirx86$\test\sample.exe | C:\Program Files (x86)\test\sample.exe |
| $rootdir$ | $rootdir$\test\sample.exe | C:\test\sample.exe |
| $systemdir$ | $systemdir$\test\sample.exe | C:\Windows\System32\test\sample.exe |
| $systemdirx86$ | $systemdirx86$\test\sample.exe | C:\Windows\SysWOW64\test\sample.exe |
| $tempdir$ | $tempdir$\test\sample.exe | C:\Windows\Temp\test\sample.exe |
| $userprofile$ | $userprofile$\test\sample.exe | C:\user\{current_user_account}\test\sample.exe |
| $windir$ | $windir$\test\sample.exe | C:\Windows\test\sample.exe |

# Zaufany program

Programy wymienione na liście zaufanych programów nie będą monitorowane pod kątem dostępu do podejrzanych plików.

## Konfigurowanie zaufanego programu

**Uwaga**

Lista zaufanych programów nie obsługuje symboli wieloznacznych ani zmiennych środowiskowych.

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

   Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.
4. Kliknij przycisk **Zaufany program**.

   Zostanie wyświetlony nowy ekran.
5. Aby program nie był monitorowany pod kątem dostępu do podejrzanych plików, wpisz pełną ścieżkę określonego pliku i kliknij opcję **Dodaj do listy zaufanych programów**.

   `<nazwa_dysku>:/<ścieżka>/<nazwa_pliku>`

   Przykład 1: `C:\Windows\system32\regedit.exe`

   Przykład 2: `D:\backup\tool.exe`

   Uniemożliwi to hakerom używanie nazw programów zawartych na liście wykluczeń, które umieszczono do wykonania w katalogu o innej ścieżce.

6. Kliknij przycisk **Zapisz**.

# Katalog kwarantanny

Jeśli operacją wybraną w odniesieniu do zarażonego pliku jest „Kwarantanna", plik jest przez program Security Agent szyfrowany i **czasowo** przenoszony do folderu kwarantanny w następującej lokalizacji:

- `<folder instalacji programu Security Agent>\quarantine` w przypadku agentów zaktualizowanych z wersji 6.x lub starszej;
- `<folder instalacji programu Security Agent>\SUSPECT\Backup` w przypadku agentów nowo zainstalowanych i aktualizowanych z wersji 7.x lub nowszej.

Zarażony plik jest następnie wysyłany przez program Security Agent do centralnego katalogu kwarantanny, który można skonfigurować w konsoli internetowej w pozycji **Urządzenia** > **{Grupa}** > **Konfiguruj regułę** > **Kwarantanna**.

## Domyślny centralny katalog kwarantanny

Domyślny centralny katalog kwarantanny znajduje się na serwerze Security Server. Katalog jest podawany w formie adresu URL i zawiera nazwę hosta serwera Security Server lub jego adres IP, na przykład `http://serwer`. Odpowiadająca mu ścieżka bezwzględna to `<folder instalacji programu Security Server>\PCCSRV\Virus`.

- Jeśli serwer zarządza agentami wykorzystującymi zarówno adresowanie IPv4, jak i IPv6, należy użyć nazwy hosta, aby wszystkie agenty mogły wysyłać na serwer pliki poddane kwarantannie.
- Jeśli serwer ma tylko adres IPv4 lub jest identyfikowany przy użyciu takiego adresu, tylko agenty wykorzystujące wyłącznie protokół IPv4 i agenty z dwoma stosami będą mogły wysyłać na serwer pliki poddane kwarantannie.
- Jeśli serwer ma tylko adres IPv6 lub jest identyfikowany przy użyciu takiego adresu, tylko agenty wykorzystujące wyłącznie protokół IPv6 i agenty z dwoma stosami będą mogły wysyłać na serwer pliki poddane kwarantannie.

### Alternatywny centralny katalog kwarantanny

Można podać alternatywny katalog kwarantanny, wpisując lokalizację w postaci adresu URL, ścieżki UNC lub bezwzględnej ścieżki pliku. Programy Security Agent powinny mieć możliwość połączenia się z tym katalogiem. Przykład: katalog powinien mieć adres IPv6, jeśli będzie odbierać pliki poddane kwarantannie z klientów z dwoma stosami i klientów wykorzystujących wyłącznie protokół IPv6. Firma Trend Micro zaleca wskazanie katalogu z dwoma stosami poprzez identyfikację katalogu według nazwy hosta i użycie ścieżki UNC podczas wpisywania katalogu.

### Wytyczne dotyczące określania centralnego katalogu kwarantanny

Wskazówki na temat okoliczności korzystania z adresu URL, ścieżki UNC i bezwzględnej ścieżki dostępu znajdują się w poniższej tabeli:

**TABELA 5-4. Katalog kwarantanny**

| KATALOG KWARANTANNY | AKCEPTOWALNY FORMAT | PRZYKŁAD | UWAGI |
|---|---|---|---|
| Domyślny katalog na serwerze Security Server | URL | `http:// <nazwa lub adres IP hosta serwera>` | Jeśli nie zmieniasz katalogu domyślnego, skonfiguruj ustawienia obsługi katalogu, takie jak wielkość folderu kwarantanny, w sekcji **Administracja** > **Ustawienia globalne** > **karta System** > **Obsługa kwarantanny**. |
| | Ścieżka UNC | `\\<nazwa lub adres IP hosta serwera>\ ofcscan\Virus` | |
| Inny katalog na serwerze Security Server | Ścieżka UNC | `\\<nazwa lub adres IP hosta serwera>\ D$ \Quarantined Files` | Jeśli nie chcesz używać katalogu domyślnego (np. ze względu na zbyt małą ilość miejsca na dysku), wpisz ścieżkę UNC do innego katalogu. Aby ustawienia obsługi zostały zastosowane, wpisz następnie odpowiednią ścieżkę bezwzględną w sekcji **Administracja** > **Ustawienia globalne** > **karta System** > **Obsługa kwarantanny**. |

| Katalog kwarantanny | Akceptowalny format | Przykład | Uwagi |
|---|---|---|---|
| Katalog na innym komputerze serwera Security Server (jeśli w sieci działają inne serwery Security Server) | URL | `http:// <nazwa lub adres IP hosta serwera2>` | Upewnij się, że agenty mogą łączyć się z tym katalogiem. W przypadku podania nieprawidłowego katalogu agent przechowuje pliki kwarantanny 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”.<br><br>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 | `\\<nazwa lub adres IP hosta serwera2>\ofcscan\Virus` | |
| Inny komputer w sieci | Ścieżka UNC | `\\<computer_name>\temp` | |
| Inny katalog na kliencie | Ścieżka bezwzględna | `C:\temp` | Podaj ścieżkę bezwzględną, jeśli:<br>• Chcesz, aby pliki poddane kwarantannie znajdowały się tylko na kliencie.<br>• Nie chcesz, aby agenty przechowywały pliki w katalogu domyślnym na kliencie.<br><br>Jeżeli ścieżka nie istnieje, program Security Agent utworzy ją automatycznie. |

## Konfigurowanie katalogu kwarantanny

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

   Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.
4. Kliknij pozycję **Kwarantanna**.

   Zostanie wyświetlony nowy ekran.
5. Skonfiguruj katalog kwarantanny. Aby uzyskać więcej informacji, zobacz *Katalog kwarantanny na stronie 5-18*.
6. Kliknij przycisk **Zapisz**.

# Usługa Web Reputation

Usługa Web Reputation pomaga uniemożliwiać dostęp do adresów URL w sieci lub adresów zawartych w wiadomościach e-mail stanowiących zagrożenie bezpieczeństwa. Usługa Web Reputation sprawdza reputację adresu URL, korzystając z serwerów Web Reputation firmy Trend Micro, a następnie dopasowuje tę reputację do określonej reguły usługi Web Reputation, która jest egzekwowana na kliencie. W zależności od stosowanej reguły:

- Program Security Agent zablokuje dostęp do witryny lub zezwoli na dostęp do niej.
- Program Messaging Security Agent (tylko w wersji Advanced) podda kwarantannie, usunie lub dołączy znacznik do wiadomości e-mail zawierającej złośliwe adresy URL albo zezwoli na wysłanie wiadomości, jeśli adresy URL są bezpieczne.

Usługa Web Reputation dostarcza zarówno powiadomienia e-mail dla administratora, jak i powiadomienia online dla użytkownika dotyczące wykrytych zagrożeń.

W zależności od lokalizacji (W biurze/Poza biurem) klienta, należy skonfigurować odpowiedni poziom zabezpieczeń w programach Security Agent.

Jeśli usługa Web Reputation blokuje adres URL, który wydaje się bezpieczny, można dodać ten adres do listy dozwolonych adresów URL.

**Porada**

W celu zmniejszenia natężenia ruchu sieciowego firma Trend Micro zaleca dodanie wewnętrznych firmowych witryn internetowych do listy dozwolonych adresów URL usługi Web Reputation.

### Ocena punktowa reputacji

„Ocena punktowa reputacji" adresu URL określa, czy stanowi on zagrożenie internetowe czy nie. Firma Trend Micro wyznacza ocenę przy użyciu własnych mierników.

Firma Trend Micro uznaje adres URL za zagrożenie internetowe, jeśli jego wynik mieści się w określonym zakresie, oraz za bezpieczny, jeśli wynik wykracza poza ten zakres.

W programie Security Agent stosowane są trzy poziomy zabezpieczeń, które określają, czy będzie on zezwalać na dostęp do adresu URL czy go blokować.

- **Wysoki**: blokuje strony:
  - **Niebezpieczne**: zweryfikowano jako fałszywe lub znane źródła zagrożeń.
  - **Bardzo podejrzane**: potencjalnie fałszywe lub prawdopodobne źródła zagrożeń
  - **Podejrzane**: strony powiązane ze spamem lub mogące stanowić zagrożenie.
  - **Nieprzetestowane**: Firma Trend Micro aktywnie testuje strony internetowe pod kątem bezpieczeństwa, mimo to podczas odwiedzania nowych lub mniej popularnych witryn użytkownicy mogą natknąć się na strony nieprzetestowane. Zablokowanie dostępu do stron nieprzetestowanych może podnieść poziom bezpieczeństwa, ale także uniemożliwić dostęp do bezpiecznych stron.
- **Średni**: blokuje strony:

- **Niebezpieczne**: zweryfikowano jako fałszywe lub znane źródła zagrożeń.
- **Bardzo podejrzane**: potencjalnie fałszywe lub prawdopodobne źródła zagrożeń

- **Niski**: blokuje strony:
  - **Niebezpieczne**: zweryfikowano jako fałszywe lub znane źródła zagrożeń.

## Konfigurowanie usługi Web Reputation dla programów Security Agent

Usługa Web Reputation ocenia potencjalne zagrożenia wszystkich żądanych adresów URL, przeglądając bazę danych Trend Micro Security dla każdego żądania HTTP/HTTPS.

---

**Uwaga**

(wyłącznie opcja Standard) Ustawienia usługi Web Reputation należy skonfigurować dla lokalizacji W biurze i Poza biurem. Jeśli rozpoznawanie lokalizacji jest wyłączone, dla połączeń Poza biurem będą używane ustawienia W biurze. Szczegółowe informacje na temat rozpoznawania lokalizacji zawiera część *Konfigurowanie ustawień komputerów/serwerów na stronie 11-5*.

Jeśli funkcja Web Reputation i funkcja zapobiegania wykorzystaniu przeglądarki są włączone, adresy URL, które nie zostały zablokowane przez funkcję Web Reputation są następnie skanowane przez funkcję zapobiegania wykorzystaniu przeglądarki. Funkcja zapobiegania wykorzystaniu przeglądarki skanuje obiekty osadzone (np. jar, class, pdf, swf, html, js) na stronach internetowych pod danym adresem URL.

---

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

   Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.

4. Kliknij opcję **Usługa Web Reputation** > **W biurze** lub **Usługa Web Reputation** > **Poza biurem**.

   Zostanie wyświetlony nowy ekran.

5. Zmień odpowiednio następujące ustawienia:

   - **Włącz usługę Web Reputation**
   - Poziom zabezpieczeń: **Wysoka**, **Średnia**, lub **Niska**
   - Zapobieganie wykorzystaniu przeglądarki: **zablokuj strony zawierające złośliwy skrypt**

6. Kliknij przycisk **Zapisz**.

# Filtrowanie adresów URL

Funkcja filtrowania adresów URL pomaga w kontrolowaniu dostępu do witryn internetowych w celu zwiększenia produktywności pracowników, ograniczenia zużycia przepustowości połączenia internetowego i tworzenia bezpieczniejszego środowiska roboczego. Można wybrać poziom filtrowania adresów URL lub dostosować listę blokowanych witryn internetowych.

**Uwaga**

W celu ochrony klientów firma Trend Micro automatycznie blokuje wszystkie adresy URL zawierające treści uważane za nielegalne w większości krajów na świecie.

## Konfigurowanie filtrowania adresów URL

Można wybrać określone typy witryn internetowych, które będą blokowane w różnych porach dnia. W tym celu należy wybrać opcję **Niestandardowy**.

**Procedura**

1. Przejdź do menu **Urządzenia**.

2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

   Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.
4. Kliknij opcję **Filtrowanie adresów URL**.

   Zostanie wyświetlony nowy ekran.
5. Zmień odpowiednio następujące ustawienia:
   - **Włącz filtrowanie adresów URL**
   - **Poziom filtrowania**
     - **Wysoki**: blokuje znane lub potencjalne zagrożenia bezpieczeństwa, nieodpowiednią lub obraźliwą zawartość, treści, które mogą wpływać na produktywność czy przepustowość, oraz strony niesklasyfikowane.
     - **Średni**: blokuje znane zagrożenia bezpieczeństwa oraz nieodpowiednią zawartość
     - **Niski**: blokuje zagrożenia bezpieczeństwa.
     - **Niestandardowy**: można wybrać własne kategorie oraz określić, czy mają one być blokowane w godzinach pracy czy w godzinach wolnych.
   - **Zasady filtrowania**: wybierz do blokowania całe kategorie lub podkategorie.
   - **Godziny pracy**: wszystkie dni i godziny, które nie są zdefiniowane jako godziny pracy, są traktowane jak godziny wolne.
6. Kliknij przycisk **Zapisz**.

---

# Dozwolone/zablokowane adresy URL

Automatyczne zatwierdzanie i blokowanie adresów URL pomaga kontrolować dostęp do stron internetowych i stworzyć bezpieczne środowisko internetowe. Dozwolone lub zablokowane adresy URL należy określić w ustawieniach globalnych.

Można także utworzyć niestandardowe listy dozwolonych i zablokowanych adresów URL dla określonych grup. Po zaznaczeniu opcji **Dostosuj dozwolone/zablokowane adresy URL dla tej grupy** program Security Agent wykorzystuje niestandardową listę dozwolonych lub zablokowanych adresów URL w celu kontrolowania dostępu do stron internetowych.

## Konfigurowanie dozwolonych/zablokowanych adresów URL

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

   Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.
4. Kliknij przycisk **Dozwolone/zablokowane adresy URL**.

   Zostanie wyświetlony nowy ekran.
5. Zmień odpowiednio poniższe ustawienia.

   - **Dostosuj dozwolone/zablokowane adresy URL dla tej grupy**: adresy URL uwzględnione na tej liście zastępują wszystkie inne ustawienia.
   - W polu tekstowym **Adresy URL do zatwierdzenia** wpisz adresy URL stron internetowych, które mają być wykluczone z weryfikacji usługi Web Reputation i funkcji filtrowania adresów URL. poszczególne adresy URL oddzielaj średnikiem (;). Kliknij przycisk **Dodaj**.

     **Porada**

     Aby wstawić wszystkie wpisy, kliknij opcję **Importuj z ustawień globalnych**. Następnie możesz dostosować adresy URL dla tej grupy.
   - W polu tekstowym **Adresy URL do zablokowania** wpisz adresy URL stron internetowych, które mają zostać zablokowane podczas filtrowania adresów

URL. poszczególne adresy URL oddzielaj średnikiem (;). Kliknij przycisk **Dodaj**.

**Porada**

Aby wstawić wszystkie wpisy, kliknij opcję **Importuj z ustawień globalnych**. Następnie możesz dostosować adresy URL dla tej grupy.

6. Kliknij przycisk **Zapisz**.

# Zapora

Zapora może blokować lub zezwalać na określone typy ruchu sieciowego przez tworzenie bariery między klientem a siecią. Dodatkowo zapora identyfikuje w pakietach sieciowych sygnatury, które mogą wskazywać na ataki skierowane przeciw klientom.

Program Worry-Free Business Security pozwala wybrać jedną z dwóch opcji podczas konfigurowania zapory: tryb prosty i tryb zaawansowany. W trybie prostym włączane są domyślne ustawienia zapory, zalecane przez firmę Trend Micro. Aby dostosować ustawienia zapory, należy użyć trybu zaawansowanego.

**Porada**

Firma Trend Micro zaleca odinstalowanie innych zapór programowych z klientów przed zainstalowaniem i włączeniem zapory firmy Trend Micro.

## Domyślne ustawienia trybu prostego zapory

Zapora zapewnia ustawienia domyślne, które stanowią podstawę opracowywania strategii ochrony klientów. Domyślne reguły i wyjątki powinny obejmować sytuacje często występujące podczas pracy na klientach, takie jak potrzeba dostępu do Internetu bądź pobierania lub przesyłania plików przy użyciu protokołu FTP.

**Uwaga**

Domyślnie w programie Worry-Free Business Security zapora jest wyłączona dla wszystkich nowych grup i programów Security Agent.

**Tabela 5-5. Domyślne ustawienia zapory**

| Ustawienia | Stan |
|---|---|
| Poziom zabezpieczeń | Niski<br>Dozwolony ruch przychodzący i wychodzący, zablokowane tylko wirusy sieciowe. |
| System wykrywania włamań (IDS) | Wyłączone |
| Komunikat ostrzeżenia (wysyłanie) | Wyłączone |

**Tabela 5-6. Domyślne wyjątki zapory**

| Nazwa wyjątku | Akcja | Kierunek | Protokół | Port |
|---|---|---|---|---|
| DNS | Zezwól | Przychodzące i wychodzące | TCP/UDP | 53 |
| NetBIOS | Zezwól | Przychodzące i wychodzące | TCP/UDP | 137, 138, 139, 445 |
| HTTPS | Zezwól | Przychodzące i wychodzące | TCP | 443 |
| HTTP | Zezwól | Przychodzące i wychodzące | TCP | 80 |
| Telnet | Zezwól | Przychodzące i wychodzące | TCP | 23 |
| SMTP | Zezwól | Przychodzące i wychodzące | TCP | 25 |
| FTP | Zezwól | Przychodzące i wychodzące | TCP | 21 |
| POP3 | Zezwól | Przychodzące i wychodzące | TCP | 110 |
| MSA | Zezwól | Przychodzące i wychodzące | TCP | 16372, 16373 |

| Nazwa wyjątku | Akcja | Kierunek | Protokół | Port |
|---|---|---|---|---|
| LDAP | Zezwól | Przychodzące i wychodzące | TCP/UDP | 389 |

**Tabela 5-7. Domyślne ustawienia zapory zależnie od lokalizacji**

| Lokalizacja | Ustawienia zapory |
|---|---|
| W biurze | Wył. |
| Poza biurem | Wył. |

### Filtrowanie ruchu

Zapora 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
- Komputer docelowy

### Skanowanie w poszukiwaniu wirusów sieciowych

Zapora sprawdza również każdy pakiet pod kątem występowania wirusów sieciowych.

### Kontrola stanowa

Zapora to zapora stanowa, która monitoruje wszystkie próby podłączenia do klienta 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.

### Ogólny sterownik zapory

Ogólny sterownik zapory, w połączeniu ze zdefiniowanymi przez użytkownika ustawieniami zapory, blokuje porty podczas epidemii. W celu wykrycia wirusów sieciowych ogólny sterownik zapory korzysta także z pliku sygnatur wirusów sieciowych.

## Konfigurowanie zapory

Zaporę należy skonfigurować dla lokalizacji W biurze i Poza biurem. Jeśli rozpoznawanie lokalizacji jest wyłączone, dla połączeń Poza biurem będą używane ustawienia W biurze.

Szczegółowe informacje na temat rozpoznawania lokalizacji zawiera część *Konfigurowanie ustawień komputerów/serwerów na stronie 11-5*.

W oprogramowaniu Trend Micro zapora jest domyślnie wyłączona.

---

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

   Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.
4. Kliknij opcję **Zapora** > **W biurze** lub **Poza biurem**.
5. Wybierz opcję **Włącz zaporę**.
6. Wybierz odpowiednie opcje:
   - **Tryb prosty**: Włącza zaporę z ustawieniami domyślnymi.

     Aby uzyskać więcej informacji, zobacz *Zapora na stronie 5-27*.
   - **Tryb zaawansowany**: włącza zaporę z ustawieniami niestandardowymi.
7. W przypadku wybrania opcji **Tryb zaawansowany** zaktualizuj odpowiednio następujące opcje:
   - **Poziom zabezpieczeń**: poziom zabezpieczeń określa reguły ruchu, które mają być stosowane na portach spoza listy wyjątków.

- **Wysoki**: blokuje cały ruch przychodzący i wychodzący z wyjątkiem ruchu dopuszczonego na liście wyjątków.
- **Średni**: blokuje cały ruch przychodzący i zezwala na cały ruch wychodzący z wyjątkiem ruchu dopuszczonego lub zablokowanego na liście wyjątków.
- **Niski**: dopuszcza cały ruch przychodzący i wychodzący z wyjątkiem ruchu zablokowanego na liście wyjątków. Jest to ustawienie domyślne trybu prostego.

- **Ustawienia**
  - **Włącz system wykrywania intruzów**: system wykrywania intruzów identyfikuje w sieciowych pakietach sygnatury, które mogą wskazywać na atak.

    Aby uzyskać więcej informacji, zobacz *System wykrywania włamań (IDS) na stronie D-3*.
  - **Włącz komunikaty ostrzeżeń**: gdy program Worry-Free Business Security wykryje naruszenie, klient zostanie powiadomiony.
- **Wyjątki**: porty na liście wyjątków nie będą blokowane.

  Aby uzyskać więcej informacji, zobacz *Praca z wyjątkami zapory na stronie 5-31*

8. Kliknij przycisk **Zapisz**.

## Praca z wyjątkami zapory

Lista wyjątków zapory zawiera pozycje, które można konfigurować, aby umożliwiać lub blokować różnego rodzaju ruch sieciowy w zależności od numerów portów i adresów IP klientów. Podczas epidemii program Security Server stosuje wyjątki od reguł firmy Trend Micro wdrażanych automatycznie w celu ochrony sieci.

Na przykład podczas epidemii można zablokować cały ruch generowany przez klientów, łącznie z ruchem przez port HTTP (port 80). Jeśli jednak zablokowane klienty mają mieć dostęp do Internetu, można dodać internetowy serwer proxy do listy wyjątków.

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

   Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.
4. Kliknij opcję **Zapora** > **W biurze** lub **Zapora** > **Poza biurem**.

   Zostanie wyświetlony nowy ekran.
5. Wybierz opcję **Włącz zaporę**.
6. Wybierz opcję **Tryb zaawansowany**.
7. Aby dodać wyjątek:
   a. Kliknij przycisk **Dodaj**.

      Zostanie wyświetlony nowy ekran.

   b. Wpisz nazwę wyjątku.

   c. W obszarze **Operacja** kliknij jedną z następujących opcji:

      - **Zezwalaj na cały ruch sieciowy**
      - **Zablokuj cały ruch sieciowy**

   d. W obszarze **Kierunek** kliknij opcję **Przychodzący** lub **Wychodzący**, aby wybrać rodzaj ruchu, do którego należy zastosować ustawienia wyjątków.

   e. Wybierz rodzaj protokołu sieciowego z listy Protokół:

      - **Wszystkie**
      - **TCP/UDP** (domyślne)
      - **TCP**
      - **UDP**

- **ICMP**
- **ICMPv6**

f. Kliknij jedną z poniższych opcji, aby określić porty klienckie:

- **Wszystkie porty** (domyślne)
- **Zakres**: wpisz zakres portów.
- **Określone porty**: Określ pojedyncze porty. Numery portów oddzielaj przecinkiem (,).

g. W obszarze **Komputery** wybierz adresy IP klientów, które należy uwzględnić w wyjątku. Na przykład po wybraniu opcji **Zablokuj cały ruch sieciowy (Ruch przychodzący i wychodzący)** i wpisaniu adresu IP klienta w sieci żaden klient, którego dotyczy ten wyjątek reguły, nie będzie mógł wysyłać ani otrzymywać danych z tego adresu IP. Kliknij jedną z poniższych opcji:

- **Wszystkie adresy IP** (domyślne)
- **Pojedynczy adres IP**: wpisz adres IPv4 lub IPv6 bądź nazwę hosta. Aby uzyskać nazwę hosta klienta w formie adresu IP, kliknij opcję **Rozwiąż**.
- **Zakres IP (dla IPv4 lub IPv6)**: Wpisz dwa adresy IPv4 albo dwa adresy IPv6 w polach **Od** i **Do**. Nie można wpisać w jednym polu adresu IPv6, a w drugim adresu IPv4.
- **Zakres IP (dla IPv6)**: wpisz prefiks adresu IPv6 i długość.

h. Kliknij przycisk **Zapisz**.

**8.** Aby edytować wyjątek, kliknij przycisk **Edytuj** i na wyświetlonym ekranie zmodyfikuj ustawienia.

**9.** Aby przenieść wyjątek w górę lub w dół listy, zaznacz go, a następnie klikaj przyciski **Przesuń w górę** lub **Przesuń w dół**, aż wyjątek znajdzie się na wybranej pozycji.

**10.** Aby usunąć wyjątek, zaznacz go, a następnie kliknij przycisk **Usuń**.

## Wyłączanie zapory w grupie agentów

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

   Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.
4. Kliknij opcję **Zapora** > **W biurze** lub **Zapora** > **Poza biurem**.

   Zostanie wyświetlony nowy ekran.
5. Wybierz polecenie **Wyłącz zaporę**.
6. Kliknij przycisk **Zapisz**.

## Wyłączanie zapory na wszystkich agentach

**Procedura**

1. Przejdź do menu **Administracja** > **Ustawienia globalne**.
2. Kliknij pozycję **Komputer/serwer**.
3. W obszarze **Ustawienia zapory** wybierz opcję **Wyłącz zaporę i odinstaluj sterowniki**.
4. Kliknij przycisk **Zapisz**.

# Kontrola urządzeń

Funkcja kontroli urządzeń nadzoruje dostęp do zewnętrznych urządzeń pamięci masowej podłączonych do punktów końcowych. Funkcja kontroli urządzeń ogranicza

w szczególności dostęp do wszystkich urządzeń pamięci masowej łączących się za pośrednictwem interfejsu USB, z wyjątkiem urządzeń mobilnych i aparatów cyfrowych.

## Konfigurowanie kontroli urządzeń

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

   Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.
4. Kliknij opcję **Kontrola urządzeń**.
5. Zmień odpowiednio następujące ustawienia:
   - **Włącz kontrolę urządzeń**
   - **Włącz zapobieganie automatycznemu uruchamianiu z urządzenia USB**
   - **Uprawnienia**:należy skonfigurować uprawnienia dotyczące zarówno urządzeń USB, jak i zasobów sieciowych.

     **TABELA 5-8. Uprawnienia kontroli urządzeń**

| UPRAWNIENIA | PLIKI NA URZĄDZENIU | PLIKI PRZYCHODZĄCE |
|---|---|---|
| Pełny dostęp | Dozwolone operacje: kopiowanie, przenoszenie, otwieranie, zapisywanie, usuwanie, wykonywanie | Dozwolone operacje: zapisywanie, przenoszenie, kopiowanie<br><br>Oznacza to, że plik można zapisywać, przenosić oraz kopiować na urządzenie. |

| UPRAWNIENIA | PLIKI NA URZĄDZENIU | PLIKI PRZYCHODZĄCE |
|---|---|---|
| Brak dostępu | Niedozwolone operacje: wszystkie operacje<br><br>Urządzenie oraz zapisane na nim pliki są widoczne dla użytkownika (np. z programu Windows Explorer). | Niedozwolone operacje: zapisywanie, przenoszenie, kopiowanie |
| Odczyt | Dozwolone operacje: kopiowanie, otwieranie<br><br>Niedozwolone operacje: zapisywanie, przenoszenie, usuwanie, wykonywanie | Niedozwolone operacje: zapisywanie, przenoszenie, kopiowanie |
| Modyfikuj | Dozwolone operacje: kopiowanie, przenoszenie, otwieranie, zapisywanie, usuwanie<br><br>Niedozwolone operacje: wykonywanie | Dozwolone operacje: zapisywanie, przenoszenie, kopiowanie |
| Odczyt i wykonywanie | Dozwolone operacje: kopiowanie, otwieranie, wykonywanie<br><br>Niedozwolone operacje: zapisywanie, przenoszenie, usuwanie | Niedozwolone operacje: zapisywanie, przenoszenie, kopiowanie |

- **Wyjątki**: jeśli użytkownik nie ma przyznanych uprawnień do odczytu określonego urządzenia, może nadal wykonywać i otwierać dowolne pliki oraz programy znajdujące się na liście elementów zatwierdzonych.

  Jeśli jednak jest włączona usługa zapobiegania automatycznemu uruchamianiu, plików znajdujących się na liście elementów zatwierdzonych nie można uruchamiać.

  Aby dodać wyjątek do listy elementów zatwierdzonych, należy wprowadzić nazwę pliku i ścieżkę lub cyfrowy podpis, a następnie kliknąć polecenie **Dodaj do listy zatwierdzonych**.

6. Kliknij przycisk **Zapisz**.

# Narzędzia użytkownika

- **Pasek narzędzi Anti-Spam**: filtruje spam w programie Microsoft Outlook, prezentuje statystyki i pozwala zmieniać określone ustawienia.
- **HouseCall**: określa bezpieczeństwo połączenia bezprzewodowego poprzez sprawdzanie autentyczności punktów dostępu na podstawie poprawności identyfikatorów SSID, metod uwierzytelniania oraz wymagań szyfrowania tych punktów. Okno podręczne z ostrzeżeniem zostanie wyświetlone, jeżeli połączenie jest niebezpieczne.
- **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 to jest dostępne tylko w konsoli programu Security Agent.
- **Narzędzie Client Mover**: narzędzie to służy do przenoszenia klientów z jednego serwera na drugi. Serwery muszą być tej samej wersji językowej i tego samego typu.
- **Narzędzie komunikacji klient-serwer**: Za pomocą tego narzędzia można rozwiązywać problemy z komunikacją klient-serwer.

## Konfigurowanie narzędzi użytkownika

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.

4. Kliknij opcję **Narzędzia użytkownika**.

   Zostanie wyświetlony nowy ekran.

5. Zmień odpowiednio następujące ustawienia:

   - **Narzędzie Wi-Fi Advisor**: Sprawdza bezpieczeństwo sieci bezprzewodowych pod względem poprawności identyfikatorów SSID, metod uwierzytelniania oraz wymagań szyfrowania.
   - **Pasek narzędzi Anti-spam Toolbar** : Filtruje spam w programie Microsoft Outlook.

6. Kliknij przycisk **Zapisz**.

# Uprawnienia agenta

Istnieje możliwość przyznawania agentom uprawnień do modyfikowania ustawień programu Security Agent na danym kliencie.

**Porada**

Aby zachować określone zasady zabezpieczeń w całej organizacji, firma Trend Micro zaleca nadanie użytkownikom ograniczonych uprawnień. Dzięki temu użytkownicy nie będą mogli modyfikować ustawień skanowania ani usuwać programu Security Agent z pamięci.

## Konfigurowanie uprawnień agenta

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz grupę komputerów lub serwerów.
3. Kliknij pozycję **Konfiguruj regułę**.

Pojawi się ekran **Konfiguruj regułę: <nazwa grupy>**.

4. Kliknij opcję **Uprawnienia agenta**.

5. Zmień odpowiednio następujące ustawienia:

| SEKCJA | UPRAWNIENIA |
|---|---|
| Oprogramowanie antywirusowe/ antyszpiegowskie | • Ustawienia skanowania w czasie rzeczywistym<br>• Ustawienia skanowania ręcznego<br>• Ustawienia skanowania zaplanowanego<br>• Pomiń skanowanie zaplanowane |
| Zapora | Ustawienia zapory |
| Usługa Web Reputation — Kontynuuj przeglądanie | Zostanie wyświetlone łącze umożliwiające użytkownikom kontynuowanie przeglądania konkretnego złośliwego adresu URL do momentu ponownego uruchomienia komputera. W dalszym ciągu będą wyświetlane ostrzeżenia dotyczące innych złośliwych adresów URL. |
| Filtrowanie adresów URL — Kontynuuj przeglądanie | Zostanie wyświetlone łącze umożliwiające użytkownikom kontynuowanie przeglądania konkretnego adresu URL objętego ograniczeniami do momentu ponownego uruchomienia komputera. W dalszym ciągu będą wyświetlane ostrzeżenia dotyczące innych adresów URL objętych ograniczeniami. |
| Monitorowanie zachowania | Pozwalaj użytkownikom modyfikować ustawienia monitorowania zachowania. |
| Zaufany program | Pozwalaj użytkownikom na modyfikowanie listy zaufanych programów. |
| Ustawienia proxy | Pozwalaj użytkownikom na konfigurowanie ustawień proxy.<br><br>**Uwaga**<br>Wyłączenie tej funkcji spowoduje przywrócenie domyślnych ustawień proxy. |

| SEKCJA | UPRAWNIENIA |
|---|---|
| Aktualizuj uprawnienia | • Pozwalaj użytkownikom na przeprowadzanie ręcznych aktualizacji<br>• Użyj serwera Trend Micro ActiveUpdate jako dodatkowego źródła aktualizacji<br>• Wyłącz wdrażanie pakietów hot fix<br><br>**Uwaga**<br>Wdrażanie pakietów hot fix, poprawek, poprawek bezpieczeństwa/krytycznych oraz dodatków Service Pack jednocześnie na dużej liczbie agentów może znacząco zwiększyć ruch sieciowy. Należy zastanowić się nad włączeniem tej opcji w kilku grupach, aby rozłożyć wdrożenie w czasie.<br><br>Włączenie tej opcji spowoduje również wyłączenie automatycznych **uaktualnień kompilacji** na agentach (na przykład z kompilacji beta do kompilacji wydania bieżącej wersji produktu), jednak NIE spowoduje wyłączenia automatycznych **uaktualnień wersji** (na przykład z wersji 7.x do bieżącej wersji). Aby wyłączyć automatyczne uaktualnienia wersji, należy uruchomić pakiet instalacyjny serwera zabezpieczeń Security Server i wybrać opcję opóźniania uaktualnień. |
| Zabezpieczenia klienta | Uniemożliwia użytkownikom lub procesom modyfikowanie plików programów Trend Micro, rejestrów i procesów. |

6. Kliknij przycisk **Zapisz**.

# Rozdział 6

# Zarządzanie podstawowymi ustawieniami zabezpieczeń w programach Messaging Security Agent (tylko w wersji Advanced)

W tym rozdziale opisano program Messaging Security Agent i wyjaśniono sposób korzystania z opcji skanowania w czasie rzeczywistym, konfigurowania ustawień ochrony antyspamowej, filtrowania zawartości, blokowania załączników oraz obsługi kwarantanny w tym programie.

# Messaging Security Agent

Programy Messaging Security Agent chronią serwery Microsoft Exchange. Agent pomaga unieszkodliwiać zagrożenia rozprzestrzeniające się za pośrednictwem poczty e-mail przez skanowanie wiadomości przychodzących do i wychodzących z magazynu skrzynek pocztowych programu Microsoft Exchange, jak również poczty e-mail przesyłanej między serwerem Microsoft Exchange a adresami zewnętrznymi. Ponadto program Messaging Security Agent pozwala:

- zmniejszać ilość spamu;
- blokować wiadomości e-mail na podstawie zawartości;
- blokować lub ograniczać wiadomości e-mail z załącznikami;
- wykrywać złośliwe adresy URL w wiadomościach e-mail;
- zapobiegać wyciekom poufnych danych.

## Ważne informacje o programach Messaging Security Agent

- Program Messaging Security Agent można instalować tylko na serwerach Microsoft Exchange.
- Program Messaging Security Agent nie obsługuje niektórych funkcji serwera Microsoft Exchange Server Enterprise, takich jak grupa dostępności danych.
- Wszystkie programy Messaging Security Agent wyświetlane są w drzewie grup zabezpieczeń w konsoli internetowej. Nie można połączyć w grupę wielu programów Messaging Security Agent. Administrowanie i zarządzanie każdym z nich musi odbywać się oddzielnie.
- Program Worry-Free Business Security używa programu Messaging Security Agent do zbierania informacji na temat zabezpieczeń z serwerów Microsoft Exchange. Program Messaging Security Agent zgłasza na przykład wykrycie spamu lub zakończenie aktualizacji składników programu Security Server. Informacje te są wyświetlane w konsoli internetowej. Program Security Server używa też tych informacji do generowania dzienników i raportów dotyczących stanu zabezpieczeń serwerów Microsoft Exchange.

  Każde wykrycie zagrożenia powoduje wygenerowanie jednego wpisu w dzienniku/powiadomienia. Oznacza to, że wykrycie wielu zagrożeń w pojedynczej wiadomości

e-mail przez program Messaging Security Agent spowoduje wygenerowanie wielu wpisów w dzienniku i powiadomień. To samo zagrożenie może zostać wykryte wielokrotnie, szczególnie w przypadku pracy w trybie buforowym w programie Outlook 2003. Po uruchomieniu trybu buforowego to samo zagrożenie może zostać wykryte w folderze kolejki transportu oraz folderze Elementy wysłane lub w folderze Skrzynka nadawcza.

- W przypadku komputerów korzystających z programu Exchange Server 2007 program Messaging Security Agent korzysta z bazy danych serwera SQL. Aby zapobiec problemom, usługi programu Messaging Security Agent są zależne od instancji usługi serwera SQL `MSSQL$SCANMAIL`. W momencie, gdy ta instancja zostanie zatrzymana lub uruchomiona ponownie, następujące usługi programu Messaging Security Agent również zostaną zatrzymane:

  - `ScanMail_Master`
  - `ScanMail_RemoteConfig`

  Jeżeli usługa `MSSQL$SCANMAIL` zostanie zatrzymana lub uruchomiona ponownie, należy ponownie uruchomić te usługi ręcznie. W innych sytuacjach, np. w momencie aktualizacji serwera SQL Server, może dojść do ponownego uruchomienia lub zatrzymania usługi `MSSQL$SCANMAIL`.

## Skanowanie wiadomości e-mail przez program Messaging Security Agent

Program Messaging Security Agent korzysta z następującej procedury w celu skanowania wiadomości e-mail:

1. Skanowanie pod kątem spamu (funkcja Antyspam)
   a. Porównywanie wiadomości e-mail z listą dozwolonych/zablokowanych nadawców administratora
   b. Sprawdzanie pod kątem zagrożeń typu phishing
   c. Porównywanie wiadomości e-mail z listą wyjątków dostarczoną przez firmę Trend Micro
   d. Porównywanie wiadomości e-mail z bazą danych sygnatur spamu

e. Stosowanie reguł skanowania heurystycznego

2. Skanowanie pod kątem naruszenia reguł filtrowania zawartości
3. Skanowanie pod kątem załączników przekraczających parametry zdefiniowane przez użytkownika
4. Skanowanie w poszukiwaniu wirusów/złośliwego oprogramowania (funkcja antywirusowa)
5. Skanowanie w poszukiwaniu złośliwych adresów URL

## Domyślne ustawienia programu Messaging Security Agent

Opcje wymienione w tabeli ułatwiają optymalizację konfiguracji programu Messaging Security Agent.

**TABELA 6-1. Operacje domyślne programu Messaging Security Agent**

| OPCJA SKANOWANIA | SKANOWANIE W CZASIE RZECZYWISTYM | SKANOWANIE RĘCZNE I ZAPLANOWANE |
|---|---|---|
| **Ochrona antyspamowa** | | |
| Spam | Poddaj wiadomość kwarantannie w folderze spamu użytkownika (domyślna opcja, jeżeli zainstalowano filtr wiadomości-śmieci w programie Outlook lub narzędzie End User Quarantine) | Nie dotyczy |
| Phishing | Usuń całą wiadomość | Nie dotyczy |
| **Filtrowanie zawartości** | | |
| Filtruj wiadomości, które spełniają którykolwiek ze zdefiniowanych warunków | Poddaj całą wiadomość kwarantannie | Zamień |

| Opcja skanowania | Skanowanie w czasie rzeczywistym | Skanowanie ręczne i zaplanowane |
|---|---|---|
| Filtruj wiadomości, które spełniają wszystkie zdefiniowane warunki | Poddaj całą wiadomość kwarantannie | Nie dotyczy |
| Monitoruj zawartość wiadomości z konkretnych kont e-mail | Poddaj całą wiadomość kwarantannie | Zamień |
| Utwórz wyjątki dla konkretnych kont e-mail | Pomiń | Pomiń |
| **Blokowanie załączników** | | |
| Akcja | Zastąp załącznik tekstem/ plikiem | Zastąp załącznik tekstem/ plikiem |
| **Inne** | | |
| Pliki zaszyfrowane i chronione hasłem | Pomiń (po skonfigurowaniu akcji „Pomiń” pliki zaszyfrowane oraz pliki chronione hasłem są pomijane, a zdarzenie nie jest rejestrowane). | Pomiń (po skonfigurowaniu akcji „Pomiń” pliki zaszyfrowane oraz pliki chronione hasłem są pomijane, a zdarzenie nie jest rejestrowane). |
| Pliki wykluczone (pliki wykraczające poza określone ograniczenia skanowania) | Pomiń (po skonfigurowaniu operacji „Pomiń” pliki lub treść wiadomości wykraczające poza określone ograniczenia skanowania są pomijane, a zdarzenie nie jest rejestrowane). | Pomiń (po skonfigurowaniu operacji „Pomiń” pliki lub treść wiadomości wykraczające poza określone ograniczenia skanowania są pomijane, a zdarzenie nie jest rejestrowane). |

# Skanowanie w czasie rzeczywistym w programach Messaging Security Agent

Skanowanie w czasie rzeczywistym zapewnia stałą ochronę. Funkcja skanowania w czasie rzeczywistym w programie **Messaging Security Agent** (tylko w wersji Advanced) pozwala chronić wszystkie znane punkty wejścia wirusów: wszystkie przychodzące wiadomości e-mail, wiadomości SMTP, dokumenty wysyłane do folderów publicznych oraz pliki replikowane z innych serwerów Microsoft Exchange.

## Konfigurowanie skanowania w czasie rzeczywistym dla programów Messaging Security Agent

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij opcję **Ochrona antywirusowa**.

   Zostanie wyświetlony nowy ekran.
5. Zaznacz opcję **Włącz ochronę antywirusową w czasie rzeczywistym**.
6. Skonfiguruj ustawienia skanowania. Aby uzyskać więcej informacji, zobacz *Cele skanowania i operacje dotyczące programów Messaging Security Agent na stronie 7-20*.
7. Kliknij przycisk **Zapisz**.

   Skonfiguruj odbiorców powiadomień w przypadku wystąpienia zdarzenia. Patrz sekcja *Konfigurowanie zdarzeń dla powiadomień na stronie 10-5*.

# Ochrona antyspamowa

Program Worry-Free Business Security udostępnia dwie metody zwalczania spamu: usługi **Email Reputation** i **Skanowanie zawartości**

Program Messaging Security Agent korzysta z następujących elementów w celu filtrowania wiadomości e-mail i zdarzeń typu phishing:

- Silnik antyspamowy firmy Trend Micro
- Pliki sygnatur spamu firmy Trend Micro

Firma Trend Micro często aktualizuje zarówno silnik, jak i plik sygnatur i udostępnia je do pobrania. Program Security Server może pobrać te składniki za pomocą ręcznej lub zaplanowanej aktualizacji.

W celu filtrowania wiadomości e-mail silnik anty-spam korzysta z sygnatur wirusów i reguł heurystycznych. Skanuje on wiadomości e-mail i na podstawie stopnia dopasowania do reguł i sygnatur zawartych w pliku sygnatur przypisuje każdej z nich ocenę dotyczącą zawartości spamu. Program Messaging Security Agent porównuje stopień dopasowania do reguł z określonym przez użytkownika poziomem wykrywania spamu. Kiedy stopień dopasowania do reguł przekracza poziom wykrywania, agent wykonuje odpowiednią operację w odniesieniu do spamu.

Na przykład: Spamerzy często używają w wiadomościach e-mail wielu wykrzykników lub ciągów znaków składających się z kilku wykrzykników (!!!!). Gdy program Messaging Security Agent wykryje wiadomość charakteryzującą się takim użyciem znaków wykrzyknika, podwyższa ocenę dotyczącą zawartości spamu dla danej wiadomości e-mail.

**Porada**

Oprócz zastosowania anty-spamu do blokowania spamu, można skonfigurować funkcję filtrowania zawartości tak, aby w celu odfiltrowania spamu i innej, niepożądanej zawartości filtrowała nagłówek wiadomości, jej temat, treść i informacje o załączniku.

Użytkownicy nie mogą zmodyfikować metody, z której silnik anty-spam korzysta w celu oceny stopnia dopasowania do reguł, ale mogą dostosować poziomy wykrywania, stosowane przez program Messaging Security Agent, aby określić, jakie wiadomości są spamem.

**Uwaga**

Program Microsoft Outlook może automatycznie filtrować wiadomości, które program Messaging Security Agent wykrył jako spam, i przesyłać je do folderu wiadomości-śmieci.

## Usługa Email Reputation

Technologia Email Reputation określa spam na podstawie reputacji źródłowego agenta MTA (Mail Transport Agent). Zwalnia to program Security Server z konieczności wykonywania tego zadania. Po włączeniu usługi Email Reputation cały przychodzący ruch SMTP jest sprawdzany przez bazy danych adresów IP w celu ustalenia, czy źródłowy adres IP jest poprawny lub czy nie został umieszczony na liście jako znany dostawca spamu.

Istnieją dwa poziomy usługi dla usługi Email Reputation. Zostały one przedstawione poniżej:

- **Standardowy**: usługa standardowa korzysta z bazy danych, która śledzi reputację około dwóch miliardów adresów IP. Adresy IP, które są stale powiązane z dostarczaniem wiadomości typu spam, zostają dodane do bazy danych i rzadko są z niej usuwane.
- **Zaawansowany**: poziom zaawansowany to usługa DNS, która jest oparta na zapytaniach i przypomina usługę standardową. Podstawą tej usługi jest standardowa baza danych reputacji oraz dynamiczna baza danych reputacji, która blokuje wiadomości ze znanych i podejrzanych źródeł spamu.

Po znalezieniu wiadomości e-mail z zablokowanego lub podejrzanego adresu IP funkcja Email Reputation blokuje tę wiadomość, zanim osiągnie ona bramę.

### Konfigurowanie usługi Email Reputation

Usługę Email Reputation należy skonfigurować w celu blokowania wiadomości ze znanych lub podejrzanych źródeł spamu. Ponadto można utworzyć wyłączenia, aby dopuścić lub blokować wiadomości od innych nadawców.

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij pozycje **Ochrona antyspamowa** > **Email Reputation**.

   Zostanie wyświetlony nowy ekran.
5. Zmień odpowiednio następujące opcje na karcie **Miejsce docelowe**:
   - **Włącz oprogramowanie antyspamowe działające w czasie rzeczywistym (usługa Email Reputation)**
   - **Poziom usługi**:
     - **Standardowy**
     - **Zaawansowany**
   - **Dozwolone adresy IP**: wiadomości e-mail z tych adresów IP nigdy nie będą blokowane. Wpisz adres IP do zatwierdzenia i kliknij przycisk **Dodaj**. W razie potrzeby można zaimportować listę adresów IP z pliku tekstowego. Aby usunąć adres IP, wybierz adres i kliknij przycisk **Usuń**.
   - **Zablokowane adresy IP**: wiadomości e-mail z tych adresów IP będą zawsze blokowane. Wpisz adres IP do zablokowania i kliknij przycisk **Dodaj**. W razie potrzeby można zaimportować listę adresów IP z pliku tekstowego. Aby usunąć adres IP, wybierz adres i kliknij przycisk **Usuń**.
6. Kliknij przycisk **Zapisz**.
7. Przejdź do witryny: http://ers.trendmicro.com/, aby przeglądać raporty.

**Uwaga**

Email Reputation jest usługą internetową. Z poziomu konsoli internetowej administrator może skonfigurować tylko poziom usługi.

## Skanowanie zawartości

Skanowanie zawartości identyfikuje spam na podstawie zawartości wiadomości, a nie jej źródłowego adresu IP. Program Messaging Security Agent używa silnika antyspamowego i plików sygnatur spamu firmy Trend Micro do badania wszystkich wiadomości e-mail pod względem spamu przed dostarczeniem ich do magazynu informacji. Serwer Microsoft Exchange nie przetwarza odrzuconych wiadomości zawierających spam, dzięki czemu nie trafiają one do skrzynek pocztowych użytkowników.

**Uwaga**

Nie należy mylić skanowania zawartości (ochrona przed spamem na podstawie sygnatur i reguł heurystycznych) z filtrowaniem zawartości (skanowanie wiadomości e-mail i blokowanie ich na podstawie określonych słów kluczowych). Patrz sekcja *Filtrowanie zawartości na stronie 6-16*.

### Konfigurowanie skanowania zawartości

Program Messaging Security Agent wykrywa wiadomości typu spam w **czasie rzeczywistym** i podejmuje działania chroniące serwery Microsoft Exchange.

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij pozycje **Ochrona antyspamowa** > **Skanowanie zawartości**.

   Zostanie wyświetlony nowy ekran.

5. Wybierz pozycję **Włącz ochronę antyspamową działającą w czasie rzeczywistym**.

6. Wybierz kartę **Cel**, aby wybrać metodę oraz współczynnik wykrywania spamu, których program Messaging Security Agent używa do blokowania spamu.

   a. Wybierz poziom wykrywania (**niski**, **średni** lub **wysoki**) z listy współczynników wykrywania spamu. Program Messaging Security Agent używa tego współczynnika do blokowania wszystkich wiadomości.

      - **Wysoki**: Jest to najbardziej rygorystyczny poziom wykrywania spamu. Program Messaging Security Agent monitoruje wszystkie wiadomości e-mail w poszukiwaniu podejrzanych plików lub tekstu, ale powoduje to zwiększenie liczby fałszywych alarmów. Fałszywe alarmy to wiadomości e-mail, które program Messaging Security Agent filtruje jako spam, chociaż są one prawidłowymi wiadomościami e-mail.

      - **Średni**: jest to ustawienie domyślne i zalecane. Program Messaging Security Agent monitoruje na wysokim poziomie wykrywania spamu przy średnim ryzyku wystąpienia fałszywych alarmów.

      - **Niski**: jest to najmniej rygorystyczny poziom wykrywania spamu. Program Messaging Security Agent będzie filtrował najbardziej oczywiste i powszechne wiadomości typu spam, pomijając zwykle fałszywe alarmy. Filtrowanie według stopnia dopasowania.

   b. Kliknij pozycję **Wykrywanie zdarzeń typu phishing**, aby program Messaging Security Agent blokował zdarzenia typu phishing. Aby uzyskać więcej informacji, zobacz *Zdarzenie typu phishing na stronie 1-14*.

   c. Dodaj adresy do list Zatwierdzeni nadawcy i Zablokowani nadawcy. Aby uzyskać więcej informacji, zobacz *Listy dozwolonych i zablokowanych nadawców na stronie 6-13*.

      - **Zatwierdzeni nadawcy**: Wiadomości e-mail z tych adresów lub nazw domen nigdy nie będą blokowane. Wpisz adresy lub nazwy domen do zatwierdzenia, a następnie kliknij przycisk **Dodaj**. W razie potrzeby można zaimportować listę adresów lub nazw domen z pliku tekstowego. Aby usunąć adresy lub nazwy domen, wybierz adres i kliknij przycisk **Usuń**.

- **Zablokowani nadawcy**: wiadomości e-mail z tych adresów lub nazw domen będą zawsze blokowane. Wpisz adresy lub nazwy domen do zablokowania, a następnie kliknij przycisk **Dodaj**. W razie potrzeby można zaimportować listę adresów lub nazw domen z pliku tekstowego. Aby usunąć adresy lub nazwy domen, wybierz adres i kliknij przycisk **Usuń**.

**Uwaga**

Administrator serwera Microsoft Exchange prowadzi oddzielną listę zatwierdzonych i zablokowanych nadawców dla serwera Microsoft Exchange. Jeśli użytkownik końcowy utworzy zatwierdzonego nadawcę, ale ten nadawca będzie znajdować się na liście nadawców zablokowanych utworzonej przez administratora, program Messaging Security Agent uzna wiadomości od tego nadawcy za spam i podejmie akcję przeciwko tym wiadomościom.

7. Wybierz kartę **Operacja**, aby określić działania, jakie program Messaging Security Agent będzie wykonywać po wykryciu wiadomości będącej spamem lub zdarzenia typu phishing.

**Uwaga**

Szczegółowe informacje na temat operacji zawiera sekcja *Cele skanowania i operacje dotyczące programów Messaging Security Agent na stronie 7-20*.

Program Messaging Security Agent, w zależności od konfiguracji, podejmuje jedno z następujących działań:

- **Poddaj wiadomość kwarantannie w folderze spamu na serwerze**
- **Poddaj wiadomość kwarantannie w folderze wiadomości typu spam użytkownika**

**Uwaga**

Po wybraniu tego działania skonfiguruj narzędzie End User Quarantine. Aby uzyskać więcej informacji, zobacz *Konfigurowanie obsługi wiadomości typu spam na stronie 6-74*.

- **Usuń całą wiadomość**
- **Oznacz i dostarcz**

8. Kliknij przycisk **Zapisz**.

## Listy dozwolonych i zablokowanych nadawców

Lista zatwierdzonych nadawców to lista zaufanych nadawców wiadomości e-mail. Program Messaging Security Agent nie filtruje pod kątem spamu wiadomości nadesłanych z tych adresów, z wyjątkiem sytuacji, gdy włączona jest opcja **Wykrywanie zdarzeń typu phishing**. Jeśli opcja **Wykrywanie zdarzeń typu phishing** jest włączona i agent wykryje zdarzenie typu phishing w wiadomości e-mail, taka wiadomość nie zostanie dostarczona, nawet jeśli pochodzi od nadawcy umieszczonego na liście dozwolonych nadawców. Lista zablokowanych nadawców to lista podejrzanych adresów e-mail. Wiadomości e-mail od zablokowanych nadawców agent zawsze klasyfikuje jako spam i wykonuje odpowiednią operację.

Istnieją dwie listy zatwierdzonych nadawców: lista dla administratora serwera Microsoft Exchange i lista dla użytkowników końcowych.

- Lista dozwolonych nadawców i lista zablokowanych nadawców administratora serwera Microsoft Exchange (na ekranie **Antyspam**) umożliwia kontrolowanie, w jaki sposób program Messaging Security Agent obsługuje wiadomości e-mail wysyłane na serwer Microsoft Exchange.
- Użytkownicy końcowi zarządzają folderem spamu, który jest dla nich tworzony podczas instalacji programu. Listy użytkowników końcowych wpływają tylko na wiadomości wysłane do magazynu skrzynek pocztowych poszczególnych użytkowników końcowych po stronie serwera.

### Wytyczne ogólne

- Listy zatwierdzonych i zablokowanych nadawców na serwerze Microsoft Exchange mają wyższy priorytet niż listy zatwierdzonych i zablokowanych nadawców na kliencie. Na przykład, nadawca „uzytkownik@przyklad.com” znajduje się na liście zablokowanych nadawców administratora, ale użytkownik końcowy dodał ten adres do swojej listy dozwolonych nadawców. Wiadomości od tego nadawcy docierają do magazynu serwera Microsoft Exchange, a program Messaging Security Agent

wykrywa je jako spam i wykonuje na nich operacje. Jeśli agent wykona operację „Poddaj wiadomość kwarantannie w folderze wiadomości typu spam użytkownika", spróbuje dostarczyć wiadomość do folderu spamu użytkownika końcowego. Wiadomość zostanie jednak przekierowana do skrzynki odbiorczej tego użytkownika, ponieważ zezwolił on na odbieranie wiadomości od tego nadawcy.

- W przypadku programu Outlook istnieje limit wielkości, który dotyczy liczby i długości adresów na liście. W celu uniknięcia błędu systemowego program Messaging Security Agent ogranicza ilość adresów, które użytkownik końcowy może umieścić na swojej liście dozwolonych nadawców (ten limit oblicza się zależnie od długości i liczby adresów e-mail).

### Dopasowanie z zastosowaniem symboli wieloznacznych

Program Messaging Security Agent obsługuje dopasowanie z zastosowaniem symboli wieloznacznych dla list nadawców dozwolonych i zablokowanych. Jako symbol wieloznaczny używana jest gwiazdka (*).

Program Messaging Security Agent nie obsługuje dopasowania z zastosowaniem symboli wieloznacznych w części „nazwa użytkownika". Po wpisaniu wzorca takiego jak „*@trend.com" agent potraktuje go jednak jako „@trend.com".

Symbolu wieloznacznego można używać tylko w następujących miejscach:

- obok tylko jednej kropki i pierwszego lub ostatniego znaku łańcucha,
- po lewej stronie symbolu @ i pierwszego znaku łańcucha,
- dowolna brakująca część łańcucha na jego początku lub końcu pełni taką samą rolę co symbol wieloznaczny.

**TABELA 6-2. Dopasowanie adresu e-mail z zastosowaniem symboli wieloznacznych**

| WZORZEC | PRZYKŁADY DOPASOWANIA | PRZYKŁADY NIEDOPASOWANIA |
|---|---|---|
| jan@przyklad.com | jan@przyklad.com | Każdy adres inny niż wzorzec. |

| Wzorzec | Przykłady dopasowania | Przykłady niedopasowania |
|---|---|---|
| @przyklad.com<br>*@przyklad.com | jan@przyklad.com<br>maria@przyklad.com | jan@ms1.przyklad.com<br>jan@przyklad.com.pl<br>maria@przyklad.com.pl |
| przyklad.com | jan@przyklad.com<br>jan@ms1.przyklad.com<br>maria@ms1.rd.przyklad.com<br>maria@przyklad.com | jan@przyklad.com.pl<br>maria@mojprzyklad.com.pl<br>jurek@przyklad.comon |
| *.przyklad.com | jan@ms1.przyklad.com<br>maria@ms1.rd.przyklad.com<br>jurek@ms1.przyklad.com. | jan@przyklad.com<br>jan@mojprzyklad.com.pl<br>maria@ms1.przyklad.comon |
| przyklad.com.* | jan@przyklad.com.pl<br>jan@ms1.przyklad.com.pl<br>jan@ms1.rd.przyklad.com.pl<br>maria@przyklad.com.pl | jan@przyklad.com<br>maria@ms1.przyklad.com<br>jan@mojprzyklad.com.pl |
| *.przyklad.com.* | jan@ms1.przyklad.com.pl<br>jan@ms1.rd.przyklad.com.pl<br>maria@ms1.przyklad.com.pl | jan@przyklad.com<br>jan@ms1.przyklad.com<br>jan@trend.przyklad.pl |
| *.*.*.przyklad.com<br>*****.przyklad.com | Takie same jak „*.przyklad.com” | |

| WZORZEC | PRZYKŁADY DOPASOWANIA | PRZYKŁADY NIEDOPASOWANIA |
|---|---|---|
| *przyklad.com<br>przyklad.com*<br>przyklad.*.com<br>@*.przyklad.com | Nieprawidłowe wzorce | |

# Filtrowanie zawartości

Funkcja Filtrowanie zawartości ocenia przychodzące i wychodzące wiadomości e-mail na podstawie reguł określonych przez użytkownika. Każda reguła zawiera listę słów kluczowych i fraz. Funkcja Filtrowanie zawartości ocenia nagłówek i/lub zawartość wiadomości przez ich porównanie z listą słów kluczowych. Gdy filtr zawartości znajdzie słowo zgodne ze słowem kluczowym, może wykonać operację, która zapobiega dostarczeniu niepożądanej zawartości do klientów Microsoft Exchange. Program Messaging Security Agent może wysyłać powiadomienia za każdym razem, gdy podejmuje operacje przeciw niepożądanej zawartości.

**Uwaga**

Nie należy mylić skanowania zawartości (ochrona przed spamem na podstawie sygnatur i reguł heurystycznych) z filtrowaniem zawartości (skanowanie wiadomości e-mail i blokowanie ich na podstawie określonych słów kluczowych). Patrz sekcja *Skanowanie zawartości na stronie 6-10*.

Filtr zawartości umożliwia administratorom ocenę i kontrolę dostarczania poczty e-mail na podstawie samego tekstu wiadomości. Można go użyć do monitorowania przychodzących i wychodzących wiadomości e-mail w celu sprawdzenia ich pod kątem występowania napastliwych, obraźliwych lub innych niepożądanych treści. Filtr zawartości zawiera także funkcję sprawdzania synonimów, która umożliwia rozszerzenie zasięgu reguł. Można na przykład utworzyć reguły sprawdzające:

- Napastliwe treści o charakterze seksualnym

- Treści rasistowskie
- Spam osadzony w treści wiadomości e-mail

**Uwaga**

Domyślnie filtrowanie zawartości jest wyłączone.

## Zarządzanie regułami filtrowania zawartości

Wszystkie reguły filtrowania zawartości w programie Messaging Security Agent wyświetlane są na ekranie **Filtrowanie zawartości**. Aby uzyskać dostęp do tego ekranu, przejdź do pozycji:

- W przypadku skanowania w czasie rzeczywistym:

  **Urządzenia** > **{Messaging Security Agent}** > **Konfiguruj regułę** > **Filtrowanie zawartości**

- Skanowanie ręczne:

  **Skanowania** > **Ręczne** > **{rozwiń pozycję Messaging Security Agent}** > **Filtrowanie zawartości**

- Skanowanie zaplanowane:

  **Skanowania** > **Zaplanowane** > **{rozwiń pozycję Messaging Security Agent}** > **Filtrowanie zawartości**

**Procedura**

1. Przejrzyj podsumowanie informacji na temat reguł, w tym:

   - **Reguła**: Program Worry-Free Business Security zawiera domyślne reguły filtrujące zawartość według następujących kategorii: **wulgaryzmy**, **dyskryminacja rasowa**, **dyskryminacja ze względu na orientację seksualną**, **fałszerstwa** i **łańcuszki**. Są one domyślnie wyłączone. Reguły te można zmienić odpowiednio do wymagań albo usunąć. Jeśli żadna z reguł nie spełnia wymagań, dodaj własne reguły.

- **Operacja**: program Messaging Security Agent wykonuje tę operację po wykryciu niepożądanej treści.
- **Priorytet**: program Messaging Security Agent stosuje poszczególne filtry zgodnie z kolejnością wyświetlaną na tej stronie.
- **Włączone**: ikona w kolorze zielonym oznacza regułę włączoną, a ikona w kolorze czerwonym — wyłączoną.

2. Wykonaj następujące czynności:

| ZADANIE | CZYNNOŚCI |
|---|---|
| Włączanie/ wyłączanie filtrowania zawartości | Zaznacz lub usuń zaznaczenie pola **Włącz filtrowanie zawartości w czasie rzeczywistym** na górze ekranu. |
| Dodawanie reguły | Kliknij przycisk **Dodaj**.<br><br>Pojawi się nowy ekran, gdzie można wybrać typ dodawanej reguły. Szczegółowe informacje zawiera część *Typy reguł filtrowania zawartości na stronie 6-21*. |

| ZADANIE | CZYNNOŚCI |
|---|---|
| Modyfikowanie reguły | a. Kliknij nazwę reguły.<br><br>Zostanie wyświetlony nowy ekran.<br><br>b. Opcje dostępne na tym ekranie zależą od typu reguły. Aby określić typ reguły, zaznacz krótkie informacje znajdujące się na górze ekranu i zwróć uwagę na ich drugi element. Na przykład:<br><br>Filtrowanie zawartości > **Dopasuj dowolny warunek reguły** > Edytuj regułę<br><br>Szczegółowe informacje na temat ustawień reguł, które można modyfikować, zawierają poniższe tematy:<br><br>• *Dodawanie reguły filtrowania zawartości w przypadku zgodności dowolnego warunku na stronie 6-25*<br><br>• *Dodawanie reguły filtrowania zawartości w przypadku zgodności wszystkich warunków na stronie 6-22*<br><br>**Uwaga**<br>Ten typ reguły jest niedostępny w przypadku ręcznego i planowanego skanowania filtrowania zawartości.<br><br>• *Dodawanie reguły monitorowania filtrowania zawartości na stronie 6-28*<br><br>• *Tworzenie wyjątków do reguł filtrowania zawartości na stronie 6-31* |

| Zadanie | Czynności |
|---|---|
| Zmiana kolejności reguł | Program Messaging Security Agent stosuje reguły filtrowania zawartości w stosunku do wiadomości e-mail w kolejności wyświetlanej na ekranie **Filtrowanie zawartości**. Istnieje możliwość określenia kolejności stosowania reguł. Agent filtruje wszystkie wiadomości e-mail zgodnie z każdą z reguł, dopóki naruszenie zawartości nie uruchomi operacji uniemożliwiającej dalsze skanowanie (takiej jak usunięcie lub poddanie kwarantannie). Aby zoptymalizować filtrowanie zawartości, można zmienić kolejność reguł.<br><br>a. Zaznacz pole wyboru odpowiadające regule, której kolejność chcesz zmienić.<br><br>b. Kliknij opcję **Zmień kolejność**.<br><br>Wokół liczby wskazującej kolejność reguły zostanie wyświetlone pole.<br><br>c. Usuń istniejący numer kolejności w polu kolumny **Priorytet** i wpisz nowy numer.<br><br>**Uwaga**<br>Należy pamiętać, że nie można wprowadzić numeru większego od łącznej liczby reguł na liście. W razie wprowadzenia numeru większego od łącznej liczby reguł program Worry-Free Business Security zignoruje taki wpis i nie zmieni kolejności reguł.<br><br>d. Kliknij przycisk **Zapisz zmienioną kolejność**.<br><br>Reguła zostanie przesunięta na wprowadzony poziom priorytetu, a numery wszystkich pozostałych reguł zostaną odpowiednio zmienione.<br><br>Na przykład wybranie reguły o numerze 5 i zmiana tego numeru na 3 spowoduje, że reguły o numerach 1 i 2 pozostaną bez zmian, natomiast numery pozostałych reguł, począwszy od numeru 3, zostaną zwiększone o 1. |
| Włączanie/ wyłączanie reguł | Kliknij ikonę w kolumnie Włączone. |

| ZADANIE | CZYNNOŚCI |
|---|---|
| Usuwanie reguł | Po usunięciu reguły program Messaging Security Agent aktualizuje kolejność innych reguł, aby uwzględnić zmianę.<br><br>**Uwaga**<br>Usunięcie reguły jest nieodwracalne, dlatego należy rozważyć możliwość wyłączenia reguły zamiast jej usuwania.<br><br>a. Wybierz regułę.<br>b. Kliknij przycisk **Usuń**. |

3. Kliknij przycisk **Zapisz**.

## Typy reguł filtrowania zawartości

Możliwe jest utworzenie reguł filtrujących wiadomości e-mail zgodnie z określonymi warunkami bądź adresem e-mail nadawcy lub odbiorcy wiadomości. W regule można określić następujące warunki: pola nagłówka do skanowania, włączenie lub wyłączenie przeszukiwania treści wiadomości e-mail oraz wyszukiwane słowa kluczowe.

Możliwe jest utworzenie regul, które:

- **Filtrują wiadomości spełniające którykolwiek ze zdefiniowanych warunków**: za pomocą reguły tego typu można filtrować zawartość dowolnej wiadomości podczas skanowania. Aby uzyskać więcej informacji, zobacz *Dodawanie reguły filtrowania zawartości w przypadku zgodności dowolnego warunku na stronie 6-25*.
- **Filtrują wiadomości, które spełniają wszystkie zdefiniowane warunki**: za pomocą reguły tego typu można filtrować zawartość dowolnej wiadomości podczas skanowania. Aby uzyskać więcej informacji, zobacz *Dodawanie reguły filtrowania zawartości w przypadku zgodności wszystkich warunków na stronie 6-22*.

**Uwaga**

Ten typ reguły jest niedostępny w przypadku ręcznego i planowanego skanowania filtrowania zawartości.

- **Monitorują zawartość wiadomości z konkretnych kont e-mail**: reguła tego typu służy do monitorowania zawartości wiadomości z konkretnych kont e-mail. Reguły monitorowania są podobne do ogólnych reguł filtrowania zawartości poza tym, że filtrują zawartość wiadomości pochodzących wyłącznie z określonych kont e-mail. Aby uzyskać więcej informacji, zobacz *Dodawanie reguły monitorowania filtrowania zawartości na stronie 6-28*.

- **Tworzą wyjątki dla konkretnych kont e-mail**: reguła tego typu powoduje utworzenie wyjątku dla konkretnych kont e-mail. Gdy konkretne konto e-mail zostanie w ten sposób wyłączone, nie będzie ono filtrowane pod kątem naruszenia reguł zawartości. Aby uzyskać więcej informacji, zobacz *Tworzenie wyjątków do reguł filtrowania zawartości na stronie 6-31*.

Po utworzeniu reguły program Messaging Security Agent rozpocznie filtrowanie wszystkich przychodzących i wychodzących wiadomości według tej reguły. W przypadku wystąpienia naruszenia zawartości program Messaging Security Agent wykonuje operację dla wiadomości e-mail, która naruszyła reguły. Operacja wykonywana przez program Security Server jest zależna również od operacji zdefiniowanych w regule.

## Dodawanie reguły filtrowania zawartości w przypadku zgodności wszystkich warunków

Ten typ reguły jest niedostępny w przypadku ręcznego i planowanego skanowania filtrowania zawartości.

---

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij opcję **Filtrowanie zawartości**.

   Zostanie wyświetlony nowy ekran.

5. Kliknij przycisk **Dodaj**.

   Zostanie wyświetlony nowy ekran.

6. Wybierz opcję **Filtruj wiadomości, które spełniają wszystkie zdefiniowane warunki**.

7. Kliknij przycisk **Dalej**.

8. Wpisz nazwę reguły w polu **Nazwa reguły**.

9. Wybierz część wiadomości, która ma być filtrowana pod kątem niepożądanej zawartości. Program Messaging Security Agent może filtrować wiadomości e-mail według następujących pól:

   - Nagłówek (Od, Do i DW)
   - Temat
   - Wielkość treści wiadomości lub załącznika
   - Nazwa pliku załącznika

   **Uwaga**

   Program Messaging Security Agent filtruje zawartość nagłówka i tematu jedynie podczas skanowania w czasie rzeczywistym.

10. Kliknij przycisk **Dalej**.

11. Wybierz rodzaj działania, które program Messaging Security Agent ma podjąć po wykryciu niepożądanej treści. Program Messaging Security Agent może wykonywać następujące operacje (opisy zawiera część *Cele skanowania i operacje dotyczące programów Messaging Security Agent na stronie 7-20*):

    - Zastąp tekstem/plikiem

      **Uwaga**

      Nie można zastąpić tekstu w polach: Od, Do, DW i Temat.

    - Poddaj całą wiadomość kwarantannie

- Poddaj część wiadomości kwarantannie
- Usuń całą wiadomość
- Archiwizacja
- Pomiń całą wiadomość

12. Wybierz polecenie **Powiadom odbiorców**, aby program Messaging Security Agent powiadamiał odbiorców o wiadomościach e-mail z odfiltrowaną zawartością.

    Aby wysłać powiadomienia wyłącznie do wewnętrznych odbiorców poczty, wybierz opcję **Nie powiadamiaj odbiorców zewnętrznych**. Zdefiniuj adresy wewnętrzne, używając opcji **Operacje** > **Ustawienia powiadamiania** > **Definicja poczty wewnętrznej**.

13. Wybierz polecenie **Powiadom nadawców**, aby program Messaging Security Agent powiadamiał nadawców o wiadomościach e-mail z odfiltrowaną zawartością.

    Aby wysłać powiadomienia wyłącznie do wewnętrznych nadawców poczty, wybierz opcję **Nie powiadamiaj nadawców zewnętrznych**. Zdefiniuj adresy wewnętrzne, używając opcji **Operacje** > **Ustawienia powiadamiania** > **Definicja poczty wewnętrznej**.

14. W sekcji **Opcje zaawansowane** kliknij ikonę plus (+), aby rozwinąć podsekcję **Ustawienia archiwizacji**.

    a. W polu **Katalog kwarantanny** wpisz ścieżkę folderu, w którym funkcja Filtrowanie zawartości ma umieścić wiadomość e-mail poddaną kwarantannie, lub zaakceptuj wartość domyślną: `<folder instalacji programu Messaging Security Agent>\storage\quarantine`

    b. W polu **Katalog archiwum** wpisz ścieżkę folderu, w którym funkcja Filtrowanie zawartości ma umieścić wiadomość e-mail poddaną archiwizacji, lub zaakceptuj wartość domyślną: `<folder instalacji programu Messaging Security Agent>\storage\backup for content filter`

15. Kliknij ikonę z symbolem znaku plus (+), aby rozwinąć podsekcję **Ustawienia zastępowania**.

    a. W polu **Nazwa pliku zastępującego** wpisz nazwę pliku, którym funkcja Filtrowanie zawartości zastąpi wiadomość e-mail, gdy zostanie uaktywniona

reguła związana z działaniem „Zamień na tekst/plik”, lub zaakceptuj wartość domyślną.

b. W polu **Tekst zastępczy** wpisz lub wklej zawartość tekstu zastępczego funkcji Filtrowanie zawartości, który będzie używany, gdy wiadomość e-mail uaktywni regułę związaną z działaniem „Zamień na tekst/plik”, lub zaakceptuj tekst domyślny.

16. Kliknij przycisk **Zakończ**.

Kreator zostanie zamknięty i nastąpi powrót do ekranu Filtrowanie zawartości.

## Dodawanie reguły filtrowania zawartości w przypadku zgodności dowolnego warunku

- W przypadku skanowania w czasie rzeczywistym:

  **Urządzenia** > **{Messaging Security Agent}** > **Konfiguruj regułę** > **Filtrowanie zawartości**

- Skanowanie ręczne:

  **Skanowania** > **Ręczne** > **{rozwiń pozycję Messaging Security Agent}** > **Filtrowanie zawartości**

- Skanowanie zaplanowane:

  **Skanowania** > **Zaplanowane** > **{rozwiń pozycję Messaging Security Agent}** > **Filtrowanie zawartości**

**Procedura**

1. Kliknij przycisk **Dodaj**.

   Zostanie wyświetlony nowy ekran.

2. Wybierz opcję **Filtruj wiadomości, które spełniają którykolwiek ze zdefiniowanych warunków**.

3. Kliknij przycisk **Dalej**.

4. Wpisz nazwę reguły w polu **Nazwa reguły**.

5. Wybierz część wiadomości, która ma być filtrowana pod kątem niepożądanej zawartości. Program Messaging Security Agent może filtrować wiadomości e-mail według następujących pól:

   - Nagłówek (Od, Do i DW)
   - Temat
   - Treść
   - Załącznik

   **Uwaga**

   Program Messaging Security Agent filtruje zawartość nagłówka i tematu jedynie podczas skanowania w czasie rzeczywistym.

6. Kliknij przycisk **Dalej**.

7. Dodaj słowa kluczowe dla części docelowej, która ma być filtrowana w poszukiwaniu niepożądanej zawartości. Szczegółowe informacje na temat korzystania ze słów kluczowych zawiera część *Słowa kluczowe na stronie D-5*.

   a. W razie potrzeby wybierz, czy filtr zawartości ma uwzględniać wielkość liter.

   b. W razie potrzeby zaimportuj nowe pliki słów kluczowych z pliku `.txt`.

   c. Zdefiniuj listę synonimów.

8. Kliknij przycisk **Dalej**.

9. Wybierz rodzaj działania, które program Messaging Security Agent ma podjąć po wykryciu niepożądanej treści. Program Messaging Security Agent może wykonywać następujące operacje (opisy zawiera część *Cele skanowania i operacje dotyczące programów Messaging Security Agent na stronie 7-20*):

   - Zastąp tekstem/plikiem

   **Uwaga**

   Nie można zastąpić tekstu w polach: Od, Do, DW i Temat.

- Poddaj całą wiadomość kwarantannie
- Poddaj część wiadomości kwarantannie
- Usuń całą wiadomość
- Archiwizacja

10. Wybierz polecenie **Powiadom odbiorców**, aby program Messaging Security Agent powiadamiał odbiorców o wiadomościach e-mail z odfiltrowaną zawartością.

    Aby wysłać powiadomienia wyłącznie do wewnętrznych odbiorców poczty, wybierz opcję **Nie powiadamiaj odbiorców zewnętrznych**. Zdefiniuj adresy wewnętrzne, używając opcji **Operacje** > **Ustawienia powiadamiania** > **Definicja poczty wewnętrznej**.

11. Wybierz polecenie **Powiadom nadawców**, aby program Messaging Security Agent powiadamiał nadawców o wiadomościach e-mail z odfiltrowaną zawartością.

    Aby wysłać powiadomienia wyłącznie do wewnętrznych nadawców poczty, wybierz opcję **Nie powiadamiaj nadawców zewnętrznych**. Zdefiniuj adresy wewnętrzne, używając opcji **Operacje** > **Ustawienia powiadamiania** > **Definicja poczty wewnętrznej**.

12. W sekcji **Opcje zaawansowane** kliknij ikonę plus (+), aby rozwinąć podsekcję **Ustawienia archiwizacji**.

    a. W polu **Katalog kwarantanny** wpisz ścieżkę folderu, w którym funkcja Filtrowanie zawartości ma umieścić wiadomość e-mail poddaną kwarantannie, lub zaakceptuj wartość domyślną: `<folder instalacji programu Messaging Security Agent>\storage\quarantine`

    b. W polu **Katalog archiwum** wpisz ścieżkę folderu, w którym funkcja Filtrowanie zawartości ma umieścić wiadomość e-mail poddaną archiwizacji, lub zaakceptuj wartość domyślną: `<folder instalacji programu Messaging Security Agent>\storage\backup for content filter`

13. Kliknij ikonę z symbolem znaku plus (+), aby rozwinąć podsekcję **Ustawienia zastępowania**.

    a. W polu **Nazwa pliku zastępującego** wpisz nazwę pliku, którym funkcja Filtrowanie zawartości zastąpi wiadomość e-mail, gdy zostanie uaktywniona

reguła związana z działaniem „Zamień na tekst/plik”, lub zaakceptuj wartość domyślną.

b. W polu **Tekst zastępczy** wpisz lub wklej zawartość tekstu zastępczego funkcji Filtrowanie zawartości, który będzie używany, gdy wiadomość e-mail uaktywni regułę związaną z działaniem „Zamień na tekst/plik”, lub zaakceptuj tekst domyślny.

**14.** Kliknij przycisk **Zakończ**.

Kreator zostanie zamknięty i nastąpi powrót do ekranu Filtrowanie zawartości.

---

## Dodawanie reguły monitorowania filtrowania zawartości

- W przypadku skanowania w czasie rzeczywistym:

  **Urządzenia** > **{Messaging Security Agent}** > **Konfiguruj regułę** > **Filtrowanie zawartości**

- Skanowanie ręczne:

  **Skanowania** > **Ręczne** > **{rozwiń pozycję Messaging Security Agent}** > **Filtrowanie zawartości**

- Skanowanie zaplanowane:

  **Skanowania** > **Zaplanowane** > **{rozwiń pozycję Messaging Security Agent}** > **Filtrowanie zawartości**

---

**Procedura**

**1.** Kliknij przycisk **Dodaj**.

Zostanie wyświetlony nowy ekran.

**2.** Wybierz opcję **Monitoruj zawartość wiadomości z konkretnych kont e-mail**.

**3.** Kliknij przycisk **Dalej**.

**4.** Wpisz nazwę reguły w polu **Nazwa reguły**.

5. Ustaw konta e-mail do monitorowania.

6. Kliknij przycisk **Dalej**.

7. Wybierz część wiadomości, która ma być filtrowana pod kątem niepożądanej zawartości. Program Messaging Security Agent może filtrować wiadomości e-mail według następujących pól:

   - Temat
   - Treść
   - Załącznik

   **Uwaga**

   Program Messaging Security Agent filtruje te elementy wiadomości e-mail jedynie podczas skanowania w czasie rzeczywistym. Nie obsługuje filtrowania zawartości nagłówka i tematu podczas skanowania ręcznego i zaplanowanego.

8. Dodaj słowa kluczowe dla części docelowej, która ma być filtrowana w poszukiwaniu niepożądanej zawartości. Szczegółowe informacje na temat korzystania ze słów kluczowych zawiera część *Słowa kluczowe na stronie D-5*.

   a. W razie potrzeby wybierz, czy filtr zawartości ma uwzględniać wielkość liter.

   b. W razie potrzeby zaimportuj nowe pliki słów kluczowych z pliku `.txt`.

   c. Zdefiniuj listę synonimów.

9. Kliknij przycisk **Dalej**.

10. Wybierz rodzaj działania, które program Messaging Security Agent ma podjąć po wykryciu niepożądanej treści. Program Messaging Security Agent może wykonywać następujące operacje (opisy zawiera część *Cele skanowania i operacje dotyczące programów Messaging Security Agent na stronie 7-20*):

    - Zastąp tekstem/plikiem

      **Uwaga**

      Nie można zastąpić tekstu w polach: Od, Do, DW i Temat.

- Poddaj całą wiadomość kwarantannie
- Poddaj część wiadomości kwarantannie
- Usuń całą wiadomość
- Archiwizacja

**11.** Wybierz polecenie **Powiadom odbiorców**, aby program Messaging Security Agent powiadamiał odbiorców o wiadomościach e-mail z odfiltrowaną zawartością.

Aby wysłać powiadomienia wyłącznie do wewnętrznych odbiorców poczty, wybierz opcję **Nie powiadamiaj odbiorców zewnętrznych**. Zdefiniuj adresy wewnętrzne, używając opcji **Operacje** > **Ustawienia powiadamiania** > **Definicja poczty wewnętrznej**.

**12.** Wybierz polecenie **Powiadom nadawców**, aby program Messaging Security Agent powiadamiał nadawców o wiadomościach e-mail z odfiltrowaną zawartością.

Aby wysłać powiadomienia wyłącznie do wewnętrznych nadawców poczty, wybierz opcję **Nie powiadamiaj nadawców zewnętrznych**. Zdefiniuj adresy wewnętrzne, używając opcji **Operacje** > **Ustawienia powiadamiania** > **Definicja poczty wewnętrznej**.

**13.** W sekcji **Opcje zaawansowane** kliknij ikonę plus (+), aby rozwinąć podsekcję **Ustawienia archiwizacji**.

a. W polu **Katalog kwarantanny** wpisz ścieżkę folderu, w którym funkcja Filtrowanie zawartości ma umieścić wiadomość e-mail poddaną kwarantannie, lub zaakceptuj wartość domyślną: `<folder instalacji programu Messaging Security Agent>\storage\quarantine`

b. W polu **Katalog archiwum** wpisz ścieżkę folderu, w którym funkcja Filtrowanie zawartości ma umieścić wiadomość e-mail poddaną archiwizacji, lub zaakceptuj wartość domyślną: `<folder instalacji programu Messaging Security Agent>\storage\backup for content filter`

**14.** Kliknij ikonę z symbolem znaku plus (+), aby rozwinąć podsekcję **Ustawienia zastępowania**.

a. W polu **Nazwa pliku zastępującego** wpisz nazwę pliku, którym funkcja Filtrowanie zawartości zastąpi wiadomość e-mail, gdy zostanie uaktywniona

reguła związana z działaniem „Zamień na tekst/plik”, lub zaakceptuj wartość domyślną.

b. W polu **Tekst zastępczy** wpisz lub wklej zawartość tekstu zastępczego funkcji Filtrowanie zawartości, który będzie używany, gdy wiadomość e-mail uaktywni regułę związaną z działaniem „Zamień na tekst/plik”, lub zaakceptuj tekst domyślny.

15. Kliknij przycisk **Zakończ**.

    Kreator zostanie zamknięty i nastąpi powrót do ekranu Filtrowanie zawartości.

---

## Tworzenie wyjątków do reguł filtrowania zawartości

- W przypadku skanowania w czasie rzeczywistym:

  **Urządzenia** > **{Messaging Security Agent}** > **Konfiguruj regułę** > **Filtrowanie zawartości**

- Skanowanie ręczne:

  **Skanowania** > **Ręczne** > **{rozwiń pozycję Messaging Security Agent}** > **Filtrowanie zawartości**

- Skanowanie zaplanowane:

  **Skanowania** > **Zaplanowane** > **{rozwiń pozycję Messaging Security Agent}** > **Filtrowanie zawartości**

---

**Procedura**

1. Kliknij przycisk **Dodaj**.

   Zostanie wyświetlony nowy ekran.

2. Wybierz opcję **Utwórz wyjątki dla konkretnych kont e-mail**.

3. Kliknij przycisk **Dalej**.

4. Wpisz nazwę reguły.

5. W określonym miejscu wpisz konta e-mail, które chcesz wyłączyć z filtrowania zawartości, a następnie kliknij przycisk **Dodaj**.

   Konto zostanie dodane do listy wyłączonych kont e-mail. Program Messaging Security Agent nie stosuje reguł zawartości o niższym priorytecie niż ta reguła do kont e-mail znajdujących się na tej liście.

6. Po utworzeniu listy kont e-mail kliknij przycisk **Zakończ**.

   Kreator zostaje zamknięty i następuje powrót do ekranu **Filtrowanie zawartości**.

---

# Zapobieganie utracie danych

Funkcja zapobiegania utracie danych zapewnia ochronę przed utratą danych przesyłanych w wiadomościach e-mail. Przykłady chronionych tą funkcją danych to numery ubezpieczeń, numery telefonów, numery kont bankowych oraz inne poufne informacje biznesowe pasujące do ustalonego wzorca.

W tej wersji są obsługiwane następujące wersje programu Microsoft Exchange:

**TABELA 6-3. Obsługiwane wersje programu Microsoft Exchange**

| OBSŁUGIWANY | NIEOBSŁUGIWANY |
|---|---|
| 2007 x64 | 2003 x86/x64 |
| 2010 x64 | 2007 x86 |
| | 2010 x86 |

## Przygotowanie

Przed rozpoczęciem monitorowania poufnych danych pod kątem potencjalnej utraty należy ustalić następujące informacje:

- które dane muszą być chronione przed nieautoryzowanymi użytkownikami,
- gdzie znajdują się te dane,

- gdzie i w jaki sposób te dane są przesyłane,
- którzy użytkownicy mają autoryzację na dostęp do lub przesyłanie takich informacji.

Ten ważny audyt na ogół wymaga kontaktu z kilkoma oddziałami oraz pracownikami, którzy mają dobrą znajomość tematu poufnych informacji danej firmy. Przedstawione w dalszej części procedury zakładają zidentyfikowanie poufnych informacji oraz wdrożenie polityk bezpieczeństwa dotyczących postępowania z poufnymi informacjami biznesowymi.

Funkcja zapobiegania utracie danych składa się z trzech zasadniczych części:

- **reguły** (wyszukiwane wzorce),
- **domeny wykluczone** z filtrowania,
- **zatwierdzeni nadawcy** (konta e-mail wykluczone z filtrowania).

Aby uzyskać więcej informacji, zobacz *Zarządzanie regułami zapobiegania utracie danych na stronie 6-33*.

## Zarządzanie regułami zapobiegania utracie danych

Program Messaging Security Agent wyświetla wszystkie reguły zapobiegania utracie danych na ekranie **Zapobieganie utracie danych** (**Urządzenia** > **{Messaging Security Agent}** > **Konfiguruj regułę** > **Zapobieganie utracie danych**).

---

**Procedura**

1. Przejrzyj podsumowanie informacji na temat reguł, w tym:
    - **Reguła**: program Worry-Free Business Security jest wyposażony w reguły domyślne (patrz *Domyślne reguły zapobiegania utracie danych na stronie 6-41*). Są one domyślnie wyłączone. Reguły te można zmienić odpowiednio do wymagań albo usunąć. Jeśli żadna z reguł nie spełnia wymagań, dodaj własne reguły.

**Porada**

Przesuń wskaźnik myszy nad nazwę reguły, aby ją wyświetlić. Reguły wykorzystujące wyrażenia regularne są oznaczone ikoną lupy ( ).

- **Operacja**: program Messaging Security Agent wykonuje tę operację w momencie uaktywnienia reguły.
- **Priorytet**: program Messaging Security Agent stosuje poszczególne reguły zgodnie z kolejnością wyświetlaną na tej stronie.
- **Włączone**: ikona w kolorze zielonym oznacza regułę włączoną, a ikona w kolorze czerwonym — wyłączoną.

2. Wykonaj następujące czynności:

| ZADANIE | CZYNNOŚCI |
|---|---|
| Włączanie/ wyłączanie zapobiegania utracie danych | Zaznacz lub usuń zaznaczenie pola **Włącz zapobieganie utracie danych w czasie rzeczywistym** na górze ekranu. |
| Dodawanie reguły | Kliknij przycisk **Dodaj**.<br><br>Pojawi się nowy ekran, gdzie można wybrać typ dodawanej reguły. Szczegółowe informacje zawiera część *Dodawanie reguł zapobiegania utracie danych na stronie 6-42*. |
| Modyfikowanie reguły | Kliknij nazwę reguły.<br><br>Zostanie wyświetlony nowy ekran. Szczegółowe informacje o ustawieniach reguł, które można modyfikować, zawiera część *Dodawanie reguł zapobiegania utracie danych na stronie 6-42*. |

| ZADANIE | CZYNNOŚCI |
|---|---|
| Importowanie i eksportowanie reguł | Zaimportuj jedną lub więcej reguł z pliku tekstowego (lub wyeksportuj je do niego), jak pokazano poniżej. Można również edytować reguły bezpośrednio w takim pliku.<br><br>`[SMEX_SUB_CFG_CF_RULE43ca5aea-6e75-44c5-94c9-d0b35d2be599]`<br><br>`RuleName=Bubbly`<br><br>`UserExample=`<br><br>`Value=Bubbly`<br><br>`[SMEX_SUB_CFG_CF_RULE8b752cf2-aca9-4730-a4dd-8e174f9147b6]`<br><br>`RuleName=Master Card No.`<br><br>`UserExample=Value=.REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b` |
| | Aby wyeksportować reguły do pliku tekstowego, zaznacz co najmniej jedną regułę na liście i kliknij przycisk **Eksportuj**.<br><br>**Porada**<br>Można wybrać tylko reguły wyświetlane na jednym ekranie. Aby wybrać reguły aktualnie znajdujące się na różnych ekranach, należy zwiększyć wartość parametru „Wierszy na stronie” dostępnego u góry tabeli z listą reguł, aby wyświetlić wszystkie reguły, które mają zostać wyeksportowane. |

| ZADANIE | CZYNNOŚCI |
| --- | --- |
| | Aby zaimportować reguły:<br>a. Utwórz plik tekstowy w formacie pokazanym powyżej. Możesz też kliknąć przycisk **Pobierz więcej reguł domyślnych** znajdujący się pod tabelą i zapisać reguły.<br>b. Kliknij przycisk **Importuj**.<br>Zostanie otwarte nowe okno.<br>c. Kliknij przycisk **Przeglądaj**, aby odnaleźć importowany plik, a następnie kliknij przycisk **Importuj**.<br>Funkcja zapobiegania utracie danych zaimportuje reguły z pliku i dołączy je na końcu listy bieżących reguł.<br>**Porada**<br>Jeżeli dostępnych jest już więcej niż 10 reguł, zaimportowane reguły nie będą widoczne na pierwszej stronie. Aby wyświetlić ostatnią stronę listy, należy użyć ikon przeglądania stron u góry lub u dołu listy reguł. Nowo zaimportowane reguły powinny znajdować się na ostatniej stronie. |

| ZADANIE | CZYNNOŚCI |
|---|---|
| Zmiana kolejności reguł | Program Messaging Security Agent stosuje reguły zapobiegania utracie danych do wiadomości e-mail w kolejności widocznej na ekranie **Zapobieganie utracie danych**. Istnieje możliwość określenia kolejności stosowania reguł. Agent filtruje wszystkie wiadomości e-mail zgodnie z każdą z reguł, dopóki naruszenie zawartości nie uruchomi operacji uniemożliwiającej dalsze skanowanie (takiej jak usunięcie lub poddanie kwarantannie). Kolejność tych reguł można zmienić w celu optymalizacji zapobiegania utracie danych.<br><br>a. Zaznacz pole wyboru odpowiadające regule, której kolejność chcesz zmienić.<br><br>b. Kliknij opcję **Zmień kolejność**.<br><br>Wokół liczby wskazującej kolejność reguły zostanie wyświetlone pole.<br><br>c. Usuń istniejący numer kolejności w polu kolumny **Priorytet** i wpisz nowy numer.<br><br>**Uwaga**<br>Należy pamiętać, że nie można wprowadzić numeru większego od łącznej liczby reguł na liście. W razie wprowadzenia numeru większego od łącznej liczby reguł program Worry-Free Business Security zignoruje taki wpis i nie zmieni kolejności reguł.<br><br>d. Kliknij przycisk **Zapisz zmienioną kolejność**.<br><br>Reguła zostanie przesunięta na wprowadzony poziom priorytetu, a numery wszystkich pozostałych reguł zostaną odpowiednio zmienione.<br><br>Na przykład wybranie reguły o numerze 5 i zmiana tego numeru na 3 spowoduje, że reguły o numerach 1 i 2 pozostaną bez zmian, natomiast numery pozostałych reguł, począwszy od numeru 3, zostaną zwiększone o 1. |
| Włączanie/ wyłączanie reguł | Kliknij ikonę w kolumnie Włączone. |

| ZADANIE | CZYNNOŚCI |
| --- | --- |
| Usuwanie reguł | Po usunięciu reguły program Messaging Security Agent aktualizuje kolejność innych reguł, aby uwzględnić zmianę.<br><br>**Uwaga**<br>Usunięcie reguły jest nieodwracalne, dlatego należy rozważyć możliwość wyłączenia reguły zamiast jej usuwania.<br><br>a. Wybierz regułę.<br>b. Kliknij przycisk **Usuń**. |

| ZADANIE | CZYNNOŚCI |
|---|---|
| Wykluczanie określonych kont domeny | W firmie codziennie wymieniane są poufne informacje biznesowe. Ponadto obciążenie serwerów Security Servers byłoby bardzo duże w przypadku wykorzystania funkcji zapobiegania utracie danych do filtrowania wszystkich wiadomości wewnętrznych. Konieczne jest więc skonfigurowanie jednej lub kilku domen domyślnych, reprezentujących ruch sieciowy związanych z korespondencją wewnętrzną, tak aby funkcja Zapobieganie utracie danych nie filtrowała wiadomości przesyłanych między kontami e-mail w domenie firmy.<br><br>Na tej liście znajdują się wszystkie wewnętrzne (przesyłane w domenie firmowej) wiadomości e-mail, które mają być pomijane przez reguły funkcji Zapobieganie utracie danych (DLP). Wymagana jest przynajmniej jedna taka domena. Jeśli jest używana więcej niż jedna domena, należy uzupełnić tę listę.<br><br>Na przykład: `*@przyklad.com`<br><br>a. Kliknij ikonę z symbolem znaku plus (+), aby rozwinąć sekcję **Konta domeny wykluczone z zapobiegania utracie danych**.<br><br>b. Umieść kursor w obrębie pola **Dodaj** i wprowadź domenę w następującym formacie: `*@przyklad.com`<br><br>c. Kliknij przycisk **Dodaj**.<br><br>Wprowadzona domena pojawi się na liście wyświetlanej pod polem **Dodaj**.<br><br>d. Kliknij przycisk **Zapisz**, aby ukończyć proces.<br><br>**OSTRZEŻENIE!**<br>Funkcja zapobiegania utracie danych nie doda domeny do momentu kliknięcia przycisku **Zapisz**. Kliknięcie przycisku **Dodaj** bez kliknięcia przycisku **Zapisz** nie spowoduje dodania domeny. |

| ZADANIE | CZYNNOŚCI |
|---|---|
| Dodawanie kont e-mail do listy Zatwierdzeni nadawcy | Wiadomości pocztowe od zatwierdzonych nadawców podróżują poza obrębem sieci użytkownika bez filtrowania zapewnianego funkcją Zapobieganie utracie danych. Funkcja Zapobieganie utracie danych będzie ignorować zawartość wszystkich wiadomości wysyłanych z kont e-mail znajdujących się na liście zatwierdzonych nadawców.<br>a. Kliknij ikonę z symbolem znaku plus (+), aby rozwinąć sekcję **Zatwierdzeni nadawcy**.<br>b. Umieść kursor w obrębie pola **Dodaj** i wprowadź pełny adres e-mail w następującym formacie: `przykład@przykład.pl`<br>c. Kliknij przycisk **Dodaj**.<br>Wprowadzony adres pojawi się na liście wyświetlanej pod polem **Dodaj**.<br>d. Kliknij przycisk **Zapisz**, aby ukończyć proces.<br>**Uwaga**<br>Funkcja zapobiegania utracie danych nie doda adresu do momentu kliknięcia przycisku **Zapisz**. Kliknięcie przycisku **Dodaj** bez kliknięcia przycisku **Zapisz** nie spowoduje dodania adresu. |

| ZADANIE | CZYNNOŚCI |
|---|---|
| Importowanie kont e-mail do listy Zatwierdzeni nadawcy | Listę adresów można zaimportować z pliku tekstowego o formacie jednego adresu e-mail na wiersz, jak w przykładzie:<br>`admin@przykład.com`<br>`dyrektor@przykład.com`<br>`prezes@przykład.com`<br>a. Kliknij ikonę z symbolem znaku plus (+), aby rozwinąć sekcję **Zatwierdzeni nadawcy**.<br>b. Kliknij przycisk **Importuj**.<br>Zostanie otwarte nowe okno.<br>c. Kliknij przycisk **Przeglądaj**, aby odnaleźć importowany plik tekstowy, a następnie kliknij przycisk **Importuj**.<br>Funkcja zapobiegania utracie danych zaimportuje reguły z pliku i dołączy je na końcu listy. |

3. Kliknij przycisk **Zapisz**.

## Domyślne reguły zapobiegania utracie danych

Z funkcją Zapobieganie utracie danych związanych jest kilka reguł domyślnych opisanych w poniższej tabeli.

**TABELA 6-4. Domyślne reguły zapobiegania utracie danych**

| NAZWA REGUŁY | PRZYKŁAD | WYRAŻENIE REGULARNE |
|---|---|---|
| Numer rachunku karty Visa | 4111-1111-1111-1111 | .REG. \b4\d{3}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b |
| Numer rachunku karty MasterCard | 5111-1111-1111-1111 | .REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b |

| Nazwa reguły | Przykład | Wyrażenie regularne |
|---|---|---|
| Numer rachunku karty American Express | 3111-111111-11111 | .REG. \b3[4,7]\d{2}\-?\x20?\d{6}\-?\x20?\d{5}\b |
| Numer rachunku karty Diners Club/Carte Blanche | 3111-111111-1111 | .REG. [^\d-]((36\d{2}\|38\d{2}\|30[0-5]\d)-?\d{6}-?\d{4})[^\d-] |
| IBAN | BE68 5390 0754 7034, FR14 2004 1010 0505 0001 3M02 606, DK50 0040 0440 1162 43 | .REG. [^\w](([A-Z]{2}\d{2}[-\|\s]?)([A-Za-z0-9]{11,27}\|([A-Za-z0-9]{4}[-\|\s]){3,6}[A-Za-z0-9]{0,3}\|([A-Za-z0-9]{4}[-\|\s]){2}[A-Za-z0-9]{3,4}))[^\w] |
| Swift BIC | BANK US 99 | .REG. [^\w-]([A-Z]{6}[A-Z0-9]{2}([A-Z0-9]{3})?)[^\w-] |
| Data ISO | 2004/01/23, 04/01/23, 2004-01-23, 04-01-23 | .REG. [^\d\/-]([1-2]\d{3}[-\/][0-1]?\d[-\/][0-3]?\d\|\d{2}[-\/][0-1]?\d[-\/][0-3]?\d)[^\d\/-] |

**Uwaga**

Plik zip zawierający więcej reguł zapobiegania utracie danych można pobrać z konsoli internetowej. Przejdź do obszaru **Ustawienia zabezpieczeń** > **{Messaging Security Agent}** > **Konfiguruj ustawienia** > **Zapobieganie utracie danych** i kliknij polecenie **Pobierz więcej reguł domyślnych**.

## Dodawanie reguł zapobiegania utracie danych

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.

4. Kliknij pozycję **Zapobieganie utracie danych**.

   Zostanie wyświetlony nowy ekran.

5. Kliknij przycisk **Dodaj**.

   Zostanie wyświetlony nowy ekran.

6. Zaznacz część wiadomości, którą chcesz poddać ocenie. Program Messaging Security Agent może filtrować wiadomości e-mail według następujących pól:

   - Nagłówek (Od, Do i DW)
   - Temat
   - Treść
   - Załącznik

7. Dodaj regułę.

   **Aby dodać regułę bazującą na słowie kluczowym:**

   a. Wybierz pozycję **Słowo kluczowe**.

   b. W wyświetlonym polu wpisz słowo kluczowe. Słowo kluczowe musi zawierać od 1 do 64 znaków alfanumerycznych.

   c. Kliknij przycisk **Dalej**.

   **Aby dodać regułę bazującą na wyrażeniach generowanych automatycznie:**

   a. Wskazówki dotyczące definiowania wyrażeń regularnych zawiera część *Wyrażenia regularne na stronie D-11*.

   b. Wybierz pozycję **Wyrażenie regularne (generowane automatycznie)**.

   c. W dostępnym polu wprowadź **nazwę reguły**. Jest to pole wymagane.

   d. W polu **Przykład** wpisz lub wklej przykładowy rodzaj ciągu (o długości maksymalnie 40 znaków), do którego ma pasować dane wyrażenie regularne. Znaki alfanumeryczne pojawią się jako wielkie litery w przyciemnionym obszarze z rzędami pól wyboru pod polem **Przykład**.

e. Jeżeli wyrażenie zawiera jakiekolwiek stałe, należy je wybrać, klikając pola, gdzie wyświetlane są odpowiednie znaki.

Po kliknięciu każdego pola jego obramowanie staje się czerwone, wskazując, że jest to stała, a narzędzie do generowania automatycznego modyfikuje wyrażenie regularne widoczne poniżej wyszarzonego obszaru.

**Uwaga**

Znaki inne niż alfanumeryczne (takie jak spacje, średniki oraz inne znaki interpunkcyjne) są automatycznie uznawane za stałe i nie można ich konwertować na zmienne.

f. Aby sprawdzić, czy wygenerowane wyrażenie regularne pasuje do zamierzonej sygnatury, wybierz opcję **Podaj inny przykład, aby sprawdzić regułę (opcjonalnie)**.

Pod tą opcją pojawi się pole testu.

g. Wpisz inny przykład wprowadzonej sygnatury.

Jeżeli to wyrażenie ma na przykład dopasować serię numerów kont do sygnatury „01-EX????? 20??", wpisz inny pasujący przykład, taki jak „01-Extreme 2010", a następnie kliknij przycisk **Testuj**.

Narzędzie sprawdzi nowy przykład na istniejącym wyrażeniu regularnym i jeśli nowy przykład będzie dopasowany, obok pola zostanie wyświetlony zielony znacznik wyboru. Jeśli wyrażenie regularne nie będzie pasować do nowego przykładu, obok pola zostanie wyświetlona czerwona ikona X.

**OSTRZEŻENIE!**

W wyrażeniach regularnych tworzonych za pomocą tego narzędzia wielkość liter nie jest rozpoznawana. Te wyrażenia umożliwiają tylko wyszukiwanie dokładnie takiej samej liczby znaków, jak w przykładzie; nie umożliwiają wyszukiwania „jednego lub kilku" odpowiedników danego znaku.

h. Kliknij przycisk **Dalej**.

**Aby dodać regułę bazującą na wyrażeniach definiowanych przez użytkownika:**

**OSTRZEŻENIE!**

Wyrażenia regularne to bardzo skuteczne narzędzie służące do dopasowywania łańcuchów znaków. Takie wyrażenia mogą być używane wyłącznie przez osoby o doskonałej znajomości składni wyrażeń regularnych. Błędnie napisane wyrażenia regularne mogą znacznie obniżyć wydajność. Firma Trend Micro zaleca rozpoczęcie pracy od prostych wyrażeń regularnych. Tworząc nowe reguły, używaj operacji archiwizacji i obserwuj, jak funkcja Zapobieganie utracie danych zarządza wiadomościami przy użyciu tych reguł. Gdy okaże się, że reguła nie wprowadza żadnych nieoczekiwanych zmian, można zmienić operację.

a. Wskazówki dotyczące definiowania wyrażeń regularnych zawiera część *Wyrażenia regularne na stronie D-11*.

b. Wybierz opcję **Wyrażenie regularne (definiowane przez użytkownika)**.

   Pojawią się pola **Nazwa reguły** i **Wyrażenie regularne**.

c. W dostępnym polu wprowadź **nazwę reguły**. Jest to pole wymagane.

d. W polu **Wyrażenie regularne** wpisz wyrażenie regularne rozpoczynające się od prefiksu „`.REG.`” (maksymalnie 255 znaków łącznie z prefiksem).

   **OSTRZEŻENIE!**

   Przy wklejaniu takiego wyrażenia do tego pola należy zachować szczególną ostrożność. Jeżeli w zawartości schowka znajdą się dodatkowe znaki (na przykład znaczniki HTML albo znak LF systemu operacyjnego), wklejone wyrażenie będzie nieścisłe. Z tego powodu firma Trend Micro zaleca ręczne wprowadzanie tych wyrażeń.

e. Aby sprawdzić, czy wyrażenie regularne pasuje do pożądanej sygnatury, należy wybrać opcję **Podaj inny przykład, aby sprawdzić regułę (opcjonalnie)**.

   Pod tą opcją pojawi się pole testu.

f. Wpisz inny przykład wprowadzonej sygnatury (maksymalnie 40 znaków).

   Jeżeli to wyrażenie ma na przykład dopasować serię numerów kont do sygnatury „ACC-????? 20??” wpisz inny pasujący przykład, taki jak „Acc-65432 2012”, a następnie kliknij przycisk **Testuj**.

Narzędzie sprawdzi nowy przykład na istniejącym wyrażeniu regularnym i jeśli nowy przykład będzie dopasowany, obok pola zostanie wyświetlony zielony znacznik wyboru. Jeśli wyrażenie regularne nie będzie pasować do nowego przykładu, obok pola zostanie wyświetlona czerwona ikona X.

g. Kliknij przycisk **Dalej**.

8. Wybierz operację podejmowaną przez program Messaging Security Agent w razie uaktywnienia reguły (opisy zawiera część *Cele skanowania i operacje dotyczące programów Messaging Security Agent na stronie 7-20*):

   - Zastąp tekstem/plikiem

     **Uwaga**

     Nie można zastąpić tekstu w polach: Od, Do, DW i Temat.

   - Poddaj całą wiadomość kwarantannie
   - Poddaj część wiadomości kwarantannie
   - Usuń całą wiadomość
   - Archiwizacja
   - Pomiń całą wiadomość

9. Wybierz polecenie **Powiadom odbiorców**, aby program Messaging Security Agent powiadamiał odbiorców, gdy w odniesieniu do danej wiadomości e-mail wykonana zostanie operacja związana z zapobieganiem utracie danych.

   Użytkownik może z różnych powodów chcieć uniknąć powiadamiania zewnętrznych odbiorców poczty o zablokowaniu wiadomości zawierającej poufne informacje. Aby wysłać powiadomienia wyłącznie do wewnętrznych odbiorców poczty, wybierz opcję **Nie powiadamiaj odbiorców zewnętrznych**. Zdefiniuj adresy wewnętrzne, używając opcji **Operacje** > **Ustawienia powiadamiania** > **Definicja poczty wewnętrznej**.

10. Wybierz polecenie **Powiadom nadawców**, aby program Messaging Security Agent powiadamiał wskazanych nadawców, gdy w odniesieniu do danej wiadomości e-mail wykonana zostanie operacja związana z zapobieganiem utracie danych.

Użytkownik może z różnych powodów chcieć uniknąć powiadamiania zewnętrznych nadawców poczty o zablokowaniu wiadomości zawierającej poufne informacje. Aby wysłać powiadomienia wyłącznie do wewnętrznych nadawców poczty, wybierz opcję **Nie powiadamiaj nadawców zewnętrznych**. Zdefiniuj adresy wewnętrzne, używając opcji **Operacje** > **Ustawienia powiadamiania** > **Definicja poczty wewnętrznej**.

**11.** W sekcji **Opcje zaawansowane** kliknij ikonę plus (+), aby rozwinąć podsekcję **Ustawienia archiwizacji**.

a. W polu **Katalog kwarantanny** wpisz ścieżkę folderu, w którym funkcja Zapobieganie utracie danych ma umieścić wiadomość e-mail poddaną kwarantannie, lub zaakceptuj wartość domyślną: `<folder instalacji programu Messaging Security Agent>\storage\quarantine`

b. W polu **Katalog archiwum** wpisz ścieżkę folderu, w którym funkcja Zapobieganie utracie danych ma umieścić wiadomość e-mail poddaną kwarantannie, lub zaakceptuj wartość domyślną: `<folder instalacji programu Messaging Security Agent>\storage\backup for content filter`

**12.** Kliknij ikonę z symbolem znaku plus (+), aby rozwinąć podsekcję **Ustawienia zastępowania**.

a. W polu **Nazwa pliku zastępującego** wpisz nazwę pliku, którym funkcja Zapobieganie utracie danych zastąpi wiadomość e-mail, gdy zostanie uaktywniona reguła związana z działaniem „Zamień na tekst/plik", lub zaakceptuj wartość domyślną.

b. W polu **Tekst zastępczy** wpisz lub wklej zawartość tekstu zastępczego funkcji Zapobieganie utracie danych, który będzie używany, gdy wiadomość e-mail uaktywni regułę związaną z działaniem „Zamień na tekst/plik", lub zaakceptuj tekst domyślny.

**13.** Kliknij przycisk **Zakończ**.

Kreator zostanie zamknięty i nastąpi powrót do ekranu Zapobieganie utracie danych.

# Blokowanie załączników

Funkcja blokowania załączników zapobiega dostarczaniu załączników w wiadomościach e-mail do magazynu informacji serwera Microsoft Exchange. Program Messaging Security Agent można skonfigurować tak, aby blokował załączniki według ich typu lub nazwy, a następnie zastąpił, poddał kwarantannie lub usunął wszystkie wiadomości, które zawierają załączniki spełniające określone kryteria.

Blokowanie może mieć miejsce podczas skanowania w czasie rzeczywistym, ręcznego lub zaplanowanego, ale operacje usuwania i poddawania kwarantannie nie są dostępne podczas skanowania ręcznego i zaplanowanego.

Rozszerzenie pliku załącznika pozwala zidentyfikować typ pliku, na przykład `.txt`, `.exe` lub `.dll`. Jednak program Messaging Security Agent sprawdza nagłówek pliku zamiast jego nazwy, aby uzyskać pewność co do rzeczywistego typu pliku. Wiele wirusów/złośliwych programów jest ściśle powiązana z określonymi typami plików. Konfigurując program Messaging Security Agent tak, aby blokował pliki określonego typu, można zmniejszyć zagrożenie bezpieczeństwa serwerów Microsoft Exchange ze strony tego typu plików. Określone ataki są także często powiązane z określoną nazwą pliku.

**Porada**

Stosowanie blokowania to skuteczna metoda kontrolowania epidemii wirusów. Można tymczasowo poddać kwarantannie wszystkie typy plików o wysokim ryzyku albo o określonej nazwie, związanej ze znanym wirusem/złośliwym oprogramowaniem. W dogodnym momencie można sprawdzić folder kwarantanny i podjąć działania dotyczące zarażonych plików.

## Konfigurowanie blokowania załączników

Konfigurowanie opcji blokowania załączników dla serwerów Microsoft Exchange obejmuje ustawianie reguł blokowania wiadomości z określonymi załącznikami.

- W przypadku skanowania w czasie rzeczywistym:

  **Urządzenia** > **{Messaging Security Agent}** > **Konfiguruj regułę** > **Blokowanie załączników.**

- Skanowanie ręczne:

  **Skanowania** > **Ręczne** > **{rozwiń pozycję Messaging Security Agent}** > **Blokowanie załączników**

- Skanowanie zaplanowane:

  **Skanowania** > **Zaplanowane** > **{rozwiń pozycję Messaging Security Agent}** > **Blokowanie załączników**

---

**Procedura**

1. Zmień odpowiednio następujące opcje na karcie **Miejsce docelowe**:

   - **Wszystkie załączniki**: Agent może blokować wszystkie wiadomości e-mail, które zawierają załączniki. Ten typ skanowania wymaga jednak znacznego przetwarzania. Należy uściślić ten typ skanowania, wybierając typy lub nazwy załączników do wykluczenia.

     - **Typy załączników do wykluczenia**
     - **Nazwy załączników do wykluczenia**

   - **Określone załączniki**: wybranie tego typu skanowania sprawia, że agent skanuje tylko te wiadomości e-mail, które zawierają załączniki określone przez użytkownika. Ten typ skanowania jest bardzo zawężony i sprawdza się idealnie przy wykrywaniu wiadomości e-mail z załącznikami, które prawdopodobnie zawierają zagrożenia. To skanowanie działa bardzo szybko, jeśli podana zostanie względnie mała liczba nazw lub typów załączników.

     - **Typy załączników**: Agent sprawdza nagłówek pliku zamiast jego nazwy, aby uzyskać pewność co do rzeczywistego typu pliku.
     - **Nazwy załączników**: domyślnie agent sprawdza nagłówek pliku zamiast jego nazwy, aby uzyskać pewność co do rzeczywistego typu pliku. Jeśli funkcja blokowania załączników zostanie skonfigurowana do skanowania określonych nazw, agent będzie wykrywał typy załączników według ich nazw.

   - **Blokuj typy lub nazwy załączników w plikach z rozszerzeniem ZIP**

2. Wybierz kartę **Operacja**, aby ustawić operacje, które będą wykonywane przez program Messaging Security Agent po wykryciu załączników. Program Messaging Security Agent może wykonywać następujące operacje (opisy zawiera część *Cele skanowania i operacje dotyczące programów Messaging Security Agent na stronie 7-20*):

   - Zastąp tekstem/plikiem
   - Poddaj całą wiadomość kwarantannie
   - Poddaj część wiadomości kwarantannie
   - Usuń całą wiadomość

3. Wybierz polecenie **Powiadom odbiorców**, aby program Messaging Security Agent powiadamiał odbiorców o wiadomościach e-mail z załącznikami.

   Aby wysłać powiadomienia wyłącznie do wewnętrznych odbiorców poczty, wybierz opcję **Nie powiadamiaj odbiorców zewnętrznych**. Zdefiniuj adresy wewnętrzne, używając opcji **Operacje** > **Ustawienia powiadamiania** > **Definicja poczty wewnętrznej**.

4. Wybierz polecenie **Powiadom nadawców**, aby program Messaging Security Agent powiadamiał nadawców o wiadomościach e-mail z załącznikami.

   Aby wysłać powiadomienia wyłącznie do wewnętrznych nadawców poczty, wybierz opcję **Nie powiadamiaj nadawców zewnętrznych**. Zdefiniuj adresy wewnętrzne, używając opcji **Operacje** > **Ustawienia powiadamiania** > **Definicja poczty wewnętrznej**.

5. Kliknij ikonę z symbolem znaku plus (+), aby rozwinąć podsekcję **Ustawienia zastępowania**.

   a. W polu **Nazwa pliku zastępującego** wpisz nazwę pliku, którym funkcja Blokowanie załączników zastąpi wiadomość e-mail, gdy zostanie uaktywniona reguła związana z działaniem „Zamień na tekst/plik", lub zaakceptuj wartość domyślną.

   b. W polu **Tekst zastępczy** wpisz lub wklej zawartość tekstu zastępczego funkcji Blokowanie załączników, który będzie używany, gdy wiadomość e-mail uaktywni regułę związaną z działaniem „Zamień na tekst/plik", lub zaakceptuj tekst domyślny.

6. Kliknij przycisk **Zapisz**.

# Usługa Web Reputation

Usługa Web Reputation pomaga uniemożliwiać dostęp do adresów URL w sieci lub adresów zawartych w wiadomościach e-mail stanowiących zagrożenie bezpieczeństwa. Usługa Web Reputation sprawdza reputację adresu URL, korzystając z serwerów Web Reputation firmy Trend Micro, a następnie dopasowuje tę reputację do określonej reguły usługi Web Reputation, która jest egzekwowana na kliencie. W zależności od stosowanej reguły:

- Program Security Agent zablokuje dostęp do witryny lub zezwoli na dostęp do niej.
- Program Messaging Security Agent (tylko w wersji Advanced) podda kwarantannie, usunie lub dołączy znacznik do wiadomości e-mail zawierającej złośliwe adresy URL albo zezwoli na wysłanie wiadomości, jeśli adresy URL są bezpieczne.

Usługa Web Reputation dostarcza zarówno powiadomienia e-mail dla administratora, jak i powiadomienia online dla użytkownika dotyczące wykrytych zagrożeń.

W zależności od lokalizacji (W biurze/Poza biurem) klienta, należy skonfigurować odpowiedni poziom zabezpieczeń w programach Security Agent.

Jeśli usługa Web Reputation blokuje adres URL, który wydaje się bezpieczny, można dodać ten adres do listy dozwolonych adresów URL.

**Porada**

W celu zmniejszenia natężenia ruchu sieciowego firma Trend Micro zaleca dodanie wewnętrznych firmowych witryn internetowych do listy dozwolonych adresów URL usługi Web Reputation.

## Ocena punktowa reputacji

„Ocena punktowa reputacji" adresu URL określa, czy stanowi on zagrożenie internetowe czy nie. Firma Trend Micro wyznacza ocenę przy użyciu własnych mierników.

Firma Trend Micro uznaje adres URL za zagrożenie internetowe, jeśli jego wynik mieści się w określonym zakresie, oraz za bezpieczny, jeśli wynik wykracza poza ten zakres.

W programie Security Agent stosowane są trzy poziomy zabezpieczeń, które określają, czy będzie on zezwalać na dostęp do adresu URL czy go blokować.

- **Wysoki**: blokuje strony:
  - **Niebezpieczne**: zweryfikowano jako fałszywe lub znane źródła zagrożeń.
  - **Bardzo podejrzane**: potencjalnie fałszywe lub prawdopodobne źródła zagrożeń
  - **Podejrzane**: strony powiązane ze spamem lub mogące stanowić zagrożenie.
  - **Nieprzetestowane**: Firma Trend Micro aktywnie testuje strony internetowe pod kątem bezpieczeństwa, mimo to podczas odwiedzania nowych lub mniej popularnych witryn użytkownicy mogą natknąć się na strony nieprzetestowane. Zablokowanie dostępu do stron nieprzetestowanych może podnieść poziom bezpieczeństwa, ale także uniemożliwić dostęp do bezpiecznych stron.
- **Średni**: blokuje strony:
  - **Niebezpieczne**: zweryfikowano jako fałszywe lub znane źródła zagrożeń.
  - **Bardzo podejrzane**: potencjalnie fałszywe lub prawdopodobne źródła zagrożeń
- **Niski**: blokuje strony:
  - **Niebezpieczne**: zweryfikowano jako fałszywe lub znane źródła zagrożeń.

## Konfigurowanie usługi Web Reputation w programach Messaging Security Agent

**Procedura**

1. Przejdź do menu **Urządzenia**.

2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij pozycję **Usługa Web Reputation**:

   Zostanie wyświetlony nowy ekran.
5. Zmień odpowiednio następujące ustawienia:
   - **Włącz usługę Web Reputation**
   - Poziom zabezpieczeń: **Wysoka**, **Średnia**, lub **Niska**
   - Dozwolone adresy URL
     - **Adresy URL, które mają być dozwolone**: Poszczególne adresy URL oddzielaj średnikiem (;). Kliknij przycisk **Dodaj**.

       **Uwaga**

       Dodanie adresu URL obejmuje wszystkie jego subdomeny.

       Symbole wieloznaczne należy stosować ostrożnie, ponieważ za ich pomocą można zatwierdzić duże zestawy adresów URL.
     - **Lista dozwolonych adresów URL**: adresy URL na tej liście nie będą blokowane.
6. Kliknij kartę **Operacja** i wybierz operację, którą program Messaging Security Agent ma wykonać w razie uaktywnienia reguły reputacji (opisy zawiera część *Cele skanowania i operacje dotyczące programów Messaging Security Agent na stronie 7-20*):
   - Zastąp tekstem/plikiem

     **Uwaga**

     Nie można zastąpić tekstu w polach: Od, Do, DW i Temat.
   - Poddaj wiadomość kwarantannie w folderze wiadomości typu spam użytkownika

- Usuń całą wiadomość
- Oznacz i dostarcz

7. Wybierz opcję **Wykonaj operację w przypadku adresów URL, które nie zostały ocenione przez firmę Trend Micro**, aby niesklasyfikowane adresy URL traktować jako podejrzane. Operacja określona w poprzednim kroku będzie też wykonywana w odniesieniu do wiadomości e-mail zawierających niesklasyfikowane adresy URL.

8. Wybierz polecenie **Powiadom odbiorców**, aby program Messaging Security Agent powiadamiał odbiorców, gdy w odniesieniu do danej wiadomości e-mail wykonana zostanie operacja usługi Web Reputation związana z zapobieganiem utracie danych.

   Z różnych powodów można chcieć uniknąć powiadamiania zewnętrznych odbiorców poczty o zablokowaniu wiadomości zawierającej złośliwe adresy URL. Aby wysłać powiadomienia wyłącznie do wewnętrznych odbiorców poczty, wybierz opcję **Nie powiadamiaj odbiorców zewnętrznych**. Zdefiniuj adresy wewnętrzne, używając opcji **Operacje** > **Ustawienia powiadamiania** > **Definicja poczty wewnętrznej**.

9. Wybierz polecenie **Powiadom nadawców**, aby program Messaging Security Agent powiadamiał wskazanych nadawców, gdy w odniesieniu do danej wiadomości e-mail wykonana zostanie operacja usługi Web Reputation, związana z zapobieganiem utracie danych.

   Z różnych powodów można chcieć uniknąć powiadamiania zewnętrznych nadawców poczty o zablokowaniu wiadomości zawierającej złośliwe adresy URL. Aby wysłać powiadomienia wyłącznie do wewnętrznych nadawców poczty, wybierz opcję **Nie powiadamiaj nadawców zewnętrznych**. Zdefiniuj adresy wewnętrzne, używając opcji **Operacje** > **Ustawienia powiadamiania** > **Definicja poczty wewnętrznej**.

10. Kliknij przycisk **Zapisz**.

# Mobile Security

Ustawienia programu Mobile Security uniemożliwiają nieuprawnionym urządzeniom uzyskiwanie dostępu i pobieranie informacji z serwera Microsoft Exchange Server.

Administratorzy określają, które urządzenia mogą uzyskać dostęp do serwera Microsoft Exchange Server, a następnie ustalają, czy użytkownicy tych urządzeń mogą pobierać lub aktualizować pocztę e-mail, kalendarz, kontakty albo zadania.

Administratorzy mogą także zastosować do urządzeń reguły zabezpieczeń. Umożliwiają one kontrolowanie długości i złożoności haseł, a także określenie, czy urządzenia powinny zostać zablokowane po okresie nieaktywności, czy wymagane jest stosowanie szyfrowania w urządzeniach oraz czy dane urządzenia powinny zostać wymazane po serii nieudanych prób logowania.

## Mobile Security — pomoc techniczna

**TABELA 6-5. Urządzenia mobilne — pomoc techniczna**

| SYSTEM OPERACYJNY | WERSJA PROGRAMU IIS | REGUŁY OCHRONY DANYCH NA URZĄDZENIU | | KONTROLA DOSTĘPU | | |
|---|---|---|---|---|---|---|
| | | EXCHANGE 2007 (LUB NOWSZY), WERSJA 64-BITOWA | EXCHANGE 2003, WERSJA 32-BITOWA | EXCHANGE 2010 (LUB NOWSZY), WERSJA 64-BITOWA | EXCHANGE 2007, WERSJA 64-BITOWA | EXCHANGE 2003, WERSJA 32-BITOWA |
| • Windows 2008, wersja 64-bitowa<br>• SBS 2008, wersja 64-bitowa | 7 + | Tak | Niezgodne | Tak | Nie | Niezgodne |

| System operacyjny | Wersja programu IIS | Reguły ochrony danych na urządzeniu | | Kontrola dostępu | | |
|---|---|---|---|---|---|---|
| | | Exchange 2007 (lub nowszy), wersja 64-bitowa | Exchange 2003, wersja 32-bitowa | Exchange 2010 (lub nowszy), wersja 64-bitowa | Exchange 2007, wersja 64-bitowa | Exchange 2003, wersja 32-bitowa |
| Windows 2003, wersja 64-bitowa | 6.0 | Tak | Niezgodne | Nie | Nie | Niezgodne |
| • Windows 2003, wersja 32-bitowa<br>• SBS 2003, wersja 32-bitowa | 6.0 | Niezgodne | Nie | Niezgodne | Niezgodne | Nie |

**Tabela 6-6. Systemy operacyjne urządzeń mobilnych — pomoc techniczna**

| Systemy operacyjne urządzeń mobilnych | Wersja systemu operacyjnego |
|---|---|
| iOS | 3.0 - 6.1 (4.3 - 7.0) |
| Android | 2.2 - 4.2 |
| WM/WP (Windows) | 7.0 - 8.0 |
| BB (BlackBerry) | 7.0 - 10.1 |

## Konfigurowanie kontroli dostępu urządzenia

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij przycisk **Mobile Security** > **Kontrola dostępu urządzenia**.

   Zostanie wyświetlony nowy ekran.
5. Wybierz opcję **Włącz kontrolę dostępu urządzenia**.
6. Kliknij przycisk **Dodaj**.
7. Wpisz nazwę reguły i jej treściwy opis.
8. Zaznacz urządzenia, którym należy umożliwić/zablokować dostęp do serwera Microsoft Exchange Server, określając ich właścicieli.
   - **Wszyscy**
   - **Określ właścicieli urządzeń**
9. Jeśli wybrano opcję **Określ właścicieli urządzeń**:
   a. Wpisz nazwę właściciela urządzenia i kliknij przycisk **Wyszukaj**, aby znaleźć właściciela urządzenia na globalnej liście adresów serwera Microsoft Exchange Server.
   b. Zaznacz właściciela urządzenia i kliknij przycisk **Dodaj**.
10. Jeśli znasz system operacyjny urządzenia, wybierz go na liście rozwijanej **Typ**.
11. Wybierz opcję **Określ zakres numerów wersji** (jeśli dysponujesz takimi danymi) i określ, które wersje tego systemu operacyjnego są dozwolone.
12. Określ, czy program Messaging Security Agent powinien zezwolić na dostęp do poczty, kalendarza, kontaktów lub zadań właściciela urządzenia, czy blokować go.

13. Kliknij przycisk **Zapisz**.

## Anulowanie oczekującego wymazywania urządzenia

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij przycisk **Mobile Security** > **Wymazywanie urządzenia**.

   Zostanie wyświetlony nowy ekran.
5. Określ urządzenie w tabeli wymazywania urządzeń i kliknij przycisk **Anuluj wymazywanie**.
6. Kliknij przycisk **OK**.

## Ręczne wymazywanie zawartości urządzeń

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij przycisk **Mobile Security** > **Wymazywanie urządzenia**.

   Zostanie wyświetlony nowy ekran.

5. Kliknij przycisk **Wybierz urządzenia**.

   Zostanie wyświetlony nowy ekran.

6. Wpisz nazwę właściciela urządzenia i kliknij przycisk **Wyszukaj**, aby znaleźć urządzenie.

7. Jeśli urządzenie jest dostępne do wymazywania, zaznacz je i kliknij przycisk **Wymaż**.

**Uwaga**

Nie można zaznaczyć urządzenia, jeśli jego status po wyszukiwaniu to **Wymazanie zawartości powiodło się** lub **Oczekuje na wymazanie zawartości**.

## Konfigurowanie reguł zabezpieczeń

Program Worry-Free Business Security wykorzystuje reguły domyślne systemu Microsoft Exchange jako swoje reguły domyślne. Reguły domyślne są wyświetlane na liście Reguły zabezpieczeń.

W programie Worry-Free Business Security nie są stosowane reguły inne niż domyślne, dodane za pomocą konsoli zarządzania systemu Microsoft Exchange lub polecenia Exchange Cmdlet.

Firma Trend Micro zaleca administratorom zarządzanie regułami zabezpieczeń za pomocą konsoli zarządzania programu Worry-Free Business Securitylub systemu Microsoft Exchange.

**Procedura**

1. Przejdź do menu **Urządzenia**.

2. Wybierz program Messaging Security Agent.

3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.

4. Kliknij przycisk **Mobile Security** > **Zasady bezpieczeństwa**.

   Zostanie wyświetlony nowy ekran.

5. Kliknij przycisk **Dodaj**.

6. Wpisz nazwę reguły i jej treściwy opis.

7. Wpisz nazwę właściciela urządzenia i kliknij przycisk **Wyszukaj**, aby znaleźć właściciela urządzenia na globalnej liście adresów serwera Microsoft Exchange Server.

8. Zaznacz właściciela urządzenia i kliknij przycisk **Dodaj**.

9. Wybierz kryteria zabezpieczeń, które zostaną zastosowane do urządzenia:

   - **Minimalna długość hasła**: Wytyczne dotyczące haseł do urządzeń mobilnych zawiera część *Wymagania dotyczące złożoności haseł na stronie 6-60*.
   - **Minimalna liczba wymaganych zestawów znaków**: Wytyczne dotyczące haseł do urządzeń mobilnych zawiera część *Wymagania dotyczące złożoności haseł na stronie 6-60*.
   - **Zablokuj urządzenie po braku aktywności**
   - **Wymaga szyfrowania urządzenia**: Urządzenie mobilne musi obsługiwać szyfrowanie.
   - **Wymaż urządzenie po nieudanym logowaniu**

10. Kliknij przycisk **Zapisz**.

## Wymagania dotyczące złożoności haseł

Wymagania dotyczące złożoności haseł różnią się w zależności od typu urządzenia i systemu operacyjnego.

W poniższych tabelach wymieniono skutki zastosowania każdej z "Opcji" dotyczącej złożoności dla urządzeń przetestowanych w czasie wydania programu Worry-Free Business Security 9,0 SP3.

**Uwaga**

Zakres funkcji związany ze złożonością hasła zależy od typu urządzenia i wersji systemu operacyjnego. Jeśli określone hasło nie spełnia wymagań dotyczących złożoności, na większości urządzeń jest wyświetlany komunikat dla użytkownika informujący o specjalnych wymaganiach dla danego urządzenia.

**TABELA 6-7. Urządzenia z systemem Android**

| POZIOM ZŁOŻONOŚCI | WYMAGANIA DOTYCZĄCE ZŁOŻONOŚCI | |
|---|---|---|
| | ANDROID 4 | ANDROID 2 |
| Opcja 1 | Połączenie niżej wymienionych typów znaków:<br>• Co najmniej jedna wielka (A–Z) lub mała litera (a–z)<br>• Co najmniej jedna cyfra (0–9) lub co najmniej jeden znak specjalny (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) | Znaki alfanumeryczne |
| Opcja 2 | Połączenie niżej wymienionych typów znaków:<br>• Co najmniej jedna wielka (A–Z) lub mała litera (a–z)<br>• Co najmniej dwie cyfry (0–9) lub znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) | Połączenie niżej wymienionych typów znaków:<br>• Znaki alfanumeryczne<br>• Co najmniej dwie cyfry (0–9) lub znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) |
| Opcja 3 | Połączenie niżej wymienionych typów znaków:<br>• Co najmniej jedna wielka (A–Z) lub mała litera (a–z)<br>• Co najmniej trzy cyfry (0–9) lub znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) | Połączenie niżej wymienionych typów znaków:<br>• Znaki alfanumeryczne<br>• Co najmniej trzy cyfry (0–9) lub znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) |

| Poziom złożoności | Wymagania dotyczące złożoności | |
|---|---|---|
| | Android 4 | Android 2 |
| Opcja 4 | Połączenie niżej wymienionych typów znaków:<br>• Co najmniej jedna wielka (A–Z) lub mała litera (a–z)<br>• Co najmniej cztery cyfry (0–9) lub znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) | Połączenie niżej wymienionych typów znaków:<br>• Znaki alfanumeryczne<br>• Co najmniej cztery cyfry (0–9) lub znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) |

**Tabela 6-8. Urządzenia z systemem iOS**

| Poziom złożoności | Wymagania dotyczące złożoności |
|---|---|
| Opcja 1 | Połączenie niżej wymienionych typów znaków:<br>• Znaki alfanumeryczne<br>• Co najmniej jeden znak specjalny (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) |
| Opcja 2 | Połączenie niżej wymienionych typów znaków:<br>• Znaki alfanumeryczne<br>• Co najmniej dwa znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) |
| Opcja 3 | Połączenie niżej wymienionych typów znaków:<br>• Znaki alfanumeryczne<br>• Co najmniej trzy znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) |
| Opcja 4 | Połączenie niżej wymienionych typów znaków:<br>• Znaki alfanumeryczne<br>• Co najmniej cztery znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) |

**TABELA 6-9. Urządzenia Windows Phone**

| POZIOM ZŁOŻONOŚCI | WYMAGANIA DOTYCZĄCE ZŁOŻONOŚCI | |
|---|---|---|
| | WINDOWS PHONE 8 | WINDOWS PHONE 7 |
| Opcja 1 | Co najmniej jeden z poniższych typów znaków:<br>• wielkie litery (A–Z)<br>• małe litery (a–z)<br>• cyfry (0–9)<br>• znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) | Połączenie co najmniej dwóch niżej wymienionych typów znaków:<br>• wielkie litery (A–Z)<br>• małe litery (a–z)<br>• cyfry (0–9)<br>• znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) |
| Opcja 2 | Połączenie co najmniej dwóch niżej wymienionych typów znaków:<br>• wielkie litery (A–Z)<br>• małe litery (a–z)<br>• cyfry (0–9)<br>• znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) | Połączenie co najmniej dwóch niżej wymienionych typów znaków:<br>• wielkie litery (A–Z)<br>• małe litery (a–z)<br>• cyfry (0–9)<br>• znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) |
| Opcja 3 | Połączenie co najmniej trzech niżej wymienionych typów znaków:<br>• wielkie litery (A–Z)<br>• małe litery (a–z)<br>• cyfry (0–9)<br>• znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) | Połączenie co najmniej trzech niżej wymienionych typów znaków:<br>• wielkie litery (A–Z)<br>• małe litery (a–z)<br>• cyfry (0–9)<br>• znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) |

| Poziom złożoności | Wymagania dotyczące złożoności | |
|---|---|---|
| | Windows Phone 8 | Windows Phone 7 |
| Opcja 4 | Połączenie wszystkich niżej wymienionych typów znaków:<br>• wielkie litery (A–Z)<br>• małe litery (a–z)<br>• cyfry (0–9)<br>• znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) | Połączenie wszystkich niżej wymienionych typów znaków:<br>• wielkie litery (A–Z)<br>• małe litery (a–z)<br>• cyfry (0–9)<br>• znaki specjalne (!@#$ %^&*()_-=+~`[]{}\|;:'"?/<>,.) |

**Tabela 6-10. Urządzenia BlackBerry**

| Poziom złożoności | Wymagania dotyczące złożoności |
|---|---|
| Opcja 1 | Co najmniej jedna wielka (A–Z) lub mała litera (a–z) |
| Opcja 2 | Połączenie co najmniej dwóch niżej wymienionych typów znaków:<br>• wielkie litery (A–Z)<br>• małe litery (a–z)<br>• cyfry (0–9)<br>• znaki specjalne (!@#$%^&*()_-=+~`[]{}\|;:'"?/<>,.) |
| Opcja 3 | Połączenie co najmniej trzech niżej wymienionych typów znaków:<br>• wielkie litery (A–Z)<br>• małe litery (a–z)<br>• cyfry (0–9)<br>• znaki specjalne (!@#$%^&*()_-=+~`[]{}\|;:'"?/<>,.) |

| Poziom złożoności | Wymagania dotyczące złożoności |
|---|---|
| Opcja 4 | Połączenie wszystkich niżej wymienionych typów znaków:<br>• wielkie litery (A–Z)<br>• małe litery (a–z)<br>• cyfry (0–9)<br>• znaki specjalne (!@#$%^&*()_-=+~`[]{}\|;:'"?/<>,.) |

# Kwarantanna dla programów Messaging Security Agent

Kiedy program Messaging Security Agent wykryje zagrożenie, spam, ograniczone załączniki i/lub ograniczoną zawartość w wiadomościach e-mail, może przenieść wiadomość do folderu kwarantanny. Ten proces stanowi alternatywę usunięcia wiadomości/załącznika i uniemożliwia użytkownikom otwarcie zarażonej wiadomości i rozprzestrzenianie zagrożenia.

Domyślny folder kwarantanny programu Message Security Agent to:

```
<folder instalacji programu Messaging Security Agent>\storage
\quarantine
```

Poddane kwarantannie pliki są szyfrowane w celu zwiększenia bezpieczeństwa. Aby otworzyć zarażony plik, należy użyć narzędzia Przywracanie zaszyfrowanych wirusów i oprogramowania spyware (`VSEncode.exe`). Patrz sekcja *Przywracanie zaszyfrowanych plików na stronie 14-18*.

Administratorzy mogą wysyłać zapytania do bazy danych kwarantanny w celu zebrania informacji o wiadomościach poddanych kwarantannie.

Funkcje kwarantanny umożliwiają:

- eliminację ryzyka trwałego usunięcia ważnych wiadomości, które zostały błędnie wykryte przez agresywne filtry;

- przeglądanie wiadomości e-mail, które wyzwalają akcje filtrów zawartości w celu określenia stopnia naruszenia reguł;
- zachowanie dowodów możliwego wykorzystywania systemu pocztowego firmy w niewłaściwy sposób przez pracowników.

**Uwaga**

Nie należy mylić folderu kwarantanny z folderem spamu użytkownika końcowego. Folder kwarantanny to folder oparty na plikach. Gdy program Messaging Security Agent poddaje wiadomość e-mail kwarantannie, wysyła ją do folderu kwarantanny. Folder spamu użytkownika końcowego znajduje się w magazynie informacji skrzynki pocztowej każdego użytkownika. Do folderu spamu użytkownika końcowego dostarczane są tylko te wiadomości e-mail, które zostały odpowiednio zakwalifikowane w ramach operacji kwarantanny antyspamowej, a nie w wyniku reguł filtrowania zawartości, skanowania antywirusowego/antyspyware lub blokowania załączników.

## Tworzenie zapytań dotyczących katalogów kwarantanny

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij pozycje **Kwarantanna** > **Zapytanie**.

   Zostanie wyświetlony nowy ekran.
5. Zmień odpowiednio następujące ustawienia:
   - Data/Przedział czasu
   - Przyczyny poddawania kwarantannie
     - **Wszystkie powody**

- **Określone typy**: można wybrać następujące opcje: Skanowanie antywirusowe, Anty-spam, Filtrowanie zawartości, Blokowanie załączników i/lub Części wiadomości, których nie można przeskanować.

- Stan ponownego wysyłania
  - **Nigdy nie wysłane ponownie**
  - **Przynajmniej raz wysłane ponownie**
  - **Oba powyższe**
- Kryteria zaawansowane
  - **Nadawca**: Wiadomości od określonych nadawców. W razie potrzeby można użyć symboli wieloznacznych.
  - **Odbiorca**: wiadomości do określonych odbiorców. W razie potrzeby można użyć symboli wieloznacznych.
  - **Temat**: wiadomości z określonymi tematami. W razie potrzeby można użyć symboli wieloznacznych.
  - **Sortuj według**: umożliwia skonfigurowanie warunku sortowania dla strony wyników.
  - **Wyświetlaj**: liczba wyników na stronie.

6. Kliknij przycisk **Wyszukaj**. Patrz sekcja *Wyświetlanie wyników zapytań dotyczących kwarantanny i podejmowanie działań na stronie 6-67*.

---

## Wyświetlanie wyników zapytań dotyczących kwarantanny i podejmowanie działań

Ekran **Wyniki zapytania dotyczącego kwarantanny** wyświetla następujące informacje o wiadomościach:

- **Czas skanowania**
- **Nadawca**

- **Odbiorca**
- **Temat**
- **Przyczyna**: przyczyna, dla której wiadomość e-mail została poddana kwarantannie.
- **Nazwa pliku**: pazwa zablokowanego pliku w wiadomości e-mail.
- **Ścieżka kwarantanny**: położenie folderu kwarantanny dla wiadomości e-mail. Administrator może odszyfrować plik przy użyciu narzędzia VSEncoder.exe (patrz *Przywracanie zaszyfrowanych plików na stronie 14-18*), a następnie zmienić rozszerzenie pliku na `.eml`, aby go wyświetlić.

  **OSTRZEŻENIE!**
  Wyświetlanie zarażonych plików może spowodować rozprzestrzenienie infekcji.

- **Stan ponownego wysyłania**

**Procedura**

1. Jeśli uważasz, że wiadomość jest niebezpieczna, usuń ją.

   **OSTRZEŻENIE!**
   Folder kwarantanny zawiera wiadomości e-mail cechujące się dużym ryzykiem zarażenia. W czasie obsługi wiadomości w folderze kwarantanny należy zachować ostrożność, aby przypadkowo nie zarazić komputera klienckiego.

2. Jeśli uważasz, że wiadomość jest bezpieczna, zaznacz ją i kliknij ikonę ponownego wysyłania ( ).

   **Uwaga**
   Jeżeli poddane kwarantannie wiadomości, które zostały wysłane z wykorzystaniem programu Microsoft Outlook, są wysyłane ponownie, odbiorca może otrzymać wiele kopii tej samej wiadomości. Taka sytuacja może być spowodowana rozkładaniem przez silnik skanowania w poszukiwaniu wirusów każdej skanowanej wiadomości na klika sekcji.

3. Jeśli nie możesz wysłać wiadomości ponownie, być może konto administratora systemu na serwerze Microsoft Exchange nie istnieje.

   a. Używając Edytora rejestru systemu Windows, otwórz następującą pozycję rejestru na serwerze:

      ```
      HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion
      ```

   b. Dokonaj edycji tej pozycji w następujący sposób:

      **OSTRZEŻENIE!**

      Nieprawidłowa edycja rejestru może poważnie uszkodzić system. Przed dokonaniem zmian w rejestrze należy utworzyć kopię zapasową wszystkich cennych danych na serwerze.

      - `ResendMailbox {skrzynka pocztowa administratora}`

        Przykład: `admin@przykład.com`

      - `ResendMailboxDomain {domena administratora}`

        Przykład: `przyklad.com`

      - `ResendMailSender {konto e-mail administratora}`

        Przykład: `admin`

   c. Zamknij Edytor rejestru.

## Obsługa katalogów kwarantanny

Za pomocą tej funkcji można ręcznie lub automatycznie usuwać wiadomości poddane kwarantannie. Ta funkcja pozwala usuwać wszystkie wiadomości, ponownie wysłane wiadomości lub wiadomości, które nie zostały ponownie wysłane.

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij pozycje **Kwarantanna** > **Obsługa**.

   Zostanie wyświetlony nowy ekran.
5. Zmień odpowiednio następujące ustawienia:
   - **Włącz automatyczną obsługę**: Dostępne tylko w przypadku automatycznej obsługi.
   - Pliki do usunięcia
     - **Wszystkie pliki poddane kwarantannie**
     - **Pliki poddane kwarantannie, które nigdy nie zostały ponownie wysłane**
     - **Pliki poddane kwarantannie, które co najmniej raz zostały ponownie wysłane**
   - **Operacja**: Liczba dni przechowywania wiadomości. Na przykład jeśli bieżąca data to 21 listopada, a w polu **Usuń pliki starsze niż** wpisano wartość `10`, to podczas wykonywania zadania automatycznego usuwania program Messaging Security Agent usunie wszystkie pliki sprzed 11 listopada.
6. Kliknij przycisk **Zapisz**.

## Konfigurowanie katalogów kwarantanny

Należy skonfigurować katalogi kwarantanny na serwerze Microsoft Exchange. Katalog kwarantanny zostanie wyłączony ze skanowania.

**Uwaga**

Katalogi kwarantanny bazują na plikach i nie znajdują się w magazynie informacji.

Program Messaging Security Agent poddaje kwarantannie wiadomości e-mail zgodnie ze skonfigurowanymi operacjami. Istnieją następujące katalogi kwarantanny:

- **Ochrona antywirusowa**: kwarantanna wiadomości e-mail zawierających wirusy/złośliwe oprogramowanie, spyware/grayware, robaki, trojany i inne złośliwe zagrożenia.
- **Ochrona antyspamowa** : kwarantanna poczty e-mail o charakterze spamu i stanowiącej zagrożenie typu phishing.
- **Blokowanie załączników**: kwarantanna wiadomości e-mail zawierających ograniczone załączniki.
- **Filtrowanie zawartości**: kwarantanna wiadomości e-mail zawierających ograniczoną zawartość.

Domyślnie do wszystkich katalogów prowadzi ta sama ścieżka (`<folder instalacji programu Messaging Security Agent>\storage\quarantine`). Ścieżki do każdego z tych katalogów można zmienić.

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij kolejno opcje **Kwarantanna** > **Katalog**.

   Zostanie wyświetlony nowy ekran.
5. Ustaw ścieżkę do następujących katalogów kwarantanny:
   - **Ochrona antywirusowa**

- **Ochrona antyspamowa**
- **Filtrowanie zawartości**
- **Blokowanie załączników**

6. Kliknij przycisk **Zapisz**.

# Ustawienia powiadamiania dla programów Messaging Security Agent

Program Worry-Free Business Security może wysyłać różne powiadomienia dotyczące ostrzeżeń w postaci wiadomości e-mail.

Za pomocą niestandardowych definicji poczty wewnętrznej można skonfigurować powiadomienia w taki sposób, aby dotyczyły tylko wewnętrznych wiadomości e-mail. Jest to przydatne, jeśli firma używa dwóch lub więcej domen i chce traktować wiadomości e-mail z obydwu domen jako pocztę wewnętrzną. (na przykład: przyklad.com i przyklad.net).

Odbiorcy z listy definicji poczty wewnętrznej będą otrzymywać wiadomości z powiadomieniem, jeżeli w obszarze Ustawienia powiadamiania dla **oprogramowania antywirusowego**, **filtrowania zawartości** i **blokowania załączników** zostanie zaznaczone pole wyboru **Nie powiadamiaj odbiorców zewnętrznych**. Nie należy mylić listy definicji poczty wewnętrznej z listą dozwolonych nadawców.

Aby uniknąć oznaczania wiadomości e-mail przychodzących z domen zewnętrznych, należy dodać zewnętrzne adresy e-mail do list **dozwolonych nadawców** oprogramowania antyspamowego.

## Informacje o niestandardowych definicjach poczty wewnętrznej

Program Messaging Security Agent dzieli ruch wiadomości e-mail na dwie kategorie sieciowe: wewnętrzny i zewnętrzny. Agent sprawdza serwer Microsoft Exchange w celu poznania definicji adresów wewnętrznych i zewnętrznych. Wszystkie adresy wewnętrzne posiadają wspólną domenę, do której nie należą żadne adresy zewnętrzne.

Jeśli na przykład adresem domeny wewnętrznej jest „@trend_1.com”, program Messaging Security Agent kwalifikuje adresy takie jak „abc@trend_1.com” czy

„xyz@trend_1.com" jako adresy wewnętrzne. Wszystkie pozostałe adresy, takie jak „abc@trend_2.com" czy „jondoe@123.com", agent klasyfikuje jako zewnętrzne.

W programie Messaging Security Agent jako adres wewnętrzny można zdefiniować tylko jedną domenę. W przypadku korzystania z narzędzia Menedżer systemu Exchange firmy Microsoft w celu zmiany podstawowego adresu na serwerze, program Messaging Security Agent nie rozpozna nowego adresu jako adresu wewnętrznego, ponieważ program Messaging Security Agent nie będzie mógł wykryć zmiany reguły nadawcy.

Na przykład firma ma dwa adresy domeny: @przyklad_1.com i @przyklad_2.com. Adres @przyklad_1.com ustawiony zostaje jako adres podstawowy. Program Messaging Security Agent będzie klasyfikował wiadomości e-mail zawierające adres podstawowy jako wewnętrzne (abc@przyklad_1.com lub xyz@przyklad_1.com są więc wewnętrzne). Następnie za pomocą narzędzia Menedżer systemu Exchange adres podstawowy zostaje zmieniony na @przyklad_2.com. Oznacza to, że teraz program Microsoft Exchange rozpoznaje adresy takie jak abc@przyklad_2.com oraz xyz@przyklad_2.com jako adresy wewnętrzne.

## Konfigurowanie ustawień powiadomień dla programów Messaging Security Agent

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij pozycję **Operacje** > **Ustawienia powiadamiania**.

   Zostanie wyświetlony nowy ekran.
5. Zmień odpowiednio następujące ustawienia:

   - **Adres e-mail**: Adres osoby, w imieniu której program Worry-Free Business Security będzie wysyłać powiadomienia.

- **Definicja poczty wewnętrznej**
  - **Domyślne**: programWorry-Free Business Security będzie traktować wiadomości e-mail z tej samej domeny jako pocztę wewnętrzną.
  - **Niestandardowy**: określ adresy e-mail lub domeny, z których wiadomości mają być traktowane jako poczta wewnętrzna.

6. Kliknij przycisk **Zapisz**.

---

# Konfigurowanie obsługi wiadomości typu spam

Ekran **Obsługa wiadomości typu spam** umożliwia skonfigurowanie ustawień funkcji kwarantanny po stronie użytkownika (EUQ, End User Quarantine) lub kwarantanny po stronie serwera.

---

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij kolejno opcje **Operacje** > **Obsługa wiadomości typu spam**.

   Zostanie wyświetlony nowy ekran.
5. Kliknij opcję **Włącz narzędzie End User Quarantine**.

   Po włączeniu tego narzędzia utworzony zostanie folder kwarantanny po stronie serwera skrzynki pocztowej dla każdego klienta, a w drzewie folderów w programie Outlook użytkownika końcowego pojawi się folder `Spam`. Od tej chwili funkcja EUQ będzie filtrować pocztę typu spam i umieszczać ją w utworzonym folderze spamu. Aby uzyskać więcej informacji, zobacz *Zarządzanie funkcją End User Quarantine na stronie 6-76*.

**Porada**

W przypadku wybrania tej opcji w celu zwiększenia wydajności klientów firma Trend Micro zaleca wyłączenie w agentach Trend Micro Anti-Spam Toolbar.

Usuń zaznaczenie pola wyboru **Włącz narzędzie End User Quarantine**, aby wyłączyć narzędzie End User Quarantine dla wszystkich skrzynek pocztowych znajdujących się na serwerze Microsoft Exchange. Po wyłączeniu funkcji EUQ foldery spamu użytkowników nadal będą dostępne, ale wiadomości zaklasyfikowane jako spam nie będą tam przenoszone.

6. Kliknij opcję **Utwórz folder wiadomości typu spam i usuń te wiadomości** w celu natychmiastowego utworzenia folderów spamu dla nowo utworzonych klientów poczty oraz istniejących klientów poczty, których folder spamu został usunięty. W przypadku innych istniejących klientów nastąpi usunięcie wiadomości typu spam starszych niż liczba dni określona w polu Ustawienia folderu wiadomości typu spam klienta.

7. W obszarze **Usuń wiadomości typu spam starsze niż {liczba} dni** zmodyfikuj długość okresu, przez który program Messaging Security Agent będzie przechowywać wiadomości typu spam. Wartość domyślna to 14 dni, a maksymalny limit wynosi 30 dni.

8. Wyłączanie narzędzia End User Quarantine dla wybranych użytkowników:

   a. W obszarze **Lista wyjątków narzędzia End User Quarantine** wpisz adres e-mail użytkownika, dla którego chcesz wyłączyć narzędzie EUQ.

   b. Kliknij przycisk **Dodaj**.

      Adres e-mail użytkownika końcowego zostanie dodany do listy adresów z wyłączonym narzędziem End User Quarantine.

      Aby usunąć użytkownika końcowego z listy i przywrócić usługę EUQ, zaznacz adres e-mail tego użytkownika na liście i kliknij przycisk **Usuń**.

9. Kliknij przycisk **Zapisz**.

# Zarządzanie funkcją End User Quarantine

Program Messaging Security Agent podczas instalacji dodaje na serwerze folder o nazwie `Spam` do skrzynki pocztowej każdego użytkownika. Po otrzymaniu wiadomości sklasyfikowanych jako spam, system poddaje je kwarantannie w tym folderze, zgodnie z regułami filtra spamu, wstępnie zdefiniowanymi przez program Messaging Security Agent. Użytkownicy końcowi mogą wyświetlić ten folder spamu, aby otworzyć, przeczytać lub usunąć podejrzane wiadomości e-mail. Patrz sekcja *Konfigurowanie obsługi wiadomości typu spam na stronie 6-74*.

Administratorzy mogą także utworzyć folder spamu na serwerze Microsoft Exchange. Kiedy administrator tworzy konto skrzynki pocztowej, obiekt skrzynki pocztowej nie jest tworzony na serwerze Microsoft Exchange natychmiast, a dopiero po spełnieniu następujących warunków:

- Użytkownik końcowy pierwszy raz loguje się na konto poczty e-mail
- Na konto poczty e-mail dostarczona zostanie pierwsza wiadomość e-mail

Administrator musi utworzyć obiekt skrzynki pocztowej, zanim narzędzie End User Quarantine będzie mogło utworzyć folder spamu.

## Folder poczty typu spam po stronie klienta

Użytkownicy końcowi mogą otwierać wiadomości e-mail, które zostały poddane kwarantannie w folderze spamu. Po otwarciu jednej z takich wiadomości w oknie wiadomości e-mail wyświetlane są dwa przyciski: **Zatwierdzony nadawca** oraz **Wyświetl listę zatwierdzeni nadawcy**.

- Adres nadawcy wiadomości zostanie dodany do listy **Zatwierdzeni nadawcy** użytkownika końcowego, gdy otworzy on wiadomość z folderu spamu i kliknie przycisk **Zatwierdzony nadawca**.
- Kliknięcie opcji **Wyświetl listę zatwierdzeni nadawcy** powoduje wyświetlenie ekranu, na którym użytkownik końcowy może obejrzeć i zmodyfikować swoją listę dozwolonych nadawców według adresu e-mail lub domeny.

## Zatwierdzeni nadawcy

Kiedy do folderu spamu użytkownika końcowego zostanie przesłana wiadomość e-mail i kliknie on przycisk **Zatwierdź nadawcę**, program Messaging Security Agent przeniesie

tę wiadomość do lokalnej skrzynki odbiorczej użytkownika końcowego i doda adres nadawcy do osobistej listy zatwierdzeni nadawcy. Program Messaging Security Agent zapisze to zdarzenie w dzienniku.

Kiedy serwer Microsoft Exchange odbierze wiadomości wysłane z adresów znajdujących się na liście dozwolonych nadawców użytkownika końcowego, dostarczy je do skrzynki odbiorczej tego użytkownika, niezależnie od nagłówka i zawartości wiadomości.

**Uwaga**

Program Messaging Security Agent udostępnia także administratorom listy dozwolonych i zablokowanych nadawców. Program Messaging Security Agent stosuje listy nadawców dozwolonych i zablokowanych przez administratora przed sprawdzeniem listy użytkownika końcowego.

### Funkcja porządkowania narzędzia End User Quarantine

Funkcja porządkowania programu Messaging Security Agent realizuje następujące zadania co 24 godziny domyślnie o godzinie 2:30 rano:

- Automatycznie usuwa przeterminowane wiadomości o charakterze spamu.
- Na nowo tworzy folder spamu, jeśli został on usunięty.
- Tworzy foldery spamu dla nowo tworzonych kont pocztowych.
- Obsługuje reguły wiadomości e-mail.

Funkcja porządkowania stanowi integralną część programu Messaging Security Agent i nie wymaga konfigurowania.

## Pomoc techniczna/diagnostyka firmy Trend Micro

Pomoc techniczna/diagnostyka może ułatwiać diagnostykę systemu lub jedynie generować raporty o stanie procesów programu Messaging Security Agent. Jeśli wystąpią nieoczekiwane trudności, można skorzystać z konsoli diagnostycznej, aby utworzyć raporty diagnostyczne i wysłać je do analizy do działu pomocy technicznej firmy Trend Micro.

Każdy moduł programu Messaging Security Agent wyświetla komunikaty w programie, a następnie zapisuje działania w plikach dzienników po ich wykonaniu. Dzienniki te można przekazywać do zespołu pomocy technicznej firmy Trend Micro w celu przeprowadzenia diagnostyki działania programu w środowisku użytkownika.

Za pomocą konsoli diagnostycznej można utworzyć dzienniki dla następujących modułów:

- Usługa Master programu Messaging Security Agent
- Serwer zdalnej konfiguracji programu Messaging Security Agent
- Monitor systemu programu Messaging Security Agent
- Funkcja API skanowania antywirusowego (VSAPI)
- Protokół SMTP (Simple Mail Transfer Protocol)
- Interfejs CGI (Common Gateway Interface)

Domyślnie program MSA przechowuje dzienniki w następującym katalogu:

`<folder instalacji programu Messaging Security Agent>\Debug`.

Dane wyjściowe można przeglądać w dowolnym edytorze tekstu.

## Generowanie raportów diagnostycznych

Generowanie raportów diagnostycznych ułatwia pomocy technicznej firmy Trend Micro rozwiązanie problemu.

**Procedura**

1. Przejdź do menu **Urządzenia**.
2. Wybierz program Messaging Security Agent.
3. Kliknij pozycję **Konfiguruj regułę**.

   Zostanie wyświetlony nowy ekran.
4. Kliknij kolejno opcje **Operacje** > **Pomoc techniczna/Diagnostyka**.

Zostanie wyświetlony nowy ekran.

5. Wybierz moduły do monitorowania:
   - **Usługa Master** programu Messaging Security Agent
   - **Serwer zdalnej konfiguracji** programu Messaging Security Agent
   - **Monitor systemu** programu Messaging Security Agent
   - **Funkcja API skanowania antywirusowego (VSAPI)** na serwerze Exchange Server 2003, 2007 lub 2010
   - **Skanowanie na poziomie sklepu** na serwerze Exchange Server 2013
   - **Protokół SMTP (Simple Mail Transfer Protocol)** na serwerze Exchange Server 2003
   - **Usługa transportowa** na serwerze Exchange Server 2007, 2010 lub 2013
   - **Interfejs CGI (Common Gateway Interface)**
6. Kliknij przycisk **Zastosuj**.

   Konsola diagnostyczna rozpocznie gromadzenie danych dla wybranych modułów.

# Monitorowanie w czasie rzeczywistym

Funkcja monitorowania w czasie rzeczywistym służy do wyświetlania bieżących informacji o wybranym serwerze Microsoft Exchange oraz programie Messaging Security Agent. Wyświetlane są w niej informacje o przeskanowanych wiadomościach oraz statystyki zabezpieczeń, w tym liczba wykrytych wirusów i spamu, zablokowanych załączników, a także przypadków naruszenia zawartości. Służy ona również do sprawdzania, czy agent działa prawidłowo.

## Praca z monitorowaniem w czasie rzeczywistym

**Procedura**

1. Aby uzyskać dostęp do narzędzia monitorowania w czasie rzeczywistym z konsoli internetowej:
   a. Przejdź do menu **Urządzenia**.
   b. Wybierz program Messaging Security Agent.
   c. Kliknij pozycję **Konfiguruj regułę**.
      Zostanie wyświetlony nowy ekran.
   d. Kliknij łącze **Monitor w czasie rzeczywistym** znajdujące się w prawej górnej części ekranu.
2. Aby uzyskać dostęp do narzędzia monitorowania w czasie rzeczywistym z menu Start systemu Windows, kliknij pozycje **Wszystkie programy** > **Trend Micro Messaging Security Agent** > **Monitorowanie w czasie rzeczywistym**.
3. Kliknij opcję **Resetuj**, aby wyzerować statystykę zabezpieczeń.
4. Kliknij opcję **Wyczyść zawartość**, aby usunąć starsze informacje o przeskanowanych wiadomościach.

# Dodawanie informacji o wykluczeniu odpowiedzialności do wychodzących wiadomości e-mail

Informację o wykluczeniu odpowiedzialności można dodawać tylko do wychodzących wiadomości e-mail.

**Procedura**

1. Utwórz plik tekstowy i umieść w nim tekst klauzuli wykluczenia odpowiedzialności.
2. Zmodyfikuj następujące klucze w rejestrze:
   - Pierwszy klucz:

     Ścieżka: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

     Klucz: `EnableDisclaimer`

     Typ: `REG_DWORD`

     Wartość danych: `0 — wyłącz, 1 — włącz`

   - Drugi klucz:

     Ścieżka: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

     Klucz: `DisclaimerSource`

     Typ: `REG_SZ`

     Wartość: Pełna ścieżka pliku z tekstem wykluczenia odpowiedzialności.

     Przykład: `C:\Dane\Wykluczenie.txt`

     **Uwaga**

     Program Worry-Free Business Security domyślnie ustala, czy wychodząca wiadomość e-mail jest wysyłana do domen wewnętrznych czy zewnętrznych, i dodaje informację o wykluczeniu odpowiedzialności do każdej wiadomości wysyłanej do domen zewnętrznych. Użytkownik może zastąpić ustawienie domyślne i dodawać tę klauzulę do każdej wychodzącej wiadomości, z wyjątkiem wiadomości kierowanych do domen uwzględnionych w następującym kluczu rejestru:

   - Trzeci klucz:

     Ścieżka: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

Klucz: `InternalDomains`

Typ: `REG_SZ`

Wartość: Wpisz nazwy domen do wykluczenia. Użyj średnika (;) do oddzielenia poszczególnych pozycji.

Na przykład: `domena1.org;domena2.org`

**Uwaga**

Tu nazwy domen to nazwy DNS serwerów Exchange.

# Rozdział 7

# Zarządzenie skanowaniami

W tym rozdziale opisano sposób uruchamiania skanowania w programach Security Agent i Messaging Security Agent (tylko w wersji Advanced) w celu ochrony sieci i klientów przed zagrożeniami.

# Skanowanie — informacje

Podczas skanowania współpracujący z plikiem sygnatury silnik skanowania firmy Trend Micro przeprowadza wykrywanie na pierwszym poziomie, stosując proces nazywany porównywaniem sygnatur. Ponieważ każde zagrożenie ma unikatową „sygnaturę", czyli ciąg znaków odróżniających je od innych kodów, w pliku sygnatury znajdują się nieaktywne fragmenty takiego kodu. Silnik porównuje następnie określone części każdego skanowanego pliku z sygnaturą w pliku sygnatur, szukając dopasowania.

W razie wykrycia pliku zawierającego zagrożenie silnik skanowania przeprowadzi odpowiednią operację, na przykład wyczyści ten plik, podda go kwarantannie, usunie lub zastąpi to zagrożenie tekstem lub plikiem (tylko w wersji Advanced). Te operacje można dostosować podczas konfigurowania zadań skanowania.

Program Worry-Free Business Security udostępnia **trzy rodzaje skanowania**. Każdy typ skanowania służy do innych zadań, ale wszystkie konfiguruje się w podobny sposób.

- Skanowanie w czasie rzeczywistym. Szczegółowe informacje można znaleźć w części *Skanowanie w czasie rzeczywistym na stronie 7-2*.
- Skanowanie ręczne. Szczegółowe informacje można znaleźć w części *Skanowanie ręczne na stronie 7-3*.
- Skanowanie zaplanowane. Szczegółowe informacje można znaleźć w części *Skanowanie zaplanowane na stronie 7-7*.

Programy Security Agent korzystają podczas skanowania z jednej spośród dwóch metod skanowania:

- Smart Scan
- Skanowanie standardowe

Szczegółowe informacje można znaleźć w części *Metody skanowania na stronie 5-3*.

# Skanowanie w czasie rzeczywistym

Skanowanie w czasie rzeczywistym zapewnia stałą ochronę.

Za każdym razem, gdy plik zostaje otwarty, pobrany, skopiowany lub zmodyfikowany, funkcja skanowania w czasie rzeczywistym programu **Security Agent** sprawdza ten plik w poszukiwaniu zagrożeń. Szczegółowe informacje o konfigurowaniu skanowania w czasie rzeczywistym zawiera część *Konfigurowanie skanowania w czasie rzeczywistym w programach Security Agent na stronie 5-8*.

W przypadku wiadomości e-mail program **Messaging Security Agent** (tylko w wersji Advanced) chroni wszystkie znane punkty wejścia wirusów, skanując w czasie rzeczywistym wszystkie przychodzące wiadomości e-mail, wiadomości SMTP, dokumenty wysyłane do folderów publicznych oraz pliki replikowane z innych serwerów Microsoft Exchange. Szczegółowe informacje o konfigurowaniu skanowania w czasie rzeczywistym zawiera część *Konfigurowanie skanowania w czasie rzeczywistym dla programów Messaging Security Agent na stronie 6-6*.

# Skanowanie ręczne

Skanowanie ręczne to skanowanie na żądanie.

Skanowanie ręczne **programów Security Agent** eliminuje zagrożenia z plików i usuwa ewentualne stare infekcje, aby zminimalizować ryzyko ponownego zarażenia.

Podczas skanowania ręcznego **programów Messaging Security Agent** (tylko w wersji Advanced) skanowane są wszystkie pliki w magazynie informacji serwera Microsoft Exchange.

Czas trwania skanowania zależy od zasobów sprzętowych komputera klienckiego i liczby plików do przeskanowania. Trwające skanowanie ręczne może zostać zatrzymane przez administratora programu Security Server (jeśli zostało uruchomione zdalnie z konsoli internetowej) lub przez użytkownika (jeśli zostało uruchomione bezpośrednio na kliencie).

**Porada**

Firma Trend Micro zaleca uruchomienie skanowania ręcznego po wystąpieniu epidemii zagrożeń.

## Uruchamianie skanowania ręcznego

W poniższej procedurze opisano sposób uruchamiania skanowania ręcznego **programów Security Agent** i **Messaging Security Agent** (tylko w wersji Advanced) za pomocą konsoli internetowej przez administratorów programu Security Server.

**Uwaga**

Skanowanie ręczne można także uruchomić bezpośrednio z klientów, klikając prawym przyciskiem myszy ikonę programu Security Agent na pasku zadań systemu Windows, a następnie polecenie **Skanuj teraz**. Skanowania ręcznego nie można uruchamiać bezpośrednio na serwerach Microsoft Exchange.

**Procedura**

1. Przejdź do pozycji **Skanowania** > **Skanowanie ręczne**.
2. (Opcjonalnie) Dostosuj ustawienia skanowania przed uruchomieniem skanowania ręcznego.

| Instrukcje i uwagi | Zalecane ustawienia skanowania |
|---|---|
| Aby dostosować ustawienia skanowania dla **programu Security Agent**, kliknij grupę komputerów lub serwerów.<br><br>Patrz sekcja *Cele skanowania i operacje dotyczące programów Security Agent na stronie 7-11*.<br><br>**Uwaga**<br>Ustawienia skanowania programów Security Agent są wykorzystywane także wtedy, gdy użytkownicy uruchamiają skanowanie ręczne bezpośrednio z klientów. Jeśli jednak przydzielisz użytkownikom uprawnienia do konfigurowania własnych ustawień skanowania, podczas skanowania zostaną wykorzystane ustawienia skonfigurowane przez użytkownika. | Cel<br><br>• Wszystkie pliki możliwe do skanowania: Uwzględnia wszystkie pliki możliwe do skanowania. Pliki, których nie można przeskanować to pliki chronione hasłem, pliki zaszyfrowane lub pliki wykraczające poza określone przez użytkownika ograniczenia skanowania.<br><br>• Skanuj pliki skompresowane do warstwy 1: Skanuje pliki skompresowane o 1 warstwie kompresji. Ta funkcja jest domyślnie wyłączona dla domyślnej grupy serwerów i włączona dla domyślnej grupy komputerów.<br><br>Wykluczenia<br><br>• Nie skanuj katalogów, w których zainstalowane są produkty firmy Trend Micro.<br><br>Ustawienia zaawansowane<br><br>• Zmodyfikuj listę dozwolonych spyware/grayware (tylko w przypadku skanowania antyspyware) |

| INSTRUKCJE I UWAGI | ZALECANE USTAWIENIA SKANOWANIA |
|---|---|
| Aby dostosować ustawienia skanowania dla **programu Messaging Security Agent**, rozwiń agenta i kliknij następujące pozycje:<br>• **Ochrona antywirusowa**: kliknij, aby agent skanował w poszukiwaniu wirusów i innego złośliwego oprogramowania. Patrz sekcja *Cele skanowania i operacje dotyczące programów Messaging Security Agent na stronie 7-20*.<br>• **Filtrowanie zawartości**: kliknij, aby agent skanował pocztę e-mail w poszukiwaniu zabronionej zawartości. Patrz sekcja *Zarządzanie regułami filtrowania zawartości na stronie 6-17*.<br>• **Blokowanie załączników**: kliknij, aby agent skanował pocztę e-mail pod kątem naruszenia reguł załączników. Patrz sekcja *Konfigurowanie blokowania załączników na stronie 6-48*. | • Agent skanuje wszystkie pliki, które można skanować. Podczas skanowania uwzględnia również treści wiadomości e-mail.<br>• Gdy agent wykryje plik zawierający wirusa lub inny złośliwy program, czyści ten plik. Jeśli pliku nie można wyczyścić, jest on zastępowany tekstem lub plikiem.<br>• Gdy agent wykryje plik zawierający trojana lub robaka, zastępuje go tekstem lub plikiem.<br>• Gdy agent wykryje plik zawierający samorozpakowujące się archiwum, zastępuje je tekstem lub plikiem.<br>• Agent nie czyści zarażonych plików, które są skompresowane. Skraca to czas potrzebny na skanowanie w czasie rzeczywistym. |

3. Wybierz grupy lub programy Messaging Security Agent do skanowania.

4. Kliknij przycisk **Skanuj teraz**.

   Program Security Server wysyła do agentów powiadomienie z poleceniem uruchomienia skanowania ręcznego. Na wyświetlonym następnie ekranie Wyniki powiadamiania o skanowaniu podana jest liczba agentów, które otrzymały i nie otrzymały powiadomienia.

5. Aby zatrzymać trwające skanowania, kliknij przycisk **Zatrzymaj skanowanie**.

   Program Security Server wysyła do agentów kolejne powiadomienie z poleceniem zatrzymania skanowania ręcznego. Na wyświetlonym następnie ekranie Wyniki powiadamiania o zatrzymaniu skanowania podana jest liczba agentów, które

otrzymały i nie otrzymały powiadomienia. Programy Security Agent mogą nie otrzymać powiadomienia, jeśli od momentu uruchomienia skanowania zostały przełączone w tryb offline lub jeśli wystąpiły zakłócenia w sieci.

# Skanowanie zaplanowane

Skanowanie zaplanowane działa podobnie jak skanowanie ręczne, ale wszystkie pliki i wiadomości e-mail (tylko w wersji Advanced) skanowane są w określonym czasie i z ustaloną częstotliwością. Funkcję skanowania zaplanowanego stosuje się w celu zautomatyzowania rutynowego skanowania klientów oraz zwiększenia wydajności zarządzania ochroną przed zagrożeniami.

**Porada**

Skanowanie zaplanowane należy uruchamiać poza godzinami szczytu, aby zminimalizować ewentualne zakłócenia w pracy użytkowników i działaniu sieci.

## Konfigurowanie skanowania zaplanowanego

Firma Trend Micro zaleca, aby nie planować wykonywania skanowania w tym samym czasie, co zaplanowanej aktualizacji. Może to spowodować przedwczesne zakończenie skanowania zaplanowanego. Analogicznie rozpoczęcie skanowania ręcznego w czasie skanowania zaplanowanego spowoduje przerwanie skanowania, ale zostanie ono uruchomione ponownie zgodnie z harmonogramem.

**Procedura**

1. Przejdź do pozycji **Skanowania** > **Skanowanie zaplanowane**.
2. Kliknij kartę **Harmonogram**.
   a. Określ częstotliwość (codziennie, co tydzień lub co miesiąc) oraz godzinę rozpoczęcia skanowania. Poszczególne grupy i programy Messaging Security Agent mogą mieć własny harmonogram.

**Uwaga**

W przypadku skanowania zaplanowanego w odstępach miesięcznych, jeśli po wybraniu liczby dni (31, 30 lub 29) okaże się, że dany miesiąc ma mniej dni, skanowanie nie zostanie w tym miesiącu uruchomione.

b. (Opcjonalnie) Wybierz opcję **Po ukończeniu skanowania zaplanowanego wyłącz klienta**.

c. Kliknij przycisk **Zapisz**.

3. Kliknij kartę **Ustawienia** i skonfiguruj dowolne wymagane ustawienia Skanowania zaplanowanego.

| INSTRUKCJE I UWAGI | ZALECANE USTAWIENIA SKANOWANIA |
|---|---|
| Aby dostosować ustawienia skanowania dla **programu Security Agent**, kliknij grupę komputerów lub serwerów. Patrz sekcja *Cele skanowania i operacje dotyczące programów Security Agent na stronie 7-11*.<br><br>**Uwaga**<br>Jeśli przydzielisz użytkownikom uprawnienia do konfigurowania własnych ustawień skanowania, podczas skanowania zostaną wykorzystane ustawienia skonfigurowane przez użytkownika. | Cel<br>• Wszystkie pliki możliwe do skanowania:Uwzględnia wszystkie pliki możliwe do skanowania. Pliki, których nie można przeskanować to pliki chronione hasłem, pliki zaszyfrowane lub pliki wykraczające poza określone przez użytkownika ograniczenia skanowania.<br>• Skanuj pliki skompresowane do warstwy 2: Skanuje pliki skompresowane o 2 warstwie kompresji.<br><br>Wykluczenia<br>• Nie skanuj katalogów, w których zainstalowane są produkty firmy Trend Micro.<br><br>Ustawienia zaawansowane<br>• Zmodyfikuj listę dozwolonych spyware/grayware (tylko w przypadku skanowania antyspyware) |

| INSTRUKCJE I UWAGI | ZALECANE USTAWIENIA SKANOWANIA |
|---|---|
| Aby dostosować ustawienia skanowania dla **programu Messaging Security Agent**, rozwiń agenta i kliknij następujące pozycje:<br>• **Ochrona antywirusowa**: kliknij, aby agent skanował w poszukiwaniu wirusów i innego złośliwego oprogramowania. Patrz sekcja *Cele skanowania i operacje dotyczące programów Messaging Security Agent na stronie 7-20*.<br>• **Filtrowanie zawartości**: kliknij, aby agent skanował pocztę e-mail w poszukiwaniu zabronionej zawartości. Patrz sekcja *Zarządzanie regułami filtrowania zawartości na stronie 6-17*.<br>• **Blokowanie załączników**: kliknij, aby agent skanował pocztę e-mail pod kątem naruszenia reguł załączników. Patrz sekcja *Konfigurowanie blokowania załączników na stronie 6-48*. | • Agent przeprowadza skanowanie w każdą niedzielę od godziny 5:00.<br>• Harmonogram można dostosować do godzin pozaszczytowych klientów. Agent skanuje wszystkie pliki, które można skanować. Podczas skanowania uwzględnia również treści wiadomości e-mail.<br>• Gdy agent wykryje plik zawierający wirusa lub inny złośliwy program, czyści ten plik. Jeśli pliku nie można wyczyścić, jest on zastępowany tekstem lub plikiem.<br>• Gdy agent wykryje plik zawierający trojana lub robaka, zastępuje dany obiekt tekstem lub plikiem.<br>• Gdy agent wykryje plik zawierający program pakujący, zastępuje go tekstem/plikiem.<br>• Agent nie czyści zarażonych plików, które są skompresowane. |

4. Wybierz grupy lub programy Messaging Security Agent, dla których będą stosowane ustawienia skanowania zaplanowanego.

**Uwaga**

Aby wyłączyć skanowanie zaplanowane, usuń zaznaczenie z pola wyboru danej grupy lub programu Messaging Security Agent.

5. Kliknij przycisk **Zapisz**.

# Cele skanowania i operacje dotyczące programów Security Agent

Skonfiguruj następujące ustawienia dla każdego z typów skanowania (skanowanie ręczne, skanowanie zaplanowane, skanowanie w czasie rzeczywistym):

## Karta Cel

Wybór metody:

- **Wszystkie pliki możliwe do skanowania**: Uwzględnia wszystkie pliki możliwe do skanowania. Pliki, których nie można przeskanować to pliki chronione hasłem, pliki zaszyfrowane lub pliki wykraczające poza określone przez użytkownika ograniczenia skanowania.

  **Uwaga**

  Wybranie tej opcji zapewnia najlepszą możliwą ochronę. Jednak skanowanie każdego pliku wymaga wiele czasu oraz zasobów i może być w niektórych sytuacjach nadmiarowe. Dlatego można ograniczyć liczbę plików, które agent ma przeskanować.

- **Funkcja IntelliScan wykorzystuje identyfikację rzeczywistego typu plików**: skanuje pliki na podstawie ich rzeczywistego typu. Patrz sekcja *IntelliScan na stronie D-2*.

- **Skanuj pliki z następującymi rozszerzeniami**: ręczne określenie plików do skanowania na podstawie ich rozszerzeń. Poszczególne wpisy należy oddzielać przecinkami.

Wybierz sposób uruchamiania skanowania:

- **Odczyt**: skanowanie plików, których zawartość zostanie odczytana. Pliki są odczytywane podczas otwierania, uruchamiania, kopiowania lub przenoszenia.

- **Zapisz**: skanowanie plików, których zawartość zostanie zapisana. Pliki są zapisywane podczas modyfikowania, zapisywania zawartości, pobierania lub kopiowania z innej lokalizacji.

- **Odczyt lub zapis**

### Wykluczenia ze skanowania

Można konfigurować następujące ustawienia:

- Włączyć lub wyłączyć wykluczenia
- Wykluczyć ze skanowania katalogi produktów Trend Micro
- Wykluczyć ze skanowania inne katalogi

  Wszystkie podkatalogi w określonej ścieżce zostaną również wykluczone ze skanowania
- Wykluczyć ze skanowania nazwy plików lub nazwy plików z pełną ścieżką
- Pomiń rozszerzenia plików

  Jako rozszerzeń plików nie można używać symboli wieloznacznych, takich jak „*”.

**Uwaga**

(Tylko w wersji Advanced) Jeśli na kliencie jest uruchomiony serwer Microsoft Exchange, firma Trend Micro zaleca wykluczenie ze skanowania wszystkich folderów tego serwera. Aby globalnie wykluczyć ze skanowania wszystkie foldery serwera Microsoft Exchange, wybierz kolejno opcje **Administracja** > **Ustawienia globalne** > **Komputer/serwer {karta}** > **Ogólne ustawienia skanowania**, a następnie zaznacz opcję **Wyklucz foldery serwera Microsoft Exchange, jeśli program jest zainstalowany na serwerze Microsoft Exchange**.

## Ustawienia zaawansowane

| Typ skanowania | Opcja |
|---|---|
| Skanowanie w czasie rzeczywistym | **Skanuj wiadomości POP3**: Domyślnie funkcja skanowania poczty obsługuje tylko nowe wiadomości wysyłane za pośrednictwem portu 110 w folderze wiadomości przychodzących i folderze wiadomości-śmieci. Nie jest obsługiwana poczta POP3 (SSL-POP3).<br>• Microsoft Outlook 2007, 2010 lub 2013<br>• Mozilla Thunderbird w wersji 1.5 lub nowszej<br>Funkcja skanowania poczty nie wykrywa zagrożeń bezpieczeństwa w wiadomościach IMAP. W celu wykrywania zagrożeń bezpieczeństwa i spamu w wiadomościach IMAP należy korzystać z programu Messaging Security Agent (tylko w wersji Advanced). |
| Skanowanie w czasie rzeczywistym, skanowanie ręczne | **Skanuj zmapowane dyski i udostępnione foldery sieciowe**: Wybierz tę opcję, aby skanować katalogi fizycznie znajdujące się na innych komputerach, ale zmapowane na lokalnym. |
| Skanowanie w czasie rzeczywistym | **Skanuj dyskietki podczas zamykania systemu** |
| Skanowanie w czasie rzeczywistym | **Włącz mechanizm IntelliTrap**: mechanizm IntelliTrap wykrywa złośliwy kod, na przykład boty w plikach skompresowanych. Patrz sekcja *IntelliTrap na stronie D-3*. |
| Skanowanie w czasie rzeczywistym | **W pamięci wykryto warianty złośliwego oprogramowania poddanego kwarantannie**: Jeśli włączono funkcję skanowania w czasie rzeczywistym i monitorowania zachowania oraz zaznaczono tę opcję, uruchomiony proces pamięci jest skanowany pod kątem spakowanego złośliwego oprogramowania. Wszelkie spakowane złośliwe oprogramowanie wykryte przez funkcję monitorowania zachowania jest poddawane kwarantannie. |

| Typ skanowania | Opcja |
|---|---|
| Skanowanie w czasie rzeczywistym, skanowanie ręczne, skanowanie zaplanowane | **Skanuj pliki skompresowane do warstwy: __**: W przypadku pliku skompresowanego jest tworzona dodatkowa warstwa na każdą operację kompresji. Jeśli zainfekowany plik został skompresowany kilkakrotnie, w celu uniknięcia infekcji należy przeskanować każdą jego warstwę. Skanowanie wielu warstw wymaga jednak dłuższego czasu i większych zasobów. |
| Skanowanie w czasie rzeczywistym, skanowanie ręczne, skanowanie zaplanowane | **Zmodyfikuj listę dozwolonego oprogramowania spyware/grayware**: Tego ustawienia nie można skonfigurować z poziomu konsoli agenta. |
| Skanowanie ręczne, skanowanie zaplanowane | **Wykorzystanie procesora/Szybkość skanowania**: program Security Agent może wstrzymywać działanie między skanowaniem kolejnych plików.<br><br>Wybierz odpowiednie opcje:<br><br>• **Wysoki**: brak przerw między kolejnymi operacjami skanowania.<br><br>• **Średni**: Wstrzymuje pracę podczas skanowania kolejnych plików, jeśli poziom wykorzystania procesora przekracza 50%; w przeciwnym razie skanuje bez przerw.<br><br>• **Niskie**: wstrzymuje pracę podczas skanowania kolejnych plików, jeśli poziom wykorzystania procesora przekracza 20%. W przeciwnym razie skanuje bez przerw. |
| Skanowanie ręczne, skanowanie zaplanowane | **Uruchom zaawansowane czyszczenie**: program Security Agent zatrzymuje pracę złośliwych programów udających programy zabezpieczające, znanych pod nazwą FakeAV. Agent używa także reguł czyszczenia zaawansowanego, aby aktywnie wykrywać i zatrzymywać aplikacje wykazujące zachowanie oprogramowania FakeAV.<br><br>**Uwaga**<br>Funkcja czyszczenia zaawansowanego zapewnia aktywną ochronę, ale powoduje zgłoszenie dużej liczby fałszywych alarmów. |

## Lista dozwolonego oprogramowania spyware/grayware

Niektóre aplikacje są zaliczane przez programy firmy Trend Micro do spyware/grayware nie z uwagi na szkody powodowane przez nie w systemie, w którym są zainstalowane, lecz dlatego, że mogą one narażać klienta lub sieć na działanie złośliwego oprogramowania lub ataki hakerów.

Oprogramowanie Worry-Free Business Security zawiera listę podejrzanych programów i domyślnie zapobiega ich uruchamianiu na klientach.

Jeśli zajdzie potrzeba uruchomienia na klientach jakiejkolwiek aplikacji zaklasyfikowanej przez firmę Trend Micro jako spyware/grayware, należy dodać jej nazwę do listy dozwolonych programów spyware/grayware.

## Karta Operacja

Programy Security Agent wykonują w odniesieniu do wirusów/złośliwego oprogramowania następujące operacje:

**TABELA 7-1. Operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania**

| AKCJA | OPIS |
|---|---|
| Usuń | Usuwa zarażony plik. |
| Poddaj kwarantannie | Zmienia nazwę zarażonego pliku, a następnie przenosi go do tymczasowego katalogu kwarantanny na kliencie.<br><br>Programy Security Agent wysyłają następnie pliki poddane kwarantannie do wyznaczonego katalogu kwarantanny, który domyślnie znajduje się na serwerze Security Server.<br><br>Program Security Agent szyfruje pliki poddane kwarantannie wysyłane do tego katalogu.<br><br>W przypadku konieczności przywrócenia jakiegokolwiek pliku poddanego kwarantannie należy użyć narzędzia VSEncrypt. |

| Akcja | Opis |
|---|---|
| Wyczyść | Przed zapewnieniem pełnego dostępu do danego pliku agent czyści zarażony plik.<br><br>Jeśli nie można wyczyścić pliku, program Security Agent jako drugą operację wykonuje jedną z poniższych czynności: Poddaj kwarantannie, Usuń, Zmień nazwę i Zezwól.<br><br>Operację można przeprowadzać na wszystkich typach złośliwego oprogramowania z wyjątkiem prawdopodobnego wirusa/złośliwego oprogramowania.<br><br>**Uwaga**<br>Wyczyszczenie niektórych plików jest niemożliwe. Aby uzyskać więcej informacji, zobacz *Pliki, których nie można wyczyścić na stronie D-29*. |
| Zmień nazwę | Zmienia rozszerzenie zainfekowanego pliku na „`vir`”. Użytkownicy początkowo nie mogą otworzyć pliku, którego nazwa została zmieniona; mogą to zrobić po skojarzeniu pliku z aplikacją.<br><br>Wirus/złośliwe oprogramowanie mogą zostać uruchomione podczas otwierania zarażonego pliku o zmienionej nazwie. |
| Pomiń | Operacja wykonywana tylko w przypadku skanowania ręcznego i skanowania zaplanowanego. Ta operacja skanowania nie może być używana podczas skanowania w czasie rzeczywistym, ponieważ niewykonanie żadnej czynności podczas 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 | Operacja wykonywana tylko w przypadku skanowania w czasie rzeczywistym. Po wykryciu przez program Security Agent próby otwarcia lub wykonania zarażonego pliku ta operacja jest natychmiast blokowana.<br><br>Użytkownicy mogą ręcznie usunąć zarażony plik. |

Operacja skanowania wykonywana przez program Security Agent zależy od typu skanowania, podczas którego wykryto oprogramowanie spyware/grayware. Choć możliwe jest skonfigurowanie określonych operacji w odniesieniu do poszczególnych typów wirusów/złośliwego oprogramowania, to w odniesieniu do wszystkich typów

oprogramowania spyware/grayware można skonfigurować tylko jedną operację. Na przykład w przypadku wykrycia przez program Security Agent oprogramowania spyware/grayware podczas skanowania ręcznego (typ skanowania) zagrożone zasoby systemowe zostaną wyczyszczone (operacja).

Program Security Agent wykonuje w odniesieniu do oprogramowania spyware/grayware następujące operacje:

**TABELA 7-2. Operacje skanowania w poszukiwaniu oprogramowania spyware/grayware**

| AKCJA | OPIS |
|---|---|
| Wyczyść | Przerywa procesy lub usuwa pozycje rejestrów, pliki, pliki cookie i skróty. |
| Pomiń | Agent nie wykonuje żadnej operacji na wykrytych składnikach spyware/grayware, ale w dziennikach tworzy wpisy o wykryciu oprogramowania spyware/grayware. Tę operację można wykonać tylko w przypadku skanowania ręcznego i skanowania zaplanowanego. Podczas funkcji Skanowanie w czasie rzeczywistym operacją tą jest „Odmów dostępu”.<br><br>Jeśli wykryte oprogramowanie spyware/grayware znajduje się na liście elementów dozwolonych, program Security Agent nie wykonuje żadnej operacji. |
| Odmów dostępu | Uniemożliwia dostęp (kopiowanie, otwieranie) do wykrytych składników spyware/grayware. Tę operację można wykonać tylko podczas skanowania w czasie rzeczywistym. Podczas skanowania ręcznego i skanowania zaplanowanego wykonywana jest operacja „Pomiń”. |

## ActiveAction

Różne typy wirusów/złośliwego oprogramowania wymagają różnych operacji skanowania. Konfigurowanie operacji skanowania wymaga znajomości wirusów / złośliwego oprogramowania i może być czasochłonnym zadaniem. W celu rozwiązania tych problemów w programie Security Agent zastosowano usługę ActiveAction.

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 urządzeń końcowych przez wirusy/złośliwe oprogramowanie. Ustawienia funkcji ActiveAction są aktualizowane, aby zapewnić ochronę przed najnowszymi zagrożeniami i metodami ataków wirusów/złośliwego oprogramowania.

Poniższa tabela ilustruje sposób działania usługi ActiveAction w odniesieniu do każdego typu wirusa/złośliwego oprogramowania:

**Tabela 7-3. Operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania zalecane przez firmę Trend Micro**

| Typ wirusa/ złośliwego oprogramowania | Skanowanie w czasie rzeczywistym | | Skanowanie ręczne/ Skanowanie zaplanowane | |
|---|---|---|---|---|
| | Pierwsza operacja | Druga operacja | Pierwsza operacja | Druga operacja |
| Program-żart | Poddaj kwarantannie | Usuń | Poddaj kwarantannie | Usuń |
| Programy typu „koń trojański”/ robaki | Poddaj kwarantannie | Usuń | Poddaj kwarantannie | Usuń |
| Narzędzie do kompresji | Poddaj kwarantannie | nd. | Poddaj kwarantannie | nd. |
| Prawdopodobny wirus/złośliwe oprogramowanie | Poddaj kwarantannie | nd. | Pomiń lub operacja skonfigurowana przez użytkownika | nd. |
| Wirus | Wyczyść | Poddaj kwarantannie | Wyczyść | Poddaj kwarantannie |
| Wirus testowy | Odmów dostępu | nd. | nd. | nd. |
| Inne złośliwe oprogramowanie | Wyczyść | Poddaj kwarantannie | Wyczyść | Poddaj kwarantannie |

**Uwagi i przypomnienia:**

- W przypadku prawdopodobnego wirusa/złośliwego oprogramowania domyślana operacja to "Odmów dostępu" podczas skanowania w czasie rzeczywistym lub "Pomiń" podczas skanowania ręcznego i skanowania zaplanowanego. Jeśli nie są to preferowane operacje, można zmienić je na "Poddaj kwarantannie", "Usuń" lub "Zmień nazwę".
- Wyczyszczenie niektórych plików jest niemożliwe. Aby uzyskać więcej informacji, zobacz *Pliki, których nie można wyczyścić na stronie D-29*.
- Usługa ActiveAction nie obsługuje skanowania w poszukiwaniu oprogramowania spyware/grayware.
- Wartości domyślne tych ustawień mogą ulec zmianie po udostępnieniu nowych plików sygnatur.

## Ustawienia zaawansowane

| TYP SKANOWANIA | OPCJA |
|---|---|
| Skanowanie w czasie rzeczywistym, skanowanie zaplanowane | **W przypadku wykrycia wirusa lub oprogramowania spyware wyświetl komunikat ostrzeżenia na komputerze lub serwerze** |
| Skanowanie w czasie rzeczywistym, skanowanie zaplanowane | **W przypadku wykrycia potencjalnego wirusa lub oprogramowania spyware wyświetl komunikat ostrzeżenia na komputerze lub serwerze** |
| Skanowanie ręczne, skanowanie w czasie rzeczywistym, skanowanie zaplanowane | **Uruchom czyszczenie w razie wykrycia potencjalnego wirusa/złośliwego oprogramowania**: Dostępne wyłącznie, jeśli wybierzesz opcję ActiveAction i dostosujesz działanie dla prawdopodobnego wirusa/złośliwego oprogramowania. |

# Cele skanowania i operacje dotyczące programów Messaging Security Agent

Skonfiguruj następujące ustawienia dla każdego z typów skanowania (skanowanie ręczne, skanowanie zaplanowane, skanowanie w czasie rzeczywistym):

Karta **Cel**

- Cele skanowania
- Dodatkowe ustawienia skanowania w poszukiwaniu zagrożeń
- Wykluczenia ze skanowania

Karta **Operacja**

- Operacje skanowania/ActiveAction
- Powiadomienia
- Ustawienia zaawansowane

## Cele skanowania

Wybierz cele skanowania:

- **Wszystkie pliki załączników**: wykluczane są tylko pliki zaszyfrowane lub chronione hasłem.

  **Uwaga**

  Wybranie tej opcji zapewnia najlepszą możliwą ochronę. Jednak skanowanie każdego pliku wymaga wiele czasu oraz zasobów i może być w niektórych sytuacjach nadmiarowe. Dlatego można ograniczyć liczbę plików, które agent ma przeskanować.

- **IntelliScan**: skanuje pliki na podstawie ich rzeczywistego typu. Patrz sekcja *IntelliScan na stronie D-2*.
- **Określone typy plików**: program Worry-Free Business Security będzie skanować wybrane typy plików oraz pliki z wybranymi rozszerzeniami. Poszczególne wpisy należy oddzielać średnikami (;).

Wybór innych opcji:

- **Włącz mechanizm IntelliTrap**: mechanizm IntelliTrap wykrywa złośliwy kod, na przykład boty w plikach skompresowanych. Patrz sekcja *IntelliTrap na stronie D-3*.

- **Skanuj treść wiadomości**: powoduje skanowanie treści wiadomości e-mail, która może zawierać osadzone zagrożenia.

### Dodatkowe ustawienia skanowania w poszukiwaniu zagrożeń

Istnieje możliwość wybrania innych zagrożeń, pod kątem których agent powinien przeprowadzać skanowanie. Szczegółowe informacje o tych zagrożeniach zawiera część *Informacje o zagrożeniach na stronie 1-9*.

Wybór dodatkowych opcji:

- **Przed czyszczeniem utwórz kopię zapasową zarażonego pliku**: program Worry-Free Business Security wykonuje kopię zapasową zagrożenia przed czyszczeniem. Kopia pliku zostanie zaszyfrowana i zapisana w następującym katalogu klienta:

  ```
  <folder instalacji programu Messaging Security Agent>
  \storage\backup
  ```

  Katalog można zmienić w sekcji **Opcje zaawansowane**, podsekcja **Ustawienia kopii zapasowych**.

  Informacje na temat odszyfrowywania plików znajdują się w części *Przywracanie zaszyfrowanych plików na stronie 14-18*.

- **Nie czyść zarażonych skompresowanych plików, aby zoptymalizować wydajność**

### Wykluczenia ze skanowania

Na karcie **Cel** przejdź do sekcji **Wykluczenia** i spośród poniższych opcji wybierz kryteria, których agent będzie używać przy wykluczaniu wiadomości e-mail ze skanowania:

- **Rozmiar treści wiadomości przekracza**: program Messaging Security Agent skanuje wiadomości e-mail tylko wtedy, gdy ich treść ma rozmiar mniejszy lub równy wartości, którą podano.

- **Rozmiar załącznika przekracza**: program Messaging Security Agent skanuje wiadomości e-mail tylko wtedy, gdy ich plik załącznika ma rozmiar mniejszy lub równy wartości, którą podano.

  **Porada**

  Firma Trend Micro zaleca ustawienie ograniczenia na 30 MB.

- **Liczba rozpakowanych plików przekracza**: jeżeli liczba rozpakowanych plików w pliku skompresowanym przekracza tę wartość, program Messaging Security Agent skanuje jedynie pliki mieszczące się w limicie określonym w tej opcji.
- **Rozmiar rozpakowanego pliku przekracza**: program Messaging Security Agent skanuje tylko te pliki skompresowane, które po rozpakowaniu mają rozmiar mniejszy lub równy podanej wartości.
- **Liczba warstw kompresji przekracza**: program Messaging Security Agent skanuje tylko pliki skompresowane mające nie więcej warstw kompresji niż tutaj określono. Przykładowo, jeżeli limit zostanie ustawiony na 5 warstw, program Messaging Security Agent będzie skanował pierwszych 5 warstw skompresowanych plików, jednak pominie pliki skompresowane na 6 lub więcej warstw.
- **Rozmiar rozpakowanego pliku jest „x" razy większy od rozmiaru pliku skompresowanego**: program Messaging Security Agent skanuje pliki skompresowane tylko wtedy, gdy stosunek rozmiaru rozpakowanego pliku do jego rozmiaru w formie skompresowanej jest mniejszy od podanej wartości. Funkcja ta powoduje, że program Messaging Security Agent nie skanuje plików skompresowanych, które mogłyby wywołać atak typu Denial of Service. Ataki typu Denial of Service zdarzają się wtedy, gdy zasoby serwera poczty są zajęte niepotrzebnymi operacjami. Wyłączenie w programie Messaging Security Agent opcji skanowania plików, które po rozpakowaniu są bardzo duże, zapobiega występowaniu tego problemu.

  Przykład: W poniższej tabeli jako wartość „x" podano 100.

| Rozmiar pliku (nieskompresowany) | Rozmiar pliku (nieskompresowany) | Wynik |
|---|---|---|
| 500 KB | 10 KB (współczynnik to 50:1) | Przeskanowano |
| 1 000 KB | 10 KB (współczynnik to 100:1) | Przeskanowano |
| 1 001 KB | 10 KB (współczynnik przekracza 100:1) | Nie przeskanowano * |
| 2000 KB | 10 KB (współczynnik to 200:1) | Nie przeskanowano * |

* Program Messaging Security Agent podejmuje działanie określone dla wykluczonych plików.

## Operacje skanowania

Administratorzy mogą skonfigurować program Messaging Security Agent w taki sposób, aby wykonywał akcje w zależności od typu zagrożenia, jakie niosą wirusy/złośliwe oprogramowanie, trojany i robaki. Jeśli stosowane są operacje niestandardowe, należy określić odpowiednią operację dla każdego typu zagrożenia.

**Tabela 7-4. Niestandardowe operacje programu Messaging Security Agent**

| Akcja | Opis |
|---|---|
| Wyczyść | Usuwa złośliwy kod z treści zarażonych wiadomości i załączników. Pozostała treść wiadomości, niezarażone pliki oraz wyczyszczone pliki są dostarczane do określonych odbiorców. Firma Trend Micro w przypadku wirusów/złośliwego oprogramowania zaleca używanie domyślnej operacji skanowania Wyczyść.<br><br>W niektórych przypadkach program Messaging Security Agent nie może wyczyścić pliku.<br><br>Podczas skanowania ręcznego lub skanowania zaplanowanego program Messaging Security Agent aktualizuje magazyn informacji i zastępuje plik jego wyczyszczoną wersją. |

| Akcja | Opis |
|---|---|
| Zastąp tekstem/ plikiem | Usuwa zarażoną/przefiltrowaną zawartość i zastępuje ją tekstem lub plikiem. Wiadomość e-mail zostaje dostarczona do określonego odbiorcy, ale tekst zastępczy informuje o zarażeniu i zastąpieniu oryginalnej zawartości.<br><br>W przypadku funkcji Filtrowanie zawartości i Zapobieganie utracie danych tekst można zastąpić wyłącznie w treści wiadomości lub w polach załącznika (a nie w polach Od, Do, DW czy Temat). |
| Poddaj całą wiadomość kwarantannie | (Tylko w przypadku skanowania w czasie rzeczywistym) Przeniesiona do katalogu kwarantanny i poddana kwarantannie zostaje tylko zarażona zawartość. Odbiorca otrzymuje wiadomość bez tej zawartości.<br><br>W przypadku funkcji Filtrowanie zawartości, Zapobieganie utracie danych oraz Blokowanie załączników cała wiadomość zostaje przeniesiona do katalogu kwarantanny. |
| Poddaj część wiadomości kwarantannie | (Tylko w przypadku skanowania w czasie rzeczywistym) Przeniesiona do katalogu kwarantanny i poddana kwarantannie zostaje tylko zarażona lub przefiltrowana zawartość. Odbiorca otrzymuje wiadomość bez tej zawartości. |
| Usuń całą wiadomość | (Tylko w przypadku skanowania w czasie rzeczywistym) Usuwana jest cała wiadomość e-mail. Pierwotny odbiorca nie otrzyma wiadomości. |
| Pomiń | Tworzy w dzienniku wirusów wpis o zarażeniu plików złośliwym wirusem, ale nie wykonuje żadnej operacji. Wykluczone, zaszyfrowane lub chronione hasłem pliki są dostarczane do odbiorcy bez aktualizowania dzienników.<br><br>W przypadku funkcji Filtrowanie zawartości wiadomość jest dostarczana w takim stanie, w jakim się znajduje. |
| Archiwizacja | Umieszcza wiadomość w katalogu archiwum i dostarcza ją oryginalnemu odbiorcy. |
| Poddaj wiadomość kwarantannie w folderze spamu na serwerze | Cała wiadomość jest wysyłana na serwer Security Server w celu poddania kwarantannie. |

| Akcja | Opis |
|---|---|
| Poddaj wiadomość kwarantannie w folderze wiadomości typu spam użytkownika | Cała wiadomość jest wysyłana do folderu spamu użytkownika w celu poddania kwarantannie. Folder znajduje się w magazynie informacji po stronie serwera. |
| Oznacz i dostarcz | Do informacji nagłówka wiadomości e-mail dodawany jest znacznik, który identyfikuje tę wiadomość jako spam, a następnie dostarcza ją do określonego odbiorcy. |

Oprócz tych operacji można również skonfigurować następujące:

- **Włącz operację jako reakcję na działanie typu „mass mailing”**: umożliwia wybranie opcji Wyczyść, Zastąp tekstem/plikiem, Usuń całą wiadomość, Pomiń lub Poddaj kwarantannie część wiadomości w przypadku zagrożeń typu „mass-mailing”.
- **Wykonaj tę operację, jeśli czyszczenie się nie powiodło**: należy wybrać dodatkową operację dla nieudanych prób czyszczenia. Możliwe jest wybranie opcji Zastąp tekstem/plikiem, Usuń całą wiadomość, Pomiń lub Poddaj kwarantannie część wiadomości.

### ActiveAction

Poniższa tabela ilustruje sposób działania usługi ActiveAction w odniesieniu do każdego typu wirusa/złośliwego oprogramowania:

**Tabela 7-5. Operacje skanowania w poszukiwaniu wirusów/złośliwego oprogramowania zalecane przez firmę Trend Micro**

| Typ wirusa/ złośliwego oprogramowania | Skanowanie w czasie rzeczywistym | | Skanowanie ręczne/ Skanowanie zaplanowane | |
|---|---|---|---|---|
| | Pierwsza operacja | Druga operacja | Pierwsza operacja | Druga operacja |
| Wirus | Wyczyść | Usuń całą wiadomość | Wyczyść | Zastąp tekstem/ plikiem |

| Typ wirusa/ złośliwego oprogramowania | Skanowanie w czasie rzeczywistym | | Skanowanie ręczne/ Skanowanie zaplanowane | |
|---|---|---|---|---|
| | Pierwsza operacja | Druga operacja | Pierwsza operacja | Druga operacja |
| Programy typu „koń trojański”/ robaki | Zastąp tekstem/ plikiem | nd. | Zastąp tekstem/ plikiem | nd. |
| Narzędzie do kompresji | Poddaj część wiadomości kwarantannie | nd. | Poddaj część wiadomości kwarantannie | nd. |
| Inny złośliwy kod | Wyczyść | Usuń całą wiadomość | Wyczyść | Zastąp tekstem/ plikiem |
| Inne zagrożenia | Poddaj część wiadomości kwarantannie | nd. | Zastąp tekstem/ plikiem | nd. |
| Zachowanie typu „mass-mailing” | Usuń całą wiadomość | nd. | Zastąp tekstem/ plikiem | nd. |

### Powiadomienia o operacjach skanowania

Wybierz polecenie **Powiadom odbiorców**, aby program Messaging Security Agent powiadamiał odbiorców o wykonywaniu operacji w odniesieniu do określonych wiadomości e-mail. Użytkownik może z różnych powodów chcieć uniknąć powiadamiania zewnętrznych odbiorców poczty o zablokowaniu wiadomości zawierającej poufne informacje. Aby wysłać powiadomienia wyłącznie do wewnętrznych odbiorców poczty, wybierz opcję **Nie powiadamiaj odbiorców zewnętrznych**. Zdefiniuj adresy wewnętrzne, używając opcji **Operacje** > **Ustawienia powiadamiania** > **Definicja poczty wewnętrznej**.

Można także wyłączyć wysyłanie powiadomień do odbiorców zewnętrznych, którzy podszywają się pod nadawców.

## Ustawienia zaawansowane (operacje skanowania)

| USTAWIENIA | SZCZEGÓŁY |
|---|---|
| Makra | Wirusy makr to wirusy zależne od aplikacji, które zarażają narzędzia w postaci makropoleceń towarzyszące aplikacjom. Funkcja zaawansowanego skanowania makr korzysta z technologii skanowania heurystycznego w celu wykrywania wirusów makr lub usuwania wszystkich wykrytych kodów makr. Skanowanie heurystyczne to metoda badawcza wykrywania wirusów, która wykorzystuje rozpoznawanie sygnatur i technologie oparte na regułach do wyszukiwania złośliwego kodu makr. Metoda ta sprawdza się najlepiej przy wykrywaniu nieznanych wirusów i zagrożeń, dla których nie istnieją jeszcze sygnatury wirusów.<br><br>Program Messaging Security Agent wykonuje względem złośliwego kodu makr skonfigurowaną operację.<br><br>• **Poziom skanowania heurystycznego**<br>  • Na poziomie 1 używane są najbardziej szczegółowe kryteria, lecz wykrywana jest najmniejsza liczba kodów makr.<br>  • Poziom 4 umożliwia wykrywanie największej liczby kodów makr, ale używane są najmniej szczegółowe kryteria, przez co istnieje możliwość błędnego zidentyfikowania bezpiecznego kodu makra jako przenoszącego złośliwy kod.<br><br>**Porada**<br>Firma Trend Micro zaleca stosowanie skanowania heurystycznego na poziomie 2. Poziom ten zapewnia wysoki współczynnik wykrywalności nieznanych wirusów makr, dużą szybkość skanowania i wykorzystuje tylko reguły konieczne do sprawdzania ciągów charakterystycznych dla wirusów makr. Poziom 2 cechuje się także najniższym współczynnikiem błędnego identyfikowania złośliwego kodu w bezpiecznym kodzie makra.<br><br>• **Usuń wszystkie makra wykryte przez funkcję zaawansowanego skanowania makr**: usuwa wszystkie kody makr wykryte w skanowanych plikach. |

| Ustawienia | Szczegóły |
|---|---|
| Części wiadomości, których nie można przeskanować | Ustaw operację i warunek powiadamiania w przypadku plików zaszyfrowanych i/lub zabezpieczonych hasłem. Jako operację można wybrać: Zastąp tekstem/plikiem, Poddaj kwarantannie całą wiadomość, Usuń całą wiadomość, Pomiń lub Poddaj kwarantannie część wiadomości. |
| Części wiadomości, które zostały wykluczone | Ustaw operację i warunek powiadamiania w przypadku części wiadomości, które zostały wykluczone. Jako operację można wybrać: Zastąp tekstem/plikiem, Poddaj kwarantannie całą wiadomość, Usuń całą wiadomość, Pomiń lub Poddaj kwarantannie część wiadomości. |
| Ustawienia kopii zapasowych | Miejsce zapisu kopii zapasowych zarażonych plików przed wyczyszczeniem ich przez agenta. |
| Ustawienia zastępowania | Skonfiguruj tekst i plik dla tekstu zastępczego. Jeśli skonfigurowana operacja to **zastąp tekstem/plikiem**, program Worry-Free Business Security zastąpi zagrożenie tym tekstem lub plikiem. |

# Rozdział 8

# Zarządzanie aktualizacjami

W tym rozdziale opisano składniki programu Worry-Free Business Security i procedury aktualizacji.

# Omówienie aktualizacji

Wszystkie aktualizacje składników są inicjowane przez serwer Trend Micro ActiveUpdate Server. Gdy aktualizacje są dostępne, serwer Security Server pobiera zaktualizowane składniki, a następnie rozpowszechnia je wśród programów Security Agent i Messaging Security Agent (tylko w wersji Advanced).

Jeśli serwer Security Server zarządza dużą liczbą programów Security Agent, proces aktualizacji może pochłaniać znaczną ilość zasobów komputera serwera, obniżając jego stabilność i wydajność. Aby rozwiązać ten problem, w programie Worry-Free Business Security udostępniono funkcję **Agent aktualizacji**, która umożliwia wyznaczonym programom Security Agent rozpowszechnianie aktualizacji na inne programy Security Agent.

W poniższej tabeli wymieniono opcje aktualizacji składników serwera Security Server i jego agentów oraz zalecenia dotyczące ich stosowania:

**TABELA 8-1. Opcje aktualizacji**

| SEKWENCJA AKTUALIZACJI | OPIS | ZALECENIE |
|---|---|---|
| 1. Serwer ActiveUpdate Server czy niestandardowe źródło aktualizacji<br>2. Program Security Server<br>3. Agenty | Program Trend Micro Security Server pobiera zaktualizowane składniki z serwera ActiveUpdate lub z niestandardowego źródła aktualizacji, a następnie wdraża je bezpośrednio na agentach (programach Security Agent oraz Messaging Security Agent). | Metody tej należy użyć, jeżeli między serwerem Security Server a agentami nie ma segmentów sieci o niskiej przepustowości. |

| Sekwencja aktualizacji | Opis | Zalecenie |
|---|---|---|
| 1. Serwer ActiveUpdate Server czy niestandardowe źródło aktualizacji<br>2. Program Security Server<br>3. Agenty aktualizacji, programy Messaging Security Agent, programy Security Agent bez agentów aktualizacji<br>4. Wszystkie inne programy Security Agent | Program Trend Micro Security Server otrzymuje zaktualizowane składniki z serwera ActiveUpdate lub z niestandardowego źródła aktualizacji, a następnie wdraża je bezpośrednio na następujących agentach:<br>• Agenty aktualizacji<br>• Messaging Security Agent<br>• Programy Security Agent bez agentów aktualizacji<br>Następnie agenty aktualizacji wdrażają składniki w ramach odpowiednich programów Security Agent. Jeśli te programy Security Agent nie są w stanie się zaktualizować, aktualizacja jest przeprowadzana bezpośrednio z serwera Security Server. | Jeśli między serwerem Security Server a programami Security Agent występują segmenty sieci o niskiej przepustowości, należy zastosować tę metodę w celu zrównoważenia obciążenia w sieci. |
| 1. Serwer ActiveUpdate<br>2. Security Agent | Programy Security Agent, które nie mogą zostać zaktualizowane za pomocą żadnego źródła aktualizacji bezpośrednio z serwera ActiveUpdate.<br>**Uwaga**<br>Programy Messaging Security Agent nigdy nie są aktualizowane bezpośrednio za pomocą serwera ActiveUpdate. W razie niedostępności wszystkich zasobów program Messaging Security Agent przerywa proces aktualizacji. | Ten mechanizm jest stosowany wyłącznie w ostateczności i wymaga wykonania poniższej czynności:<br>W obszarze Aktualizuj uprawnienia włącz opcję **Korzystaj z serwera Trend Micro ActiveUpdate jako z pomocniczego źródła aktualizacji** |

# Składniki, które można aktualizować

Oprogramowanie Worry-Free Business Security wykorzystuje składniki w celu ochrony agentów przed najnowszymi zagrożeniami. Należy zapewnić aktualność tych składników, aktualizując je ręcznie lub konfigurując harmonogram aktualizacji.

Listę komponentów można wyświetlić, wykonując następujące czynności:

- Przejdź do menu **Aktualizacje** > **Ręczna**.
- Przejdź do menu **Stan aktywności** i kliknij **Sprawdź stan składnika** na widgecie Status agenta.

W poniższej tabeli wymieniono składniki pobierane przez program Security Server z serwera ActiveUpdate:

**TABELA 8-2. Składniki Messaging (tylko w wersji Advanced)**

| SKŁADNIK | ROZPOWSZECHNIANIE | OPIS |
|---|---|---|
| Sygnatura antyspamowa programu Messaging Security Agent | Messaging Security Agent | Sygnatura antyspamowa identyfikuje najnowszy spam w wiadomościach e-mail oraz załącznikach do wiadomości e-mail. |
| Silnik antyspamowy programu Messaging Security Agent, 32-bitowy/64-bitowy | Messaging Security Agent | Silnik antyspamowy wykrywa spam w wiadomościach e-mail oraz załącznikach do wiadomości e-mail. |
| Silnik skanowania programu Messaging Security Agent, 32-bitowy/64-bitowy | Messaging Security Agent | Silnik skanowania wykrywa robaki internetowe, ataki typu „mass-mailing”, trojany, witryny phishingowe, spyware, zagrożenia sieciowe oraz wirusy w wiadomościach e-mail i załącznikach do wiadomości e-mail. |

| Składnik | Rozpowszechnianie | Opis |
|---|---|---|
| Silnik filtrowania adresów URL programu Messaging Security Agent, 32-bit/64-bit | Messaging Security Agent | Silnik filtrowania adresów URL umożliwia komunikację pomiędzy programem Worry-Free Business Security 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 Worry-Free Business Security. |

**Tabela 8-3. Ochrona antywirusowa i funkcja Smart Scan**

| Składnik | Rozpowszechnianie | Opis |
|---|---|---|
| Sygnatura wirusów | Security Agent korzystający z funkcji tradycyjnego skanowania | Sygnatura wirusów zawiera informacje ułatwiające Security Agent 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. |
| Sygnatura IntelliTrap | Security Agent | Sygnatura IntelliTrap służy do wykrywania plików wykonywalnych kompresowanych w czasie rzeczywistym.<br><br>Aby uzyskać więcej informacji, zobacz *IntelliTrap na stronie D-3*. |
| Sygnatura wyjątków IntelliTrap | Security Agent | Sygnatura wyjątków IntelliTrap zawiera listę „dozwolonych” plików skompresowanych. |

| Składnik | Rozpowszechnianie | Opis |
|---|---|---|
| Silnik skanowania antywirusowego, 32-bitowe/64-bitowe | Security Agent | 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.<br><br>Zamiast skanowania każdego bitu w każdym pliku silnik i plik sygnatur uzupełniają się w celu zidentyfikowania następujących elementów:<br><br>• Cech wyróżniających kod wirusa<br>• Precyzyjnej lokalizacji wirusa w pliku |

| Składnik | Rozpowszechnianie | Opis |
|---|---|---|
| Sygnatury Smart Scan | Nie jest rozsyłana do Security Agent. Ta sygnatura pozostaje na serwerze Security Server i jest używana przy wysyłaniu odpowiedzi na żądania skanowania ze strony Security Agent. | W trybie skanowania Smart Scan agenci Security Agent 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.<br><br>**Sygnatury Smart Scan** zawiera większość definicji sygnatur. **Sygnatura agenta usługi Smart Scan** zawiera wszystkie inne definicje sygnatur, których nie ma w sygnaturze Smart Scan.<br><br>Program Security Agent skanuje klienta pod kątem zagrożeń bezpieczeństwa, korzystając z **Sygnatura agenta usługi Smart Scan**. Security Agent, którzy podczas skanowania nie są w stanie określić, czy plik stanowi zagrożenie, sprawdzają to, wysyłając żądanie skanowania do usługi Scan Server obsługiwanej przez serwer Security Server. Usługa Scan Server sprawdza zagrożenie, korzystając z **Sygnatury Smart Scan**. Security Agent umieszcza wynik żądania skanowania uzyskany od serwera skanowania w pamięci podręcznej w celu zwiększenia wydajności skanowania. |
| Sygnatura agenta usługi Smart Scan | Security Agent korzystający z funkcji Smart Scan | |
| Szablon usługi Usuwania Szkód | Security Agent | Szablon usługi Usuwania Szkód, używany w Silnik usługi Usuwania Szkód, pomaga w identyfikacji plików i procesów trojanów oraz umożliwia ich eliminację. |
| Silnik usługi Usuwania Szkód (32-bitowy/64-bitowy) | Security Agent | Silnik usługi Usuwania Szkód służy do wykrywania i usuwania trojanów oraz ich procesów. |

| Składnik | Rozpowszechnianie | Opis |
|---|---|---|
| Sygnatura kontroli pamięci | Security Agent | Ta technologia zapewnia rozszerzone skanowanie wirusów pod kątem wirusów wielopostaciowych i zmutowanych, a także zwiększa liczbę skanowań opartych na sygnaturach wirusów poprzez emulowanie uruchamiania plików. Następnie wyniki są analizowane w kontrolowanym środowisku z niewielkim wpływem na wydajność systemu w celu uzyskania dowodów na złośliwe zamiary. |
| Silnik analizy kontekstowej (32/64 bity) | Security Agent | 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 | Security Agent | Sygnatura analizy kontekstowej zawiera listę dozwolonych zachowań, które nie odnoszą się do żadnych znanych zagrożeń. |
| Mechanizm obsługi zapytań analizy kontekstowej (32/64 bity) | Security Agent | 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) | Security Agent | Silnik skanowania w poszukiwaniu zagrożeń zaawansowanych wyodrębnia cechy sporadycznie występujących plików i wysyła informacje do silnika przewidującego uczenia maszynowego. |
| Wzorzec korelacji zagrożeń zaawansowanych | Security Agent | Wzorzec korelacji zagrożeń zaawansowanych zawiera listę cech plików, które nie odnoszą się do żadnych znanych zagrożeń. |

| Składnik | Rozpowszechnianie | Opis |
|---|---|---|
| Sterownik wczesnego czystego rozruchu (32/64-bitowe) | Security Agent | 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. |

**Tabela 8-4. Ochrona antyszpiegowska**

| Składnik | Rozpowszechnianie | Opis |
|---|---|---|
| Silnik skanowania w poszukiwaniu oprogramowania spyware/grayware v. 6 (32-bitowy/64-bitowy) | Security Agent | Silnik skanowania spyware/grayware skanuje w poszukiwaniu oprogramowania spyware/grayware i przeprowadza odpowiednie operacje skanowania. |
| Sygnatura oprogramowania spyware/grayware v. 6 | Security Agent | Sygnatura oprogramowania spyware/grayware identyfikuje oprogramowanie spyware/grayware w plikach i programach, modułach pamięci, rejestrze systemu Windows i skrótach URL. |
| Sygnatura spyware/grayware | Security Agent | |

**Tabela 8-5. Wirus sieciowy**

| Składnik | Rozpowszechnianie | Opis |
|---|---|---|
| Ogólna sygnatura zapory | Security Agent | Podobnie jak sygnatura wirusa, ogólna sygnatura zapory ułatwia agentom identyfikację sygnatury wirusów — unikatowe sygnatury bitów i bajtów, które sygnalizują obecność wirusa sieciowego. |

**Tabela 8-6. Monitorowanie zachowania i Kontrola urządzeń**

| Składnik | Rozpowszechnianie | Opis |
|---|---|---|
| Sygnatura wykrywania funkcji Monitorowanie zachowania (32-bitowa/64-bitowa) | Security Agent | Ta sygnatura zawiera reguły służące do wykrywania podejrzanego zachowania. |
| Sterowniki głównego monitora zachowań, 32-bit/64-bit | Security Agent | Sterownik pracujący w trybie jądra, który służy do monitorowania zachowania systemowych i przekazuje informacje o nich do głównej usługi monitorowania zachowania w celu wymuszenia realizacji zasad. |
| Główna usługa monitorowania zachowania, wersja 32-bitowa/64-bitowa | Security Agent | Ta pracująca w trybie użytkownika usługa zapewnia następujące funkcje:<br>• Wykrywanie rootkitów<br>• Sterowanie dostępem do urządzeń zewnętrznych<br>• Ochrona plików, kluczy rejestru i usług |
| Sygnatura konfiguracji monitorowania zachowania | Security Agent | Sterownik monitorowania zachowania używa sygnatury do identyfikacji normalnych zachowań systemu i wyłączenia ich z wymuszania realizacji zasad. |
| Sygnatura przywracania po uszkodzeniach | Security Agent | Sygnatura przywracania po uszkodzeniach zawiera reguły służące do monitorowania podejrzanego zachowania. |
| Sygnatura podpisu cyfrowego | Security Agent | Sygnatura z listą poprawnych podpisów cyfrowych używanych przez główną usługę monitorowania zachowania w celu określenia, czy program odpowiedzialny za zdarzenie systemowe jest bezpieczny. |

| Składnik | Rozpowszechnianie | Opis |
|---|---|---|
| Sygnatura stosowania zasad | Security Agent | Usługa główna funkcji Monitorowanie zachowania służy do analizy zdarzeń systemowych w kontekście reguł sygnatury. |
| Sygnatura Memory Scan Trigger Pattern (32/64-bitowe) | Security Agent | Usługa wywoływania skanowania pamięci uruchamia inne silniki skanowania po wykryciu rozpakowania procesu w pamięci. |
| Sygnatura monitorowania inspekcji programów | Security Agent | Sygnatura monitorowania inspekcji programów monitoruje i zapisuje punkty inspekcji, które służą do monitorowania zachowania. |

**Tabela 8-7. Wykorzystanie przeglądarki**

| Składnik | Rozpowszechnianie | Opis |
|---|---|---|
| Sygnatura zapobiegania wykorzystaniu przeglądarki | Security Agent | Ta sygnatura rozpoznaje najnowsze przypadki wykorzystania przeglądarki i zapobiega ich użyciu zagrażającemu przeglądarce. |
| Ujednolicona sygnatura analizatora skryptów | Security Agent | Ta sygnatura analizuje skrypty w stronach internetowych i rozpoznaje złośliwe skrypty. |

## 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:

- *Poprawka krytyczna na stronie D-2*
- *Pakiet Hot Fix na stronie D-2*

- *Poprawka na stronie D-10*
- *Dodatek Service Pack na stronie D-27*

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.

# Aktualizacje serwera Security Server

## Aktualizacje automatyczne

Serwer Security Server automatycznie wykonuje następujące aktualizacje:

- Bezpośrednio po zainstalowaniu serwer Security Server przeprowadza aktualizację, korzystając z serwera Trend Micro ActiveUpdate.
- Po każdym uruchomieniu się serwer Security Server aktualizuje składniki.
- Domyślnie zaplanowane aktualizacje są uruchamiane co godzinę (częstotliwość aktualizacji można zmienić za pomocą konsoli internetowej).

## Aktualizacje ręczne

Jeśli konieczne jest pilne przeprowadzenie aktualizacji, za pomocą konsoli internetowej można uruchomić aktualizacje ręczne.

## Przypomnienia i wskazówki dotyczące aktualizacji serwera

- Po zaktualizowaniu serwer Security Server automatycznie rozsyła aktualizacje składników do agentów. Szczegółowe informacje na temat składników rozsyłanych do agentów zawiera temat *Składniki, które można aktualizować na stronie 8-4*.
- Serwer Security Server wykorzystujący wyłącznie protokół IPv6 nie może wykonywać następujących zadań:

- Pobierać aktualizacji bezpośrednio z serwera Trend Micro ActiveUpdate lub niestandardowego źródła aktualizacji wykorzystującego wyłącznie protokół IPv4.
- Rozsyłać aktualizacji bezpośrednio do agentów wykorzystujących wyłącznie protokół IPv4.

Analogicznie serwer Security Server wykorzystujący wyłącznie protokół IPv4 nie może pobierać aktualizacji z niestandardowego źródła aktualizacji wykorzystującego wyłącznie protokół IPv6 ani rozsyłać aktualizacji bezpośrednio do agentów wykorzystujących wyłącznie protokół IPv6.

W takich sytuacjach, aby umożliwić serwerowi Security Server pobieranie i rozsyłanie aktualizacji, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP (np. DeleGate).

- Jeśli do łączenia z Internetem używany jest serwer proxy, użyj właściwych ustawień serwera proxy na karcie **Administracja** > **Ustawienia globalne** > **Proxy**, aby pomyślnie pobrać aktualizacje.

### Duplikacja składników

Firma Trend Micro regularnie publikuje nowe wersje plików sygnatur, aby zapewnić klientom stałą ochronę. Ponieważ aktualizacje pliku sygnatur są udostępniane regularnie, serwer Security Server używa mechanizmu zwanego **duplikowaniem składników**, który umożliwia szybsze pobieranie plików sygnatur.

Kiedy najnowsza wersja kompletnego pliku sygnatur jest dostępna do pobrania z serwera Trend Micro ActiveUpdate, dostępne są również przyrostowe pliki 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 generowany podczas pobierania najnowszego wzorca sygnatur, serwer Security Server przeprowadza duplikację składników, czyli stosuje metodę aktualizacji składników, w której serwer pobiera jedynie przyrostowe wzorce sygnatur. Aby korzystać z procedury duplikowania składników, należy regularnie

aktualizować serwer Security Server. W przeciwnym razie serwer będzie musiał pobierać pełny plik wzorca sygnatur.

Procedura duplikacji dotyczy następujących składników:

- Sygnatura wirusów
- Sygnatura agenta usługi Smart Scan
- Szablon usług Damage Cleanup
- Sygnatura wyjątków IntelliTrap
- Sygnatury spyware

## Konfigurowanie źródła aktualizacji serwera Security Server

### Przed rozpoczęciem

Domyślnie serwer Security Server pobiera aktualizacje z serwera Trend Micro ActiveUpdate. Określ niestandardowe źródło aktualizacji, jeśli serwer Security Server nie może połączyć się bezpośrednio z serwerem ActiveUpdate.

- Jeśli jako źródło wybrano serwer **Trend Micro ActiveUpdate**, należy się upewnić, że serwer Security Server ma dostęp do Internetu oraz, jeśli używany jest serwer proxy, sprawdzić, czy przy obecnych ustawieniach proxy można nawiązać połączenie z Internetem. Aby uzyskać więcej informacji, zobacz *Konfigurowanie ustawień serwera proxy w sieci Internet na stronie 11-3*.
- Jeśli jako źródło wybrano niestandardowe źródło aktualizacji (**Lokalizacja kopii bieżącego pliku w sieci intranet** lub **Alternatywne źródło aktualizacji**), należy skonfigurować dla tego źródła aktualizacji odpowiednie środowisko i zasoby na potrzeby aktualizacji. Należy się również upewnić, że połączenie między serwerem Security Server a źródłem aktualizacji działa prawidłowo. W przypadku konieczności uzyskania pomocy dotyczącej konfigurowania źródła aktualizacji należy się skontaktować z dostawcą obsługi technicznej.
- Server Security Server wykorzystujący wyłącznie protokół IPv6 nie może wykonywać aktualizacji bezpośrednio z serwera Trend Micro ActiveUpdate ani innego niestandardowego źródła aktualizacji wykorzystującego wyłącznie protokół

IPv4. Analogicznie serwer Security Server wykorzystujący wyłącznie protokół IPv4 nie może wykonywać aktualizacji bezpośrednio z niestandardowych źródeł aktualizacji wykorzystujących wyłącznie protokół IPv6. Aby umożliwić serwerowi Security Server nawiązanie połączenia ze źródłami aktualizacji, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP (np. DeleGate).

**Procedura**

1. Przejdź do pozycji **Aktualizacje** > **Źródło**.
2. Na karcie **Serwer** wybierz źródło aktualizacji.
   - **Serwer Trend Micro ActiveUpdate Server**
   - **Lokalizacja kopii bieżącego pliku w sieci Intranet**: Podaj ścieżkę do źródła w formacie UNC (Universal Naming Convention), na przykład `\\Web\ActiveUpdate`. Podaj również dane do logowania (nazwę użytkownika i hasło), których serwer Security Server będzie używać, by połączyć się z danym źródłem.
   - **Alternatywne źródło aktualizacji**: Wpisz adres URL tego źródła. Sprawdź, czy docelowy wirtualny katalog HTTP (udział w sieci Web) jest dostępny dla serwera Security Server.
3. Kliknij przycisk **Zapisz**.

## Ręczna aktualizacja serwera Security Server

Składniki przechowywane na serwerze Security Server należy ręcznie aktualizować po zainstalowaniu lub uaktualnieniu serwera oraz każdorazowo w przypadku epidemii.

**Procedura**

1. Aktualizację ręczną można rozpocząć na dwa sposoby:
   - Przejdź do menu **Aktualizacje** > **Ręczna**.

- Przejdź do menu **Stan aktywności** i kliknij **Sprawdź stan składnika** na widgecie Status agenta.

Pojawi się ekran **Ręcznej aktualizacji**.

2. Wybierz składniki do zaktualizowania.

   Szczegółowe informacje na temat składników zawiera sekcja *Składniki, które można aktualizować na stronie 8-4*.

3. Kliknij polecenie **Aktualizuj teraz**.

   Wyświetlony zostanie nowy ekran informujący o stanie aktualizacji. W przypadku pomyślnego zakończenia aktualizacji program Security Server automatycznie rozsyła zaktualizowane składniki do agentów.

## Konfigurowanie zaplanowanych aktualizacji serwera Security Server

Program Security Server można skonfigurować do okresowego sprawdzania źródła aktualizacji i automatycznego pobierania dostępnych aktualizacji. Korzystanie z zaplanowanej aktualizacji to wygodny i skuteczny sposób zapewniania stale aktualnej ochrony przed zagrożeniami.

Firma Trend Micro szybko reaguje na epidemie wirusów/złośliwego oprogramowania, uaktualniając pliki sygnatur wirusów (aktualizacje mogą być wydawane kilka razy w tygodniu). Silnik skanowania oraz inne składniki są również uaktualniane regularnie. Firma Trend Micro zaleca aktualizowanie składników codziennie — a podczas epidemii jeszcze częściej — aby agent korzystał z jak najbardziej aktualnych składników.

**Ważne**

Nie należy planować skanowania i przeprowadzania aktualizacji w tym samym czasie. Może to spowodować nieoczekiwane zakończenie skanowania zaplanowanego.

**Procedura**

1. Przejdź do pozycji **Aktualizacje** > **Zaplanowane**.

2. Wybierz składniki do zaktualizowania.

   Szczegółowe informacje na temat składników zawiera sekcja *Składniki, które można aktualizować na stronie 8-4*.

3. Kliknij kartę **Harmonogram**, a następnie ustal harmonogram aktualizacji.

   - Ustawienie **Aktualizacje skanowania standardowego** obejmuje wszystkie składniki z wyjątkiem sygnatur Smart Scan Pattern oraz Sygnatura agenta usługi Smart Scan. Zdecyduj, czy aktualizacje mają być przeprowadzane codziennie, co tydzień czy co miesiąc, a następnie podaj wartość dla opcji **Aktualizuj przez okres**, oznaczającej zakres godzinowy, w którym serwer Security Server będzie przeprowadzać aktualizacje. Serwer Security Server przeprowadza aktualizacje w dowolnym podanym czasie w tym okresie.

     **Uwaga**

     W przypadku zaplanowania aktualizacji w odstępach miesięcznych (niezalecane), jeśli po wybraniu liczby dni (31, 30 lub 29) okaże się, że dany miesiąc ma mniej dni, aktualizacja nie zostanie w tym miesiącu przeprowadzona.

   - Ustawienie **Aktualizacje usługi Smart Scan** obejmuje tylko sygnatury Smart Scan Pattern oraz Sygnatura agenta usługi Smart Scan. Jeśli żaden z agentów nie korzysta z usługi Smart Scan, zignoruj ten element.

4. Kliknij przycisk **Zapisz**.

## Wycofywanie składników

Wycofywanie dotyczy przywracania poprzedniej wersji Sygnatury wirusa, sygnatura agenta usługi Smart Scan oraz Silnika skanowania antywirusowego. Jeśli składniki te nie funkcjonują prawidłowo, należy przywrócić ich poprzednie wersje. Program Security Server umożliwia zachowanie bieżącej i wcześniejszych wersji silnika skanowania antywirusowego oraz trzech ostatnich wersji sygnatury wirusów i sygnatury agenta usługi Smart Scan.

**Uwaga**

Można wycofać tylko składniki wymienione powyżej.

Program Worry-Free Business Security używa różnych silników skanowania dla agentów wykorzystujących platformy 32- i 64-bitowe. Silniki te należy wycofać oddzielnie. Procedura wycofywania wszystkich typów silników skanowania jest jednakowa.

**Procedura**

1. Przejdź do pozycji **Aktualizacje** > **Wycofywanie**.
2. Kliknij polecenie **Synchronizuj** odnoszące się do danego składnika w celu powiadomienia agentów, aby zsynchronizowały swoje wersje składnika na serwerze.
3. Kliknij polecenie **Wycofaj** odnoszące się do danego składnika, aby przywrócić jego wcześniejszą wersję zarówno w programie Security Server, jak i w agentach.

# Aktualizacje programów Security Agent i Messaging Security Agent

## Aktualizacje automatyczne

Programy Security Agent i Messaging Security Agent (tylko w wersji Advanced) automatycznie wykonują następujące aktualizacje:

- Zaraz po instalacji agenty przeprowadzają aktualizację przy użyciu programu Security Server.
- Po każdym zakończeniu aktualizacji program Security Server automatycznie rozsyła aktualizacje do agentów.
- Po każdym zakończeniu aktualizacji agent aktualizacji automatycznie rozsyła aktualizacje do odpowiednich programów Security Agent.
- Domyślnie zaplanowane aktualizacje uruchamiane są:
  - co 8 godzin w przypadku programów Security Agent w siedzibie firmy,
  - co 2 godziny w przypadku programów Security Agent poza siedzibą firmy.

- Domyślnie program Messaging Security Agent przeprowadza aktualizację zaplanowaną co 24 godziny o godzinie 12:00.

## Uruchamianie aktualizacji ręcznej

Program Security Agent otrzymuje zaktualizowane składniki od serwera Security Server.

Można uruchomić aktualizację ręcznie w przypadku chwilowego odłączenia od sieci firmy lub w razie nagłej potrzeby pobrania najnowszych rozwiązań zabezpieczających przed zagrożeniami (na przykład po epidemii).

Jeżeli do łączenia z Internetem używany jest serwer proxy, należy sprawdzić prawidłowość jego ustawień.

**Procedura**

1. Otwórz konsolę główną i kliknij polecenie **Aktualizuj**.

   **Uwaga**

   Aktualizację ręczną można także uruchomić, klikając prawym przyciskiem myszy ikonę programu Security Agent na pasku zadań systemu Windows, a następnie wybierając polecenie **Aktualizuj teraz**.

2. Po ukończeniu aktualizacji kliknij przycisk **Zamknij**.

## Przypomnienia i wskazówki dotyczące aktualizacji agentów

- Programy Security Agent pobierają aktualizacje z programu Security Server, agentów aktualizacji lub serwera Trend Micro ActiveUpdate.

  Programy Messaging Security Agent pobierają aktualizacje tylko z programu Security Server.

  Szczegółowe informacje na temat procesu aktualizacji zawiera część *Omówienie aktualizacji na stronie 8-2*.

- Agent wykorzystujący wyłącznie protokół IPv6 nie może pobierać aktualizacji z programu Security Server, agenta aktualizacji ani serwera Trend Micro ActiveUpdate, jeśli obsługują one wyłącznie protokół IPv4.

  Analogicznie agent wykorzystujący wyłącznie protokół IPv4 nie może pobierać aktualizacji z programu Security Server ani agenta aktualizacji, jeśli wykorzystują one tylko protokół IPv6.

  Aby w takich sytuacjach umożliwić agentom pobieranie aktualizacji, wymagany jest serwer proxy z dwoma stosami, który umożliwia konwersję adresów IP (np. DeleGate).

- Szczegółowe informacje na temat składników aktualizowanych przez agenty zawiera część *Składniki, które można aktualizować na stronie 8-4*.

- Oprócz tych składników podczas pobierania aktualizacji z programu Security Server agenty otrzymują także zaktualizowane pliki konfiguracyjne. Pliki konfiguracyjne są potrzebne, aby można było zastosować nowe ustawienia agentów. Pliki konfiguracyjne zmieniają się po każdej modyfikacji ustawień agentów za pomocą konsoli internetowej.

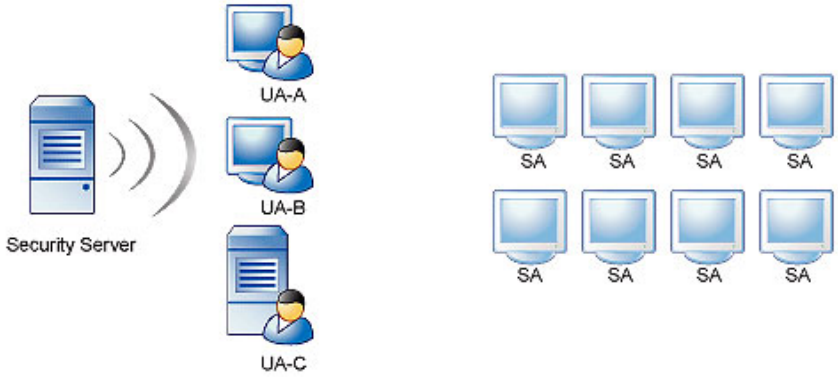
# Agenty aktualizacji

Agenty aktualizacji to programy Security Agent, które mogą odbierać zaktualizowane składniki z serwera Security Server lub serwera ActiveUpdate i instalować je na innych programach Security Agent.

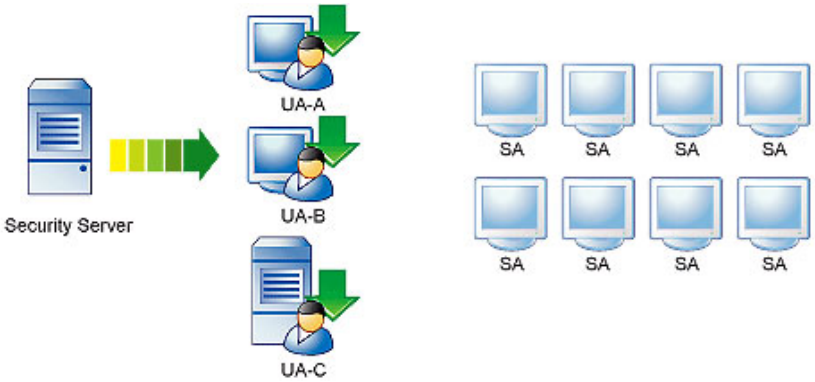
Po ustaleniu, że niektóre sekcje sieci między klientami a serwerem Trend Micro Security Server charakteryzują się „niską przepustowością" lub „intensywnym ruchem", można tak skonfigurować programy Security Agent, aby działały jako agenty aktualizacji. Agenty aktualizacji zmniejszają obciążenie sieci, eliminując konieczność uzyskiwania przez wszystkie programy Security Agent dostępu do serwera Security Server w celu pobrania aktualizacji składników. Jeśli sieć lokalna podzielona jest na segmenty według lokalizacji, a połączenie między segmentami jest często obciążone dużym ruchem, firma Trend Micro zaleca, aby przynajmniej jeden program Security Agent w każdym z segmentów pełnił funkcję agenta aktualizacji.

Proces aktualizacji za pośrednictwem agenta aktualizacji można opisać w następujący sposób:

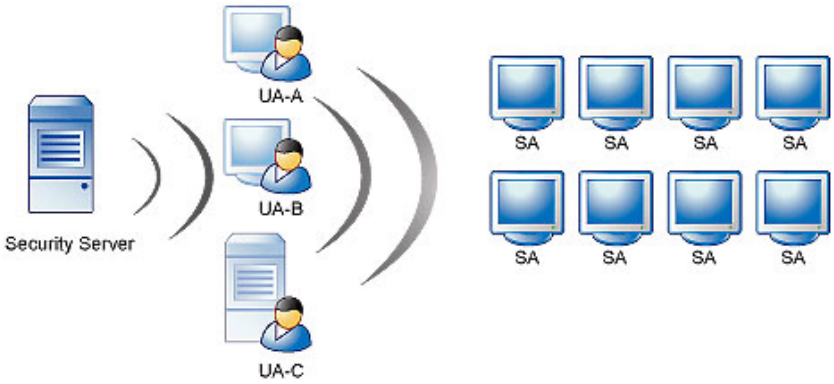
1. Program Security Server powiadamia agenty aktualizacji o dostępności nowych aktualizacji.




2. Agenty aktualizacji pobierają zaktualizowane składniki z serwera Security Server.




3. Serwer Security Server powiadamia programy Security Agent o dostępności zaktualizowanych składników.

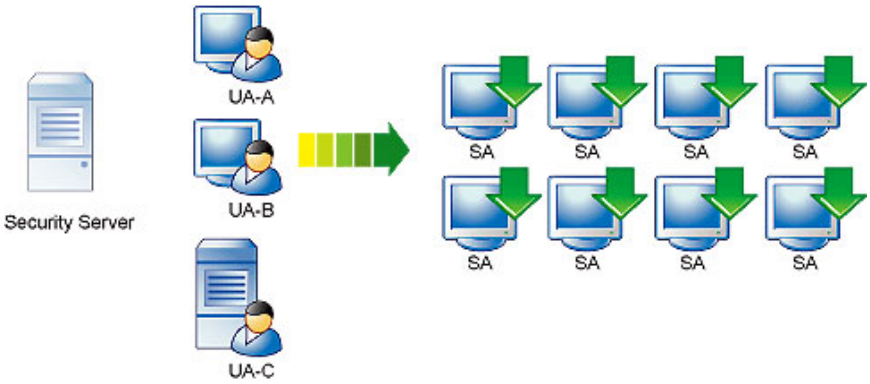



4. Każdy program Security Agent pobiera kopię tabeli kolejności agentów aktualizacji, aby określić odpowiednie źródło aktualizacji. Porządek agentów aktualizacji w tabeli kolejności jest wstępnie określony przez kolejność, w jakiej były dodawane jako alternatywne źródła aktualizacji w konsoli internetowej. Każdy program Security Agent przetwarza kolejno wpisy tabeli, rozpoczynając od pierwszego, aż do zidentyfikowania własnego źródła aktualizacji.

Tabela kolejności agentów aktualizacji

| Zakres IP | Agent aktualizacji |
|---|---|
| 10.1.1.1-10.1.1.10 | UA-A |
| 10.2.1.1-10.2.1.10 | UA-B |
| 10.3.1.1-10.3.1.10 | UA-C |

5. Następnie programy Security Agent pobierają zaktualizowane składniki od przypisanych im agentów aktualizacji. Jeżeli z jakiegoś powodu przypisany agent aktualizacji nie jest dostępny, program Security Agent podejmie próbę pobrania zaktualizowanych składników z serwera Security Server.




## Konfigurowanie agentów aktualizacji

**Procedura**

1. Przejdź do pozycji **Aktualizacje** > **Źródło**.
2. Kliknij kartę **Programy Update Agent**.
3. Wykonaj następujące czynności:

| ZADANIE | CZYNNOŚCI |
|---|---|
| Przypisanie programów Security Agent jako agentów aktualizacji | a. W sekcji **Przypisz agenta aktualizacji** kliknij przycisk **Dodaj**.<br>Zostanie wyświetlony nowy ekran.<br>b. Wybierz z listy co najmniej jednego agenta, który ma działać jako agent aktualizacji.<br>c. Kliknij przycisk **Zapisz**.<br>Ekran zostanie zamknięty.<br>d. Po powrocie do sekcji **Przypisz agenta aktualizacji** wybierz opcję **Agenty aktualizacji zawsze wykonują aktualizację bezpośrednio z serwera Security Server**, jeśli chcesz, aby agenty aktualizacji zawsze pobierały |

| Zadanie | Czynności |
|---|---|
| | zaktualizowane składniki z serwera Security Server zamiast od innego agenta aktualizacji. |
| Konfigurowanie programów Security Agent, aby dokonywały aktualizacji za pośrednictwem agentów aktualizacji | a. W sekcji **Alternatywne źródła aktualizacji** wybierz opcję **Włącz alternatywne źródła aktualizacji dla agentów zabezpieczeń i agentów aktualizacji**.<br><br>**Uwaga**<br>Wyłączenie tej opcji uniemożliwia programom Security Agent dokonywanie aktualizacji za pośrednictwem agentów aktualizacji, ustawiając z powrotem serwer Security Server jako źródło aktualizacji.<br><br>b. Kliknij przycisk **Dodaj**.<br><br>Zostanie wyświetlony nowy ekran.<br><br>c. Wpisz adresy IP programów Security Agent, które będą dokonywać aktualizacji za pośrednictwem agenta aktualizacji.<br><br>• Wpisz zakres adresów IPv4.<br><br>Aby określić pojedynczy program Security Agent, wprowadź jego adres IP zarówno w polu **od**, jak i w polu **do**.<br><br>• W przypadku adresu IPv6 wpisz prefiks IP i długość.<br><br>d. Wybierz agenta aktualizacji z listy rozwijanej.<br><br>Jeśli lista rozwijana jest niedostępna, nie skonfigurowano żadnych agentów aktualizacji.<br><br>e. Kliknij przycisk **Zapisz**.<br><br>Ekran zostanie zamknięty.<br><br>f. W zależności od potrzeb określ więcej zakresów adresów IP. Jeśli zdefiniowanych jest więcej zakresów adresów IP, można użyć opcji **Zmień kolejność** w celu ustawienia priorytetu zakresów adresów IP. Gdy serwer Security Server wysyła do programów Security Agent powiadomienie o dostępności aktualizacji, skanują one listę |

| Zadanie | Czynności |
|---|---|
| | zakresów adresów IP, aby zidentyfikować właściwe źródło aktualizacji. Najpierw sprawdzony zostaje pierwszy element na liście, a potem następne, aż do końca listy, dopóki nie zostanie odnalezione właściwe źródło aktualizacji.<br><br>**Porada**<br>W celu zabezpieczenia przed skutkami awarii dla jednego zakresu adresów IP można określić kilka agentów aktualizacji. Oznacza to, że jeśli programy Security Agent nie będą w stanie przeprowadzić aktualizacji za pośrednictwem danego agenta, spróbują skorzystać z innych. W tym celu należy utworzyć co najmniej dwa (2) wpisy dla tego samego zakresu adresów IP i przypisać każdy z wpisów do innego agenta aktualizacji. |
| Usuwanie agentów aktualizacji | Aby usunąć agenta aktualizacji i cofnąć przypisanie wszystkich przypisanych do niego programów Security Agent, przejdź do sekcji **Przypisz agenta aktualizacji**, zaznacz pole wyboru odpowiadające nazwie komputera agenta aktualizacji i kliknij opcję **Usuń**.<br><br>Ta operacja nie spowoduje usunięcia zakresu adresów IP programów Security Agent podanych w sekcji **Alternatywne źródła aktualizacji**, a tylko wymusi zmianę źródła aktualizacji „odłączonych” programów Security Agent z powrotem na serwer Security Server. Jeśli dostępny jest inny agent aktualizacji, można go przypisać do odłączonych programów Security Agent. |
| Cofanie przypisania programów Security Agent do agentów aktualizacji | Jeśli nie chcesz już, aby programy Security Agent należące do danego zakresu adresów IP były aktualizowane za pośrednictwem agenta aktualizacji, przejdź do sekcji **Alternatywne źródła aktualizacji**, zaznacz pole wyboru przy zakresie adresów IP programów Security Agent i kliknij opcję **Usuń**. |

4. Kliknij przycisk **Zapisz**.

# Rozdział 9

## Używanie stanu aktywności

# Stan aktywności

Worry-Free Business Security udostępnia widżety pełniące funkcję szybkich referencji wizualnych pomocnych w zarządzaniu programem Security Agent.

Ekran **Stan aktywności** zostanie wyświetlony po otworzeniu konsoli internetowej Worry-Free Business Security lub kliknięciu polecenia **Stan aktywności** w menu głównym.

**TABELA 9-1. Widgety na ekranie Stan aktywności**

| WIDŻET | OPIS |
|---|---|
| Centrum akcji | Ten widżet pokazuje zdarzenia wymagające od administratorów podjęcia działań w celu rozwiązania problemów. |
| Wykryte zagrożenia bezpieczeństwa w czasie | Ten widżet pokazuje podsumowanie punktów końcowych w sieci z wykrytymi zagrożeniami oraz listą typów zagrożeń dotyczących sieci w określonym przedziale czasu. |
| Podsumowanie zagrożeń typu ransomware | Ten widżet pokazuje podsumowanie wszystkich ataków podjętych przez oprogramowanie typu ransomware w określonym przedziale czasu. |
| Stan licencji | Ten widżet pokazuje podsumowanie wykorzystywanych stanowisk oraz stanu wygaśnięcia licencji. |
| Podsumowanie dla serwerów Exchange | Ten widget zapewnia przegląd stanu połączenia programów Messaging Security Agent oraz dystrybucję wykrytych zagrożeń na serwerach Exchange. |
| Stan agenta | Ten widżet pokazuje podsumowanie połączenia oraz stanu aktualizacji programów Security Agent w sieci. |

Częstotliwość odświeżania informacji na ekranie **Stan aktywności** zależy od sekcji. Przeważnie częstotliwość odświeżania wynosi od 1 do 10 minut. Aby ręcznie odświeżyć informacje na ekranie, kliknij przycisk **Odśwież** dostępny w przeglądarce.

## Centrum akcji

Ten widżet pokazuje zdarzenia wymagające od administratorów podjęcia działań w celu rozwiązania problemów.

Dla niektórych zdarzeń są dostępne przyciski zalecanych operacji. Kliknij przyciski, aby spróbować rozwiązać problemy, lub kliknij zdarzenia, aby wyświetlić więcej szczegółów.

**TABELA 9-2. Zdarzenia w Centrum akcji**

| ZDARZENIE | ZALECENIA |
|---|---|
| Antywirus — niezneutralizowane zagrożenia | Uruchom skanowanie przy użyciu narzędzia Trend Micro HouseCall Tool. |
| Antywirus — skanowanie w czasie rzeczywistym wyłączone w punktach końcowych | Włącz skanowanie w czasie rzeczywistym na wszystkich urządzeniach, aby zapewnić sobie maksymalną ochronę. |
| Antywirus — wyłączono skanowanie serwerów Exchange w czasie rzeczywistym | Włącz skanowanie w czasie rzeczywistym na wszystkich serwerach Exchange, aby zapewnić sobie maksymalną ochronę. |
| Zabezpieczenie przed spyware - przypadki wykrycia wymagające ponownego uruchomienia urządzenia | Ponownie uruchom urządzenia, aby całkowicie usunąć wykryte zagrożenia. |
| Zdarzenia związane z licencją | Wybierz opcje **Administracja** > **Licencja produktu**, aby sprawdzić status licencji. |
| Niedobór zasobów — pozostałe miejsce na dysku poniżej %threshold% | Uruchom narzędzie czyszczenia dysków, aby usunąć nieużywane pliki kopii zapasowych, dzienników i sygnatur.<br>Aby uzyskać więcej informacji, zobacz *Oszczędzanie miejsca na dysku na stronie 14-15*. |
| Usługi Smart Protection — usługa niedostępna | Sprawdź stan serwera Smart Scan Server w konsoli Worry-Free Business Security i upewnij się, że serwer działa poprawnie. |

| Zdarzenie | Zalecenia |
|---|---|
| Aktualizacja — co najmniej jeden nieaktualny agent Messaging Security Agent po upływie jednej godziny od daty wydania sygnatur | Upewnij się, że zaplanowane aktualizacje programu Messaging Security Agent są włączone na serwerze Security Server i że programy Messaging Security Agent mogą łączyć się z Internetem. |
| Aktualizacja — postęp wdrażania mniejszy niż %threshold% po upływie jednej godziny od wydania sygnatury. | Sprawdź połączenie internetowe programu Security Agent i ponownie zaktualizuj programy Security Agent. |
| Aktualizacja — składniki programu Security Server nie były aktualizowane przez ponad %threshold% dni. | Upewnij się, że zaplanowane aktualizacje składników są włączone na serwerze Security Server i że serwer Security Server może łączyć się z Internetem. |
| Aktualizacja — sygnatury Smart Scan nie były aktualizowane przez ponad %threshold% godz. | Upewnij się, że zaplanowane aktualizacje sygnatury Smart Scan są włączone na serwerze Security Server i że program Security Server może łączyć się z Internetem. |

## Oprogramowanie antywirusowe: nieusunięte zagrożenia

Można wyświetlić te informacje, klikając zdarzenie **Antywirus — niezneutralizowane zagrożenia: zdarzenie %N%** w Centrum akcji. Worry-Free Business Security generuje lub aktualizuje informacje dziennika po każdym przeprowadzeniu skanowania w czasie rzeczywistym lub skanowania zaplanowanego.

- Kliknij pozycję **Narzędzie do pobierania**, aby pobrać narzędzie Trend Micro HouseCall Tool i użyć go do przeprowadzenia skanowania odnośnego urządzenia.
- Kliknij pozycję **Odrzuć z Centrum akcji**, aby przejść do ekranu **Stan aktywności** i usunąć zdarzenie powiadomienia z Centrum akcji. Dzienniki powiązane ze zdarzeniami wyświetlanymi na tym ekranie będą nadal dostępne przy użyciu funkcji kwerendy dziennika.
- Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| Kolumna | Opis |
|---|---|
| Data/godzina | Data i godzina ostatniej nieudanej próby usunięcia wirusa lub złośliwego oprogramowania |
| Nazwa urządzenia | Nazwa zagrożonego urządzenia |
| Nazwa wirusa / złośliwego oprogramowania | Nazwa wykrytego wirusa / złośliwego oprogramowania<br>Kliknij łącze w celu przekierowania do encyklopedii zagrożeń firmy Trend Micro i uzyskania dokładnego opisu zagrożenia oraz instrukcji na temat ręcznego usuwania skutków jego działania. |
| Nazwa pliku | Nazwa pliku uszkodzonego przez wirus / złośliwe oprogramowanie |
| Ścieżka | Lokalizacja zarażonego pliku |
| Typ skanowania | Typ skanowania użyty do wykrycia wirusa lub złośliwego oprogramowania |
| Rozpoczęta operacja | Operacje wykonane przez Worry-Free Business Security w odpowiedzi na wykryte wirusy / złośliwe oprogramowanie |

## Antywirus: skanowanie w czasie rzeczywistym wyłączone na punktach końcowych

Możesz wyświetlić te informacje, klikając zdarzenie **Antywirus: skanowanie w czasie rzeczywistym wyłączone na punktach końcowych: %N%** w Centrum akcji.

- Kliknij pozycję **Włącz skanowanie w czasie rzeczywistym**, aby włączyć skanowanie na wszystkich urządzeniach.
- Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| Kolumna | Opis |
|---|---|
| Nazwa urządzenia | Nazwa urządzenia z wyłączonym skanowaniem w czasie rzeczywistym |

| KOLUMNA | OPIS |
|---|---|
| Nazwa grupy | Nazwa grupy, do której należy urządzenie |

## Antywirus — wyłączono skanowanie serwerów Exchange w czasie rzeczywistym

Możesz wyświetlić te informacje, klikając zdarzenie **Antywirus — skanowanie w czasie rzeczywistym wyłączone na serwerach Exchange: % N%** w Centrum akcji.

- Kliknij pozycję **Włącz skanowanie w czasie rzeczywistym**, aby włączyć skanowanie na wszystkich serwerach Exchange.
- Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| KOLUMNA | OPIS |
|---|---|
| Nazwa serwera Exchange | Nazwa serwera Exchange z wyłączonym skanowaniem w czasie rzeczywistym |

## Oprogramowanie anti-spyware: przypadki wykrycia wymagające ponownego uruchomienia urządzenia

Można wyświetlić informacje z tego dziennika, klikając zdarzenie **Oprogramowanie anti-spyware — przypadki wykrycia wymagające ponownego uruchomienia urządzenia: %N%** w Centrum akcji.

- Kliknij pozycję **Odrzuć z Centrum akcji**, aby przejść do ekranu **Stan aktywności** i usunąć zdarzenie powiadomienia z Centrum akcji. Dzienniki powiązane ze zdarzeniami wyświetlanymi na tym ekranie będą nadal dostępne przy użyciu funkcji kwerendy dziennika.
- Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| KOLUMNA | OPIS |
|---|---|
| Data/godzina | Data i godzina przekazania przez program Security Agent informacji na temat przypadków wykrycia oprogramowania spyware lub grayware do Worry-Free Business Security. |
| Nazwa urządzenia | Nazwa zagrożonego urządzenia |
| Nazwa oprogramowania spyware/grayware | Nazwa wykrytego oprogramowania spyware lub grayware<br><br>Kliknij łącze w celu przekierowania do encyklopedii zagrożeń firmy Trend Micro i uzyskania dokładnego opisu zagrożenia oraz instrukcji na temat ręcznego usuwania skutków jego działania. |
| Typ skanowania | Typ skanowania użyty do wykrycia oprogramowania spyware lub grayware |

## Niedobór zasobów — pozostałe miejsce na dysku

Możesz wyświetlić te informacje, klikając zdarzenie **Niedobór zasobów — pozostałe miejsce na dysku poniżej % threshold%** w Centrum akcji

Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| KOLUMNA | OPIS |
|---|---|
| Nazwa serwera | Nazwa serwera z małą ilością miejsca na dysku |
| Nazwa grupy | Nazwa grupy, do której należy serwer |

## Aktualizacja: nieaktualne agenty

Możesz wyświetlić te informacje, klikając zdarzenie**Aktualizuj: Współczynnik wdrażania mniejszy niż %progu% po godzinie od pojawienia się sygnatury** w centrum akcji. Programy Security Agent wymienione na tym ekranie wymagają aktualizacji silnika lub sygnatury.

- Kliknij **Aktualizuj teraz** powiadomić nieaktualne programy Security Agent o konieczności aktualizacji do najnowszych składników.
- Kliknij **Sprawdź stan składnika**, aby otworzyć ekran **Ręcznej aktualizacji**.
- Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| KOLUMNA | OPIS |
|---|---|
| Nazwa urządzenia | Nazwa urządzenia wymagającego aktualizacji składników |
| Nazwa grupy | Nazwa grupy, do której należy urządzenie |
| Metoda skanowania | • Smart Scan<br>• Skanowanie standardowe |

### Aktualizacja — nieaktualne agenty Messaging Security Agent

Możesz wyświetlić te informacje, klikając zdarzenie**Aktualizacja — co najmniej jeden nieaktualny agent Messaging Security Agent po upływie jednej godziny od daty wydania sygnatur** w centrum akcji.

- Kliknij **Aktualizuj teraz** powiadomić nieaktualne programy Messaging Security Agent o konieczności aktualizacji do najnowszych składników.
- Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| KOLUMNA | OPIS |
|---|---|
| Nazwa serwera Exchange | Nazwa serwera Exchange wymagającego aktualizacji składników |

## Wykryte zagrożenia bezpieczeństwa w czasie

Ten widżet pokazuje podsumowanie punktów końcowych w sieci z wykrytymi zagrożeniami oraz listą typów zagrożeń dotyczących sieci w określonym przedziale czasu.

- Kliknij przycisk lub , aby przełączać między poszczególnymi widokami.
- Kliknij kartę **Znane zagrożenia**, **Nieznane zagrożenia** lub **Naruszenia reguł**, aby wyświetlić informacje dotyczące wykrycia dla określonych zagrożeń.

| Widok | Opis |
|---|---|
| Wykres ( ) | • Klikaj nazwy typów zagrożeń na dole wykresu, aby wyświetlić/ukryć informacje na wykresie.<br>• Ustaw wskaźnik myszy nad węzłem (węzłami) z określoną datą, aby wyświetlić łączną liczbę wykrytych zagrożeń wyświetlanego typu. Kliknij węzeł, aby przejść do ekranu dzienników dotyczących typu zagrożenia wyróżnionego na liście. |
| Tabela ( ) | • Kliknij licznik przypadków wykrycia oprogramowania, aby otworzyć ekran dzienników zawierający szczegółowe informacje na temat przypadków wykrycia. |

## Wykryte zagrożenia bezpieczeństwa: wirus/złośliwe oprogramowanie

Można wyświetlić te informacje, klikając jedno z następujących łączy na karcie **Znane zagrożenia** w widżecie **Wykryte zagrożenia bezpieczeństwa w czasie**:

- Liczba wykrytych przypadków zagrożeń spowodowanych przez **wirusy/złośliwe oprogramowanie** w widoku tabeli
- Dowolny węzeł **wirus/złośliwe oprogramowanie** w widoku wykresu

Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| Kolumna | Opis |
|---|---|
| Data/godzina | Data i godzina, w której program Security Agent zgłosił informacje o wykryciu zagrożenia wirusem/złośliwym oprogramowaniem do programu Worry-Free Business Security |

| KOLUMNA | OPIS |
|---|---|
| Nazwa urządzenia | Nazwa zagrożonego urządzenia |
| Nazwa wirusa / złośliwego oprogramowania | Nazwa wykrytego wirusa / złośliwego oprogramowania<br>Kliknij łącze w celu przekierowania do encyklopedii zagrożeń firmy Trend Micro i uzyskania dokładnego opisu zagrożenia oraz instrukcji na temat ręcznego usuwania skutków jego działania. |
| Nazwa pliku | Nazwa pliku uszkodzonego przez wirus / złośliwe oprogramowanie |
| Ścieżka | Lokalizacja zarażonego pliku |
| Typ skanowania | Typ skanowania użyty do wykrycia wirusa lub złośliwego oprogramowania |
| Rozpoczęta operacja | Operacje wykonane przez Worry-Free Business Security w odpowiedzi na wykryte wirusy / złośliwe oprogramowanie |

## Wykryte zagrożenia bezpieczeństwa: oprogramowanie spyware/grayware

Można wyświetlić te informacje, klikając jedno z następujących łączy na karcie **Znane zagrożenia** w widżecie **Wykryte zagrożenia bezpieczeństwa w czasie**:

- Liczba wykrytych przypadków zagrożeń spowodowanych przez **oprogramowanie spyware/grayware** w widoku tabeli
- Dowolny węzeł **oprogramowanie spyware/grayware** w widoku wykresu

Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| KOLUMNA | OPIS |
|---|---|
| Data/godzina | Data i godzina przekazania przez program Security Agent informacji na temat przypadków wykrycia oprogramowania spyware lub grayware do Worry-Free Business Security. |

| Kolumna | Opis |
|---|---|
| Nazwa urządzenia | Nazwa zagrożonego urządzenia<br>Kliknij nazwę, aby wyświetlić listę pojedynczych programów spyware/grayware wykrytych na tym urządzeniu. |
| Nazwa oprogramowania spyware/grayware | Nazwa wykrytego oprogramowania spyware lub grayware |
| Typ skanowania | Typ skanowania użyty do wykrycia oprogramowania spyware lub grayware |
| Rozpoczęta operacja | Operacje wykonane przez Worry-Free Business Security w odpowiedzi na wykryte oprogramowanie spyware/grayware |

## Wykryte zagrożenia bezpieczeństwa: Usługa Web Reputation

Można wyświetlić te informacje, klikając jedno z następujących łączy na karcie **Znane zagrożenia** w widżecie **Wykryte zagrożenia bezpieczeństwa w czasie**:

- Liczba zagrożeń wykrytych przez usługę **Usługa Web Reputation** w widoku tabeli
- Dowolny węzeł **Usługa Web Reputation** w widoku wykresu

Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| Kolumna | Opis |
|---|---|
| Data/godzina | Data i godzina przekazania przez program Security Agent informacji na temat naruszeń adresów URL do Worry-Free Business Security |
| Nazwa urządzenia | Nazwa urządzenia próbującego uzyskać dostęp do adresu URL objętego ograniczeniem |
| URL | Adres URL objęty ograniczeniem |

| Kolumna | Opis |
|---|---|
| Poziom ryzyka | Ocena przypisana przez laboratoria TrendLabs na podstawie łatwości zarażenia i potencjalnych szkód. |

## Wykryte zagrożenia bezpieczeństwa: wirus sieciowy

Można wyświetlić te informacje, klikając jedno z następujących łączy na karcie **Znane zagrożenia** w widżecie **Wykryte zagrożenia bezpieczeństwa w czasie**:

- Liczba wykrytych **Wirus sieciowy** w widoku tabeli
- Dowolny węzeł **Wirus sieciowy** w widoku wykresu

Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| Kolumna | Opis |
|---|---|
| Data/godzina | Data i godzina, w której program Security Agent zgłosił informacje o wykryciu wirusa sieciowego do programu Worry-Free Business Security |
| Nazwa urządzenia | Nazwa zagrożonego urządzenia |
| Adres IP atakującego | Adres IP atakującego |
| Adres IP atakowanego | Adres IP ofiary |
| Kierunek ruchu pakietów | Kierunek pakietu |
| Nazwa wirusa sieciowego | Nazwa wykrytego wirusa sieciowego |
| Licznik | Każdy wirus sieciowy jest liczony za każdym razem, gdy zostanie wykryty. |

## Wykryte zagrożenia bezpieczeństwa: monitorowanie zachowania

Można wyświetlić te informacje, klikając jedno z następujących łączy na karcie **Nieznane zagrożenia** w widżecie **Wykryte zagrożenia bezpieczeństwa w czasie**:

- Liczba zagrożeń wykrytych przez **Monitorowanie zachowania** w widoku tabeli
- Dowolny węzeł **Monitorowanie zachowania** w widoku wykresu

Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

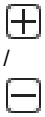
| Kolumna | Opis |
|---|---|
| Data/godzina | Data i godzina przekazania przez program Security Agent informacji na temat naruszenia monitorowania zachowania do Worry-Free Business Security |
| Nazwa urządzenia | Nazwa urządzenia, które uruchomiło naruszenie reguł |
| Zagrożenie bezpieczeństwa | Typ zagrożenia bezpieczeństwa |
| Temat | Temat operacji |
| Typ zdarzenia | Powiązane zdarzenie systemowe |
| Cel | Cel operacji |
| Operacja | Przeprowadzona przez użytkownika operacja, która wyzwoliła naruszenie |
| Wynik | Operacje wykonane przez Worry-Free Business Security w odpowiedzi na naruszenia monitorowania zachowania |

## Wykryte zagrożenia bezpieczeństwa: przewidujące uczenie maszynowe

Można wyświetlić te informacje, klikając jedno z następujących łączy na karcie **Nieznane zagrożenia** w widżecie **Wykryte zagrożenia bezpieczeństwa w czasie**:

- Liczba zagrożeń wykrytych przez **Przewidujące uczenie maszynowe** w widoku tabeli
- Dowolny węzeł **Przewidującego uczenia maszynowego** w widoku wykresu

Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| KOLUMNA | OPIS |
|---|---|
|  | Kliknij ikonę, aby rozwinąć lub zamknąć szczegóły dziennika poniżej wiersza tabeli. |
| Data/godzina | Data i godzina, kiedy program Security Agent zgłosił informacje o wykryciu zagrożenia przez Przewidujące uczenie maszynowe do programu Worry-Free Business Security |
| Nazwa urządzenia | Nazwa zagrożonego urządzenia |
| Nazwa grupy | Nazwa grupy, do której należy urządzenie |
| Nieznane zagrożenie | Nazwa prawdopodobnego zagrożenia |
| Prawdopodobieństwo zagrożenia | Wskazuje, w jakim stopniu plik/proces był zgodny z modelem złośliwego oprogramowania |
| Nazwa pliku | Nazwa obiektu pliku lub programu, który uruchomił proces<br><br>**Ważne**<br>Nazwa wykrytego pliku może nie być taka sama, jak nazwa pliku wykryta na innych punktach końcowych. Funkcja Przewidujące uczenie maszynowe kojarzy wykryte zagrożenia zgodnie z wartościami skrótu plików, a nie ich nazwami. |
| Ścieżka | Ścieżka obiektu pliku lub ścieżka programu, który uruchomił proces |
| Kanał zarażenia | Kanał, z którego pochodzi zagrożenie |
| Rozpoczęta operacja | Działanie podjęte przez program Worry-Free Business Security w reakcji na wykrycie zagrożenia |

## Wykryte zagrożenia bezpieczeństwa: szczegóły dotyczące przewidującego uczenia maszynowego

Informacje te można wyświetlić, klikając dowolną

ikonę w pierwszej kolumnie ekranu dzienników **Rejestrowanie zagrożeń bezpieczeństwa: Przewidujące uczenie maszynowe**.

Sekcja szczegółów dziennika zawiera dwie karty:

- **Nieznane zagrożenie:**: wyniki analizy przewidującego uczenia maszynowego.
- **Nazwa pliku**: ogólne informacje dotyczące właściwości pliku i informacje o certyfikacie konkretnego dziennika wykrywania.

**Porada**

Kliknij pozycję **Dodaj do listy wyjątków**, aby szybko dodać wartość skrótu pliku do globalnej listy wyjątków przewidującego uczenia maszynowego. Całą listę wyjątków można zobaczyć na ekranie **Ustawienia globalne**.

Aby uzyskać więcej informacji, patrz *Konfigurowanie ustawień listy wyjątków na stronie 11-14*.

W poniższej tabeli przedstawiono informacje zawarte na karcie **Nieznane zagrożenie**.

**TABELA 9-3. Szczegóły karty Nieznane zagrożenie**

| ELEMENT | OPIS |
|---|---|
| Prawdopodobieństwo zagrożenia | Wskazuje, w jakim stopniu plik/proces był zgodny z modelem złośliwego oprogramowania |
| Prawdopodobny typ zagrożenia | Wskazuje najbardziej prawdopodobny typ zagrożenia zawartego w pliku po porównaniu wyników analizy z innymi znanymi zagrożeniami za pomocą przewidującego uczenia maszynowego |

| Element | Opis |
|---|---|
| Identyfikatory zagrożeń | Udostępnia listę funkcji API używanych przez plik/proces, które mogą wskazywać na wykryty typ zagrożenia<br><br>**Ważne**<br>Identyfikacja funkcji API jest tylko jednym z czynników określających typ zagrożenia. Mechanizm przewidującego uczenia maszynowego wykorzystuje wiele innych funkcji plików i metod analizy do obliczania prawdopodobieństwa zagrożenia i prawdopodobnego typu zagrożenia. |
| Typ wykrytego zagrożenia | Typ obiektu, który uruchomił wykrywanie („Plik” lub „Proces”) |
| Podobne znane zagrożenia | Zawiera listę znanych typów zagrożeń, które wykazują podobne funkcje pliku/procesu do wykrytego zagrożenia |

## Wykryte zagrożenia bezpieczeństwa: filtrowanie adresów URL

Można wyświetlić te informacje, klikając jedno z następujących łączy na karcie **Naruszenia reguł** w widżecie **Wykryte zagrożenia bezpieczeństwa w czasie**:

- Liczba wykrytych przypadków przez **Filtrowanie adresów URL** w widoku tabeli
- Dowolny węzeł **Filtrowania adresów URL** w widoku wykresu

Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| Kolumna | Opis |
|---|---|
| Data/godzina | Data i godzina przekazania przez program Security Agent informacji na temat naruszeń adresów URL do Worry-Free Business Security |

| Kolumna | Opis |
|---|---|
| Nazwa urządzenia | Nazwa urządzenia próbującego uzyskać dostęp do adresu URL objętego ograniczeniem |
| URL | Adres URL objęty ograniczeniem |

## Wykryte zagrożenia bezpieczeństwa: kontrola urządzeń

Można wyświetlić te informacje, klikając jedno z następujących łączy na karcie **Naruszenia reguł** w widżecie **Wykryte zagrożenia bezpieczeństwa w czasie**:

- Liczba zagrożeń wykrytych przez funkcję **Kontrola urządzeń** w widoku tabeli
- Dowolny węzeł **Kontroli urządzeń** w widoku wykresu

Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| Kolumna | Opis |
|---|---|
| Data/godzina | Data i godzina, w których program Security Agent zgłosił informacje o naruszeniu Kontroli urządzeń do Worry-Free Business Security |
| Nazwa urządzenia | Nazwa urządzenia, które uruchomiło naruszenie reguł |
| Typ | Typ urządzenia pamięci masowej |
| Uprawnienie | Zestaw uprawnień dla urządzenia pamięci masowej |
| Temat | Temat operacji |
| Obiekt | Przedmiot działania |
| Operacja | Działanie wykonane |

# Podsumowanie zagrożeń typu ransomware

Ten widżet pokazuje podsumowanie wszystkich ataków podjętych przez oprogramowanie typu ransomware w określonym przedziale czasu.

Domyślny widok zawiera podsumowanie wszystkich przypadków wykrycia oprogramowania typu ransomware wraz z podziałem podjętych prób ataku na podstawie kanału zarażenia.

- Kliknij licznik przypadków wykrycia oprogramowania typu ransomware w widoku domyślnym, aby otworzyć ekran dzienników **Podsumowanie zagrożeń typu ransomware** zawierający szczegółowe informacje na temat wykrytego oprogramowania typu ransomware.
- Użyj rozwijanej listy, aby przełączać między poszczególnymi widokami.

Kliknij przycisk , aby wyświetlić informacje dotyczące wykrycia w postaci wykresu.

- Ustaw wskaźnik myszy nad węzłem (węzłami) z określoną datą, aby wyświetlić łączną liczbę przypadków wykrycia w wyświetlanej kategorii. Kliknij węzeł, aby przejść do ekranu dziennika **Podsumowanie zagrożeń typu ransomware**, zawierającego szczegółowe informacje na temat oprogramowania typu ransomware wykrytego danego dnia.

## Dzienniki podsumowania zagrożeń typu ransomware

Możesz wyświetlić te informacje, klikając węzeł na wykresie lub licznik wykrywania w widgecie **Podsumowanie zagrożeń typu ransomware**.

- Użyj list **Kanał zarażenia** i **Okres**, aby dostosować widok.
- Kliknij pozycję **Eksportuj**, aby zapisać zdarzenia dziennika w pliku CSV.

| KOLUMNA | OPIS |
|---|---|
| Data/godzina | Data i godzina przekazania przez program Security Agent informacji na temat przypadków wykrycia oprogramowania typu ransomware do Worry-Free Business Security |

| KOLUMNA | OPIS |
|---|---|
| Zagrożenie bezpieczeństwa | Typ ransomware<br>• Nazwa wirusa/złośliwego oprogramowania: Wyświetla nazwę znanego pliku oprogramowania ransomware<br>• Nieautoryzowane szyfrowanie plików: Pojawia się, gdy program Worry-Free Business Security wykryje, że podejrzany program zaszyfrował plik.<br>• <URL>: pojawia się, gdy program Worry-Free Business Security wykryje znany adres URL związany z oprogramowaniem ransomware |
| Source | Typ skanowania, podczas którego wykryto zagrożenie |
| Ścieżka/adres URL | • Ścieżka pliku ransomware<br>• Adres URL zainfekowany oprogramowaniem ransomware |
| Rozpoczęta operacja | Działanie podejmowane przez Worry-Free Business Security w odpowiedzi na wykrycie oprogramowania typu ransomware |
| Nazwa urządzenia | Nazwa zagrożonego urządzenia |
| Kanał zarażenia | Kanał wykrywania ransomware |
| Szczegóły | Kliknij opcję **Wyświetl**, aby wyświetlić szczegóły dziennika. |

## Ransomware: szczegóły dziennika monitorowania zachowania

Można wyświetlić te informacje, klikając łącze **Wyświetl** w kolumnie **Szczegóły** na ekranie dzienników podsumowania oprogramowania typu ransomware.

| WIERSZ | OPIS |
|---|---|
| Data/godzina | Data i godzina przekazania przez program Security Agent informacji na temat naruszenia monitorowania zachowania do Worry-Free Business Security |

| Wiersz | Opis |
|---|---|
| Nazwa urządzenia | Nazwa urządzenia, które uruchomiło naruszenie reguł |
| Zagrożenie bezpieczeństwa | Typ zagrożenia bezpieczeństwa |
| Temat | Temat operacji |
| Typ zdarzenia | Powiązane zdarzenie systemowe |
| Cel | Cel operacji |
| Operacja | Przeprowadzona przez użytkownika operacja, która wyzwoliła naruszenie |
| Wynik | Operacje wykonane przez Worry-Free Business Security w odpowiedzi na naruszenia monitorowania zachowania |

## Oprogramowanie typu ransomware: szczegóły dziennika filtrowania adresów URL

Można wyświetlić te informacje, klikając łącze **Wyświetl** w kolumnie **Szczegóły** na ekranie dzienników podsumowania oprogramowania typu ransomware.

| Wiersz | Opis |
|---|---|
| Data/godzina | Data i godzina przekazania przez program Security Agent informacji na temat naruszeń adresów URL do Worry-Free Business Security |
| Nazwa urządzenia | Nazwa urządzenia próbującego uzyskać dostęp do adresu URL objętego ograniczeniem |
| URL | Adres URL objęty ograniczeniem |
| Kategoria adresu URL | Kategoria adresu URL objętego ograniczeniem |
| Rozpoczęta operacja | Operacje wykonane przez Worry-Free Business Security w odpowiedzi na naruszenia filtrowania adresów URL |

## Oprogramowanie typu ransomware: szczegóły dziennika wirusów

Można wyświetlić te informacje, klikając łącze **Wyświetl** w kolumnie **Szczegóły** na ekranie dzienników podsumowania oprogramowania typu ransomware.

| WIERSZ | OPIS |
|---|---|
| Data/godzina | Data i godzina przekazania przez program Security Agent informacji na temat przypadków wykrycia oprogramowania typu ransomware do Worry-Free Business Security |
| Nazwa urządzenia | Nazwa zagrożonego urządzenia |
| Nazwa wirusa / złośliwego oprogramowania | Nazwa wykrytego oprogramowania typu ransomware<br>Kliknij łącze w celu przekierowania do encyklopedii zagrożeń firmy Trend Micro i uzyskania dokładnego opisu zagrożenia oraz instrukcji na temat ręcznego usuwania skutków jego działania. |
| Nazwa pliku | Nazwa pliku uszkodzonego przez oprogramowanie typu ransomware |
| Ścieżka | Lokalizacja zarażonego pliku |
| Kanał zarażenia | Medium, za którego pośrednictwem oprogramowanie typu ransomware uzyskuje dostęp do punktu końcowego |
| Typ skanowania | Typ skanowania użyty do wykrycia oprogramowania typu ransomware |
| Rozpoczęta operacja | Działanie podejmowane przez Worry-Free Business Security w odpowiedzi na wykrycie oprogramowania typu ransomware |

## Oprogramowanie typu ransomware: szczegóły dziennika usługi Web Reputation

Można wyświetlić te informacje, klikając łącze **Wyświetl** w kolumnie **Szczegóły** na ekranie dzienników podsumowania oprogramowania typu ransomware.

| Wiersz | Opis |
|---|---|
| Data/godzina | Data i godzina przekazania przez program Security Agent informacji na temat naruszeń adresów URL do Worry-Free Business Security |
| Nazwa urządzenia | Nazwa urządzenia próbującego uzyskać dostęp do adresu URL objętego ograniczeniem |
| URL | Adres URL objęty ograniczeniem |
| Poziom ryzyka | Ocena przypisana przez laboratoria TrendLabs na podstawie łatwości zarażenia i potencjalnych szkód. |
| Rozpoczęta operacja | Operacje wykonane przez Worry-Free Business Security w odpowiedzi na naruszenia filtrowania adresów URL |

## Stan licencji

Ten widżet pokazuje podsumowanie wykorzystywanych stanowisk oraz stanu wygaśnięcia licencji.

## Podsumowanie dla serwerów Exchange

Ten widget zapewnia przegląd stanu połączenia programów Messaging Security Agent oraz dystrybucję wykrytych zagrożeń na serwerach Exchange.

Kliknij poziom zabezpieczeń, aby skonfigurować poziom wykrywania spamu dla programu Messaging Security Agent.

| Kolumna | Opis |
|---|---|
| Serwer | Nazwa serwera Exchange |
| Zdarzenie | Typ wiadomości typu spam |
| Współczynnik | Jest równa liczbie detekcji podzielonej przez liczbę przeskanowanych wiadomości |

## Stan agenta

Ten widżet pokazuje podsumowanie połączenia oraz stanu aktualizacji programów Security Agent w sieci.

- Kliknij liczbę obok statusu, aby przejść do ekranu **Urządzenia** zawierającego listę szczegółów urządzenia dotyczących tego konkretnego stanu.
- Kliknij pozycję **Dodaj urządzenia**, aby przejść do ekranu **Dodaj urządzenia**, na którym można zainstalować program Security Agent na większej liczbie urządzeń.

  Aby uzyskać więcej informacji, patrz *instalowanie agentów na stronie 3-1*.
- Kliknij przycisk**Sprawdź stan składnika** aby przejść do ekranu **Ręczna aktualizacja**, na którym można wyświetlić najnowsze informacje o składniku.

  Aby uzyskać więcej informacji, patrz *Składniki, które można aktualizować na stronie 8-4*.

# Rozdział 10

# Zarządzanie powiadomieniami

W tym rozdziale opisano sposób używania różnych opcji powiadomień.

# Korzystanie z powiadomień

Aby zminimalizować czas potrzebny administratorom na monitorowanie programu Worry-Free Business Security i zapewnić im wczesne ostrzeżenia e-mail o nadchodzących sytuacjach związanych z atakiem, skonfiguruj serwer, tak aby wysyłał powiadomienia w razie wystąpienia nieprawidłowych zdarzeń w sieci.

Domyślnie wszystkie zdarzenia wyświetlone na ekranie **Powiadomienia** są zaznaczone, a ich wystąpienie powoduje wysłanie powiadomienia do administratora systemu.

**TABELA 10-1. Wymagana operacja — powiadomienia**

| TYP ZDARZENIA | OPIS |
|---|---|
| **Zdarzenia zagrożeń** | |
| Antywirus — niezneutralizowane zagrożenia | Działania podejmowane przeciw wirusom/złośliwemu oprogramowaniu nie powiodły się.<br>Liczba wykrytych zdarzeń nie obejmuje następujących działań skanowania: Pominięto potencjalne zagrożenie bezpieczeństwa |
| Antywirus — skanowanie w czasie rzeczywistym wyłączone w punktach końcowych | Wyłączono skanowanie w czasie rzeczywistym na punktach końcowych |
| Antywirus — wyłączono skanowanie serwerów Exchange w czasie rzeczywistym | Wyłączono skanowanie serwerów Exchange w czasie rzeczywistym |
| Zabezpieczenie przed spyware - przypadki wykrycia wymagające ponownego uruchomienia urządzenia | Punkty końcowe z uruchomionym wykrywaniem spyware/grayware muszą zostać ponownie uruchomione, aby całkowicie usunąć zagrożenia. |
| **Zdarzenia systemowe** | |
| Aktualizacja — nieaktualne agenty | Nieaktualne programy Security Agent wymagają aktualizacji składników. |

| Typ zdarzenia | Opis |
|---|---|
| Aktualizacja — nieaktualne agenty Messaging Security Agent | Nieaktualne programy Messaging Security Agent wymagają aktualizacji składników. |
| Aktualizacja — nieaktualne sygnatury Smart Scan | Nieaktualna sygnatura Smart Scan wymaga aktualizacji. |
| Aktualizacja — nieaktualne składniki programu Security Server | Nieaktualny program Security Server wymaga aktualizacji składników. |
| Usługi Smart Protection — usługa niedostępna | Programy Security Agent ze skonfigurowanym skanowaniem Smart Scan mogą nawiązać połączenia z usługą Smart Protection Services lub jest ona niedostępna. |
| Niedobór zasobów — pozostałe miejsce na dysku | Ilość pozostałego miejsca na dysku na serwerze Security Server jest mniejsza niż określona wartość procentowa. |
| **Zdarzenia licencji** | |
| Licencja — wygasła | Licencja wygasła. |
| Licencja — do wygaśnięcia pozostało mniej niż 60 dni | Licencja wkrótce wygaśnie. |
| Licencja — wykorzystanie stanowisk przekracza wartość 110% | Stopień wykorzystania licencji na stanowiska przekracza 110%. |
| Licencja — wykorzystanie stanowisk przekracza wartość 100% | Stopień wykorzystania licencji na stanowiska przekracza 100%. |

**Tabela 10-2. Powiadomienia ostrzegawcze**

| Typ zdarzenia | Opis |
|---|---|
| **Zdarzenia zagrożeń** | |

| Typ zdarzenia | Opis |
|---|---|
| Antywirus — przypadki wykrycia wirusów w punktach końcowych przekraczają: | Wykryte zagrożenia wirusów/złośliwego oprogramowania na punktach końcowych przekraczają podaną liczbę w określonym przedziale czasu. |
| Antywirus — przypadki wykrycia wirusów na serwerach Exchange przekraczają: | Wykryte zagrożenia wirusów/złośliwego oprogramowania na serwerach Exchange przekraczają określoną liczbę w określonym przedziale czasu. |
| Zabezpieczenie przed spyware/grayware — liczba przypadków wykrycia oprogramowania spyware/grayware przekracza: | Wykryte na punktach końcowych zagrożenia spyware/grayware przekraczają określoną liczbę w określonym przedziale czasu. |
| Antyspam — przypadki wykrycia spamu w całkowitej liczbie odebranych wiadomości przekraczają: | Liczba wykrytych wiadomości typu spam przekracza określoną wartość procentową. |
| Usługa Web Reputation — liczba przypadków naruszenia adresu URL przekracza: | Naruszenia adresu URL przekraczają określoną liczbę w określonym przedziale czasu. |
| Filtrowanie adresów URL — liczba przypadków naruszenia adresu URL przekracza: | Naruszenia adresu URL przekraczają określoną liczbę w określonym przedziale czasu. |
| Przewidujące uczenie maszynowe — liczba przypadków wykrycia nieznanych zagrożeń przekracza: | Wykryte nieznane zagrożenia przekraczają określoną liczbę w określonym przedziale czasu. |
| Monitorowanie zachowania — liczba przypadków naruszenia monitorowania zachowania przekracza: | Naruszenia monitorowania zachowania wykraczają poza podaną liczbę w określonym przedziale czasu. |

| Typ zdarzenia | Opis |
|---|---|
| Wirus sieciowy — liczba wykrytych wirusów sieciowych przekracza: | Wykrycia wirusa sieciowego przekraczają określoną liczbę w określonym przedziale czasu. |
| Kontrola urządzeń — liczba naruszeń kontroli urządzeń przekracza: | Naruszenia kontroli urządzenia przekraczają podaną liczbę w określonym przedziale czasu. |

# Konfigurowanie zdarzeń dla powiadomień

Worry-Free Business Security oferuje trzy metody dostarczania powiadomień:

- powiadomienia SNMP
- dziennik zdarzeń systemu Windows.
- powiadomienia e-mail

**Procedura**

1. Przejdź do menu **Administracja** > **Powiadomienia**.
2. Aby otrzymywać powiadomienia SNMP, skonfiguruj sekcję **Odbiorca powiadomień SNMP**.

   Simple Network Management Protocol (SNMP) to protokół używany do zarządzania siecią. Aby wyświetlić dane z pułapki SNMP, należy użyć przeglądarki baz informacji zarządzania.

   a. Wybierz **Włącz powiadomienia SNMP**.

   b. Podaj adres IP pułapki SNMP.

   c. Określ łańcuch społeczności SNMP
3. Aby otrzymywać powiadomienia dziennika zdarzeń systemu Windows, wybierz opcję **Zapisuj do dziennika zdarzeń systemu Windows** w obszarze **Rejestrowanie**.

4. Aby otrzymywać powiadomienia e-mail, określ nadawcę i odbiorców.

**Porada**

Poszczególne wpisy należy oddzielać średnikami.

5. Kliknij kartę **Wymagana operacja** lub **Ostrzeżenia**.
6. W kolumnie **Powiadomienia e-mail** zaznacz pola wyboru odpowiadające typom zdarzeń, dla których chcesz otrzymywać powiadomienia.
7. Jeśli jest to dostępne, w kolumnie **Próg alarmu** określ liczbę wykrytych lub naruszeń w każdym okresie, który wyzwala powiadomienie.
8. Aby dostosować wiersz tematu i treść wiadomości każdego powiadomienia o zdarzeniu, kliknij łącze powiadomienia w kolumnie **Typ**.

   Aby uzyskać więcej informacji na temat dostosowywania powiadomień, zobacz *Zmienne znaczników na stronie 10-6*.
9. Kliknij przycisk **Zapisz**.

## Zmienne znaczników

Korzystając ze zmiennych znaczników można dostosować wiersz tematu i treść powiadomień o zdarzeniach.

Aby uniknąć oznaczania jako spam wiadomości e-mail przychodzących z domen zewnętrznych, należy dodać zewnętrzne adresy e-mail do list dozwolonych nadawców oprogramowania antyspamowego.

Następujące znaczniki oznaczają groźne zdarzenia na komputerach/serwerach i serwerach Microsoft Exchange.

| TOKEN | OPIS | TYP ALARMU |
|---|---|---|
| `%LICZBA` | Wstawia liczbę przypadków wykrycia | Zdarzenia ostrzegawcze: Wszystkie |

| Token | Opis | Typ alarmu |
|---|---|---|
| *$CSM_SERVERNAME* | Wstawia nazwę serwera Security Server | Wszystkie |
| *%DATA* | Wstawia liczbę dni ważności licencji | Licencja — wygasła<br>Licencja — do wygaśnięcia pozostało mniej niż 60 dni |
| *%DATA_GODZINA* | Wstawia godzinę i datę zdarzenia | Antywirus — niezneutralizowane zagrożenia<br>Antywirus — skanowanie w czasie rzeczywistym wyłączone w punktach końcowych<br>Antywirus — wyłączono skanowanie serwerów Exchange w czasie rzeczywistym<br>Zabezpieczenie przed spyware - przypadki wykrycia wymagające ponownego uruchomienia urządzenia<br>Aktualizacja — nieaktualne agenty<br>Aktualizacja — nieaktualne agenty Messaging Security Agent<br>Aktualizacja — nieaktualne składniki programu Security Server<br>Usługi Smart Protection — usługa niedostępna<br>Niedobór zasobów — pozostałe miejsce na dysku |

| TOKEN | OPIS | TYP ALARMU |
|---|---|---|
| *%DEVICE_COUNT* | Wstawia liczbę urządzeń, których dotyczy problem | Antywirus — niezneutralizowane zagrożenia<br><br>Antywirus — skanowanie w czasie rzeczywistym wyłączone w punktach końcowych<br><br>Antywirus — wyłączono skanowanie serwerów Exchange w czasie rzeczywistym<br><br>Zabezpieczenie przed spyware - przypadki wykrycia wymagające ponownego uruchomienia urządzenia<br><br>Aktualizacja — nieaktualne agenty<br><br>Aktualizacja — nieaktualne agenty Messaging Security Agent<br><br>Niedobór zasobów — pozostałe miejsce na dysku<br><br>Wszystkie zdarzenia ostrzegawcze z wyjątkiem następujących:<br><br>Antyspam — przypadki wykrycia spamu w całkowitej liczbie odebranych wiadomości przekraczają: |

| Token | Opis | Typ alarmu |
|---|---|---|
| *%OD* | Wstawia datę rozpoczęcia i datę zdarzenia | Wszystkie zdarzenia ostrzegawcze z wyjątkiem następujących:<br><br>Antyspam — przypadki wykrycia spamu w całkowitej liczbie odebranych wiadomości przekraczają: |
| *%LICZBA* | Wyświetla liczbę zdarzeń | Antywirus — niezneutralizowane zagrożenia<br><br>Antywirus — skanowanie w czasie rzeczywistym wyłączone w punktach końcowych<br><br>Antywirus — wyłączono skanowanie serwerów Exchange w czasie rzeczywistym<br><br>Zabezpieczenie przed spyware - przypadki wykrycia wymagające ponownego uruchomienia urządzenia<br><br>Wszystkie zdarzenia ostrzegawcze z wyjątkiem następujących:<br><br>Antyspam — przypadki wykrycia spamu w całkowitej liczbie odebranych wiadomości przekraczają: |

| Token | Opis | Typ alarmu |
|---|---|---|
| *%SEAT_IN_USE_COUNT* | Wstawia liczbę używanych komputerów/serwerów | Licencja — liczba wykorzystanych stanowisk przekracza 110%<br><br>Licencja — liczba wykorzystanych stanowisk przekracza 100% |
| *%SEAT_PURCHASED_COUNT* | Wstawia liczbę komputerów/serwerów dostępnych w Twojej licencji | Licencja — liczba wykorzystanych stanowisk przekracza 110%<br><br>Licencja — liczba wykorzystanych stanowisk przekracza 100% |
| *%PRÓG%* | Podaje próg zdarzenia | Aktualizacja — nieaktualne agenty<br><br>Aktualizacja — nieaktualne sygnatury Smart Scan<br><br>Aktualizacja — nieaktualne składniki programu Security Server<br><br>Usługi Smart Protection — usługa niedostępna<br><br>Niedobór zasobów — pozostałe miejsce na dysku<br><br>Licencja — wykorzystanie stanowisk przekracza wartość 110%<br><br>Licencja — wykorzystanie stanowisk przekracza wartość 100%<br><br>Zdarzenia ostrzegawcze: Wszystkie |

| TOKEN | OPIS | TYP ALARMU |
|---|---|---|
| *%DO* | Wstawia końcowy czas i datę zdarzenia | Wszystkie zdarzenia ostrzegawcze z wyjątkiem następujących:<br><br>Antyspam — przypadki wykrycia spamu w całkowitej liczbie odebranych wiadomości przekraczają: |

```
Subject: [Security Server - <$CSM_SERVERNAME>] [Action
Required] Antivirus - Threats unresolved: %NUMBER
Message: Trend Micro Worry-Free Business Security Notification
* Antivirus - Threats unresolved: %NUMBER
* Report time: %DATE_TIME
* Affected devices: %DEVICE_COUNT
* Suggestion:
  Run a scan using the Trend Micro HouseCall Tool.
```

```
Subject: [Security Server - Server A] [Action Required]
Antivirus - Threats unresolved: 5
Message: Trend Micro Worry-Free Business Security Notification
* Antivirus - Threats unresolved: 5
* Report time: February 14, 2018
* Affected devices: 2
* Suggestion:
  Run a scan using the Trend Micro HouseCall Tool.
```

# Rozdział 11

# Zarządzanie ustawieniami globalnymi

W tym rozdziale omówiono ustawienia globalne agentów oraz ustawienia systemowe programu Security Server.

# Ustawienia globalne

Za pomocą konsoli internetowej można konfigurować globalne ustawienia programów Security Server i Security Agent.

| KARTA | OPIS |
|---|---|
| **Serwer proxy** | Jeśli w sieci do łączenia się z Internetem używany jest serwer proxy, należy określić ustawienia serwera proxy dla następujących usług:<br>• Aktualizacje składników i powiadomienia o licencji<br>• Usługi Web Reputation, Monitorowanie zachowania i Smart Scan<br>Aby uzyskać więcej informacji, zobacz *Konfigurowanie ustawień serwera proxy w sieci Internet na stronie 11-3*. |
| **SMTP** | Ustawienia serwera SMTP stosuje się do wszystkich powiadomień i raportów generowanych przez program Security Server.<br>Aby uzyskać więcej informacji, zobacz *Konfigurowanie ustawień serwera SMTP na stronie 11-4*. |
| **Komputer/serwer** | Ustawienia zabezpieczeń dotyczą wszystkich programów Security Agent.<br>Aby uzyskać więcej informacji, zobacz *Konfigurowanie ustawień komputerów/serwerów na stronie 11-5*. |
| **System** | Ustawienia systemowe umożliwiają automatyczne usuwanie nieaktywnych agentów, sprawdzanie połączenia agentów i utrzymywanie folderu kwarantanny.<br>Aby uzyskać więcej informacji, zobacz *Konfigurowanie ustawień systemu na stronie 11-10*. |
| **Wyjątki** | Listy wyjątków umożliwiają zastąpienie ustawień zasad zdefiniowanych w usłudze Web Reputation, Filtrowanie adresów URL i Przewidujące uczenie maszynowe.<br>Aby uzyskać więcej informacji, zobacz *Konfigurowanie ustawień listy wyjątków na stronie 11-14*. |

# Konfigurowanie ustawień serwera proxy w sieci Internet

Jeśli programy Security Server i agenty wykorzystują do łączenia się z Internetem serwer proxy, należy określić ustawienia serwera proxy w celu korzystania z następujących funkcji i usług oferowanych przez firmę Trend Micro:

- **Serwer Security Server**: aktualizacje składników i obsługa licencji
- **Agenty Security Agent**: usługi Web Reputation, filtrowanie adresów URL, monitorowanie zachowania, Smart Feedback i Smart Scan.
- **Programy Messaging Security Agent** (tylko w wersji Advanced): usługi Web Reputation i Anti-spam

---

**Procedura**

1. Przejdź do menu **Administracja** > **Ustawienia globalne**.
2. Zmień odpowiednio następujące opcje na karcie **Serwer proxy**:
   - Serwer proxy programu Security Server

     **Uwaga**

     Programy Messaging Security Agent także używają ustawień proxy programu Security Server.

     - Używaj serwera proxy podczas aktualizacji produktu oraz powiadamiania o licencji produktu
     - Używaj protokołu SOCKS 4/5 serwera proxy
     - Address: Adres IPv4/IPv6 lub nazwa hosta
     - Port
     - Uwierzytelnianie serwera proxy
       - Nazwa użytkownika

- Hasło

- Serwer proxy programu Security Agent
  - Należy zastosować poświadczenia określone dla serwera proxy aktualizacji

**Uwaga**

Programy Security Agent używają do łączenia się z Internetem serwera proxy i portu programu Internet Explorer. Wybierz tę opcję tylko wtedy, jeśli program Internet Explorer na klientach i program Security Server współdzielą te same poświadczenia uwierzytelniania.

  - Nazwa użytkownika
  - Hasło

3. Kliknij przycisk **Zapisz**.

# Konfigurowanie ustawień serwera SMTP

Ustawienia serwera SMTP stosuje się do wszystkich powiadomień i raportów, generowanych przez program Worry-Free Business Security.

**Procedura**

1. Przejdź do menu **Administracja** > **Ustawienia globalne**.
2. Kliknij kartę **SMTP** i zmień odpowiednio następujące opcje:
   - **Serwer SMTP**: Adres IPv4/IPv6 lub nazwa serwera SMTP.
   - **Port**
   - **Włącz uwierzytelnianie serwera SMTP**
     - Nazwa użytkownika

- Hasło

3. Aby sprawdzić, czy ustawienia są prawidłowe, kliknij opcję **Wyślij testową wiadomość e-mail**. Jeśli wysyłanie się nie powiedzie, zmodyfikuj ustawienia lub sprawdź stan serwera SMTP.

4. Kliknij przycisk **Zapisz**.

# Konfigurowanie ustawień komputerów/serwerów

Opcje komputera/serwera odnoszą się do ustawień globalnych programu Worry-Free Business Security. Ustawienia dla poszczególnych grup zastępują te ustawienia. Jeśli nie skonfigurowano określonej opcji dla grupy, używane są opcje komputera/serwera. Na przykład w przypadku braku dozwolonych adresów URL dla określonej grupy zostaną zastosowane do niej wszystkie adresy URL dozwolone na tym ekranie.

**Procedura**

1. Przejdź do menu **Administracja** > **Ustawienia globalne**.

2. Kliknij kartę **Komputer/serwer** i zmień odpowiednio następujące opcje:

| USTAWIENIA | OPIS |
|---|---|
| Rozpoznawanie lokalizacji | Rozpoznawanie lokalizacji pozwala administratorom kontrolować ustawienia zabezpieczeń w zależności od sposobu połączenia klienta z siecią.<br><br>Funkcja rozpoznawania lokalizacji steruje ustawieniami połączeń W biurze i Poza biurem.<br><br>Program Security Agent automatycznie identyfikuje lokalizację klienta na podstawie informacji o bramie skonfigurowanych w konsoli internetowej, a następnie kontroluje witryny, do których użytkownicy mogą uzyskiwać dostęp. Ograniczenia różnią się w zależności od lokalizacji użytkownika: |

| Ustawienia | Opis |
|---|---|
| | • **Włącz rozpoznawanie lokalizacji**: te ustawienia wpłyną na ustawienia połączeń W biurze/Poza biurem usług Zapora i Web Reputation, a także na częstotliwość zaplanowanych aktualizacji.<br>• **Informacje o bramie**: klienty i połączenia na tej liście będą korzystać z ustawień Połączenie wewnętrzne podczas zdalnego łączenia się z siecią (przy użyciu sieci VPN), jeśli włączone jest rozpoznawanie lokalizacji.<br>  • Adres IP bramy<br>  • Adres MAC: dodanie adresu MAC znacznie zwiększa bezpieczeństwo, umożliwiając łączenie tylko skonfigurowanym urządzeniom.<br>Aby usunąć wpis, kliknij odpowiadającą mu ikonę usuwania (x). |
| Powiadomienie pomocy technicznej | Opcja powiadomienia pomocy technicznej umieszcza w programie Security Agent wiadomość zawierającą dane kontaktowe osoby, która może udzielić pomocy. Zmień odpowiednio następujące ustawienia:<br>• **Etykieta pomocy technicznej**<br>• **Adres e-mail pomocy technicznej**<br>• **Dodatkowe informacje**: te informacje są wyświetlane po ustawieniu wskaźnika myszy nad etykietą. |
| Ogólne ustawienia skanowania | • **Wyłącz usługę skanowania Smart Scan**: przełącza wszystkie programy Security Agent w tryb Skanowanie standardowe. Skanowanie Smart Scan będzie niedostępne do chwili ponownego włączenia. Aby przełączyć grupę jednego lub kilku programów Security Agent, przejdź do opcji **Urządzenia** > **{Grupa}** > **Konfiguruj regułę** > **Metoda skanowania**. |

| USTAWIENIA | OPIS |
|---|---|
| | **Uwaga**<br>Wytyczne na temat przełączania metod skanowania w programach Security Agent zawiera część *Konfiguracja metod skanowania na stronie 5-5*.<br>• **Włącz odroczone skanowanie w odniesieniu do operacji na plikach**: Włącz to ustawienie, aby tymczasowo poprawić wydajność systemu.<br>**OSTRZEŻENIE!**<br>Włączenie opcji odroczonego skanowania może wiązać się z zagrożeniem bezpieczeństwa.<br>• **Wyklucz sekcje funkcji Shadow Copy**: usługi Shadow Copy lub Volume Snapshot Service tworzą ręcznie lub automatycznie kopie zapasowe lub obrazy pliku albo folderu na określonym woluminie.<br>• **Wyklucz folder bazy danych serwera Security Server**: agenty zainstalowane na Security Server nie będą skanować własnej bazy danych podczas skanowania w czasie rzeczywistym.<br>Domyślnie program WFBS nie skanuje własnej bazy danych. Firma Trend Micro zaleca zachowanie tego ustawienia, aby zapobiec ewentualnemu uszkodzeniu bazy danych podczas skanowania.<br>• **Wyklucz foldery serwera Microsoft Exchange, jeśli program zainstalowano na serwerze Microsoft Exchange**: agenty zainstalowane na serwerze Microsoft Exchange nie będą skanować folderów Microsoft Exchange.<br>• **Wyklucz foldery kontrolerów domen firmy Microsoft**: agenty zainstalowane na serwerze kontrolera domeny nie będą skanować folderów kontrolera domeny. Te foldery zawierają informacje o użytkownikach, nazwy użytkowników, hasła i inne ważne informacje. |

| Ustawienia | Opis |
|---|---|
| Ustawienia skanowania w poszukiwaniu wirusów | • **Konfiguruj ustawienia skanowania dużych skompresowanych plików**: określ maksymalną wielkość zdekompresowanego pliku oraz liczbę plików w skompresowanym pliku do przeskanowania przez agenta.<br>• **Wyczyść skompresowane pliki**: agenty wykonają próbę wyczyszczenia zarażonych plików w skompresowanym pliku.<br>• **Skanuj do {} warstw OLE**: agenty będą skanować określoną liczbę warstw OLE (Object Linking and Embedding). Warstwy OLE umożliwiają tworzenie obiektów w jednej aplikacji, a następnie łączenie lub osadzanie ich w innej aplikacji. Przykładem może być plik .xls osadzony w pliku .doc.<br>• **Dodaj skrót do skanowania ręcznego do menu skrótów Windows na klientach**: dodaje łącze **Skanuj za pomocą programu Security Agent** do menu kontekstowego. Dzięki temu użytkownicy mogą kliknąć prawym przyciskiem myszy plik lub folder (na pulpicie lub w Eksploratorze Windows) i ręcznie przeskanować ten plik lub folder. |
| Ustawienia skanowania w poszukiwaniu oprogramowania spyware/grayware | • **Skanuj w poszukiwaniu plików cookie**: Program Security Agent przeprowadza skanowanie pod kątem plików cookie.<br>• **Dodaj wykryte pliki cookie do dziennika spyware**: dodaje każdy wykryty plik cookie zidentyfikowany jako spyware do dziennika spyware. |
| Ustawienia zapory | Wybierz pole **Wyłącz zaporę i odinstaluj sterowniki** w celu odinstalowania zapory klienta Worry-Free Business Security i usunięcia sterowników powiązanych z zaporą.<br><br>**Uwaga**<br>Jeśli zapora zostanie wyłączona, to powiązane ustawienia będą dostępne dopiero w przypadku ponownego jej włączenia. |

| USTAWIENIA | OPIS |
|---|---|
| Ochrona protokołu sieciowego HTTPS przed zagrożeniami internetowymi | Włącz tę funkcję, aby uruchomić sprawdzanie adresów URL HTTPS za pomocą usługi Web Reputation i na podstawie ustawień filtrowania adresów URL w przeglądarkach Chrome, Firefox i Microsoft Edge.<br><br>**Uwaga**<br>• Ta funkcja nie obsługuje sprawdzania witryn korzystających z protokołu HTTP/2.<br>Aby uzyskać listę nieobsługiwanych witryn, zobacz http://esupport.trendmicro.com/solution/en-us/1116889.aspx.<br>• Ta funkcja nie wymaga dodatku do przeglądarki.<br>Domyślnie program Worry-Free Business Security sprawdza adresy URL dla protokołu HTTPS w programie Internet Explorer za pomocą dodatków do przeglądarki. |
| Ustawienia ostrzeżeń | **Pokaż ikonę ostrzegawczą na pasku zadań systemu Windows, jeżeli plik sygnatur wirusów nie został uaktualniony w ciągu {} dni** Wyświetla ikonę ostrzegawczą na klientach, gdy plik sygnatur nie został zaktualizowany po upływie określonej liczby dni. |
| Hasło dezinstalacji programu Security Agent | • **Zezwól klientowi na odinstalowanie programu Security Agent bez wymagania hasła**<br>• **Wymagaj hasła od użytkownika, aby odinstalować program Security Agent** |
| Wprowadź hasło zamykania i odblokowania programu Security Agent. | • **Pozwalaj klientom zamykać i odblokowywać program Security Agent na komputerach bez wprowadzania hasła.**<br>• **Wymagaj od klientów wprowadzania hasła podczas zamykania i odblokowywania programu Security Agent.** |

| Ustawienia | Opis |
|---|---|
| | **Uwaga**<br>Odblokowanie programu Security Agent umożliwia użytkownikowi zastąpienie wszystkich ustawień skonfigurowanych na ekranie **Urządzenia** > **{grupa}** > **Konfiguruj regułę** > **Uprawnienia agenta**. |
| Preferowany adres IP | Ustawienie to jest dostępne wyłącznie na serwerach Security Server z dwoma stosami i stosowane tylko do agentów z dwoma stosami.<br><br>Po zainstalowaniu lub zaktualizowaniu agenty rejestrują się na serwerze Security Server przy użyciu adresu IP.<br><br>Wybierz jedną z następujących opcji:<br><br>• **Najpierw IPv4, potem IPv6**: agenty 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.<br><br>• **Najpierw IPv6, potem IPv4**: agenty najpierw używają 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. |

3. Kliknij przycisk **Zapisz**.

# Konfigurowanie ustawień systemu

Sekcja **System** ekranu **Ustawienia globalne** zawiera opcje służące do automatycznego usuwania nieaktywnych agentów, sprawdzania połączeń agentów oraz obsługi folderu kwarantanny.

**Procedura**

1. Przejdź do menu **Administracja** > **Ustawienia globalne**.

2. Kliknij kartę **System** i zmień odpowiednio następujące opcje:

| Ustawienia | Opis |
|---|---|
| Usuwanie nieaktywnego programu Security Agent | W przypadku odinstalowywania programu Security Agent z klienta za pomocą jego własnego dezinstalatora program automatycznie powiadamia program Security Server. Gdy program Security Server otrzyma to powiadomienie, usunie ikonę klienta z drzewa grup zabezpieczeń, wskazując w ten sposób, że dany klient już nie istnieje.<br><br>Jeśli jednak program Security Agent zostanie usunięty inną metodą, na przykład w wyniku formatowania dysku twardego komputera lub ręcznego usunięcia plików klienta, do programu Security Server nie dotrą informacje o usunięciu, a program Security Agent będzie wyświetlany jako nieaktywny. Jeśli użytkownik usunie z pamięci program Security Agent lub wyłączy go na dłuższy czas, program Security Server również będzie wyświetlać program Security Agent jako nieaktywny.<br><br>Aby w drzewie grup zabezpieczeń były wyświetlane tylko aktywne klienty, można skonfigurować program Security Server tak, aby automatycznie usuwał nieaktywne programy Security Agent z drzewa grup zabezpieczeń.<br><br>• **Włącz automatyczne usuwanie nieaktywnego programu Security Agent**: Umożliwia automatyczne usuwanie klientów, które nie nawiązały kontaktu z programem Security Server przez określoną liczbę dni.<br><br>• **Automatycznie usuń program Security Agent, jeśli jest nieaktywny przez {} dni**: liczba dni, przez które klient może być nieaktywny, zanim zostanie usunięty z konsoli internetowej. |

| Ustawienia | Opis |
|---|---|
| Sprawdzanie połączenia agenta | W programie Worry-Free Business Security stan połączenia klienta jest przedstawiany w drzewie grup zabezpieczeń w postaci ikon. Jednak niektóre warunki mogą uniemożliwiać wyświetlanie właściwego stanu połączenia agenta w drzewie grup zabezpieczeń. Na przykład przypadkowe odłączenie kabla sieciowego klienta może uniemożliwić agentowi powiadomienie programu Trend Micro Security Server, że klient jest w trybie offline. W drzewie grup zabezpieczeń stan tego agenta będzie wciąż wyświetlany jako online.<br><br>Połączenie agent-serwer można sprawdzić ręcznie lub według harmonogramu za pomocą konsoli internetowej.<br><br>**Uwaga**<br>W funkcji sprawdzania połączenia nie można wybierać określonych grup lub agentów. Sprawdza ona połączenie ze wszystkimi agentami zarejestrowanymi w programie Security Server.<br><br>• **Włącz sprawdzanie zaplanowane**: Włącza zaplanowane sprawdzanie połączenia agent-serwer.<br>  • **Co godzinę**<br>  • **Codziennie**<br>  • **Co tydzień, w**<br>  • **Godzina rozpoczęcia**: godzina rozpoczęcia sprawdzania.<br>• **Sprawdź teraz**: sprawdza połączenie natychmiast. |

| USTAWIENIA | OPIS |
|---|---|
| Obsługa kwarantanny | Domyślnie programy Security Agent wysyłają zakażone pliki objęte kwarantanną do następującego katalogu na serwerze Security Server:<br><br>`<folder instalacji programu Security Server>\PCCSRV\Virus`<br><br>Jeśli konieczna jest zmiana katalogu (na przykład gdy na dysku jest za mało miejsca), należy wpisać w polu **Katalog kwarantanny** ścieżkę bezwzględną, na przykład `D:\Pliki poddane kwarantannie`. W takim przypadku należy wprowadzić te same zmiany również na ekranie **Urządzenia** > **{Grupa}** > **Konfiguruj regułę** > **Kwarantanna**, w przeciwnym razie agenty będą nadal wysyłać pliki do lokalizacji `<folder instalacji programu Security Server>\PCCSRV\Virus`.<br><br>Dodatkowo należy skonfigurować następujące ustawienia obsługi:<br><br>• **Pojemność folderu kwarantanny:**: Rozmiar folderu kwarantanny w megabajtach.<br><br>• **Maksymalny rozmiar pojedynczego pliku:**: Maksymalny rozmiar (w megabajtach) pojedynczego pliku zapisanego w folderze kwarantanny.<br><br>• **Usuń wszystkie pliki poddane kwarantannie**: Usuwa wszystkie pliki w folderze Kwarantanna. Jeśli folder jest pełny i załadowany zostanie nowy plik, nie zostanie on zapisany.<br><br>Jeśli nie chcesz, aby agenty wysyłały pliki poddane kwarantannie do serwera Security Server, skonfiguruj nowy katalog na ekranie **Urządzenia** > **{Grupa}** > **Konfiguruj regułę** > **Kwarantanna** i zignoruj wszystkie ustawienia obsługi. Instrukcje zawiera sekcja *Katalog kwarantanny na stronie 5-18*. |

| USTAWIENIA | OPIS |
|---|---|
| Instalacja programu Security Agent | **Katalog instalacji programu Security Agent**: Podczas instalacji wyświetlany jest monit o podanie katalogu instalacji programu Security Agent, czyli miejsca, w którym program instalacyjny zainstaluje poszczególne programy Security Agent.<br><br>W razie potrzeby można zmienić katalog, wpisując ścieżkę bezwzględną. Tylko przyszłe agenty zostaną zainstalowane w tym katalogu. Istniejące agenty pozostaną w bieżącym katalogu.<br><br>Aby skonfigurować ścieżkę instalacji, można użyć jednej z następujących zmiennych:<br><br>• `$BOOTDISK`: Litera dysku rozruchowego<br>• `$WINDIR`: Folder, w którym zainstalowano system Windows<br>• `$ProgramFiles`: Folder programów |

3. Kliknij przycisk **Zapisz**.

# Konfigurowanie ustawień listy wyjątków

**Procedura**

1. Przejdź do menu **Administracja** > **Ustawienia globalne**.
2. Kliknij kartę **Wyjątki** i zmień odpowiednio następujące opcje:

| SEKCJA | OPIS |
|---|---|
| Usługa Web Reputation i filtrowanie adresów URL | • **Lista dozwolonych adresów URL**:Strony internetowe (i ich subdomeny) wykluczone z weryfikacji usługi Web Reputation i filtrowania adresów URL. |

| SEKCJA | OPIS |
|---|---|
| | **Uwaga**<br>Lista elementów zatwierdzonych ma wyższy priorytet niż lista elementów zablokowanych. Gdy adres URL pasuje do wpisu na liście dozwolonych, agenty zawsze zezwalają na dostęp do adresu URL, nawet jeśli znajduje się on na liście zablokowanych.<br>Lista niestandardowych dozwolonych lub zablokowanych adresów URL w odniesieniu do określonej grupy powoduje zastąpienie globalnych ustawień wyjątków.<br>• **Lista zablokowanych adresów URL**:Strony internetowe (i ich subdomeny), które są zawsze blokowane podczas filtrowania adresów URL.<br>• **Listy wyjątków procesów**:procesy wyłączone z weryfikacji prowadzonej przez usługi Web Reputation i Filtrowanie adresów URL. Wpisz procesy krytyczne uznawane przez organizację za godne zaufania.<br>**Porada**<br>Po zaktualizowaniu listy wyjątków procesów i zainstalowaniu przez serwer zaktualizowanej listy na agentach wszystkie aktywne połączenia HTTP z komputerem klienckim (przez porty 80, 81 lub 8080) zostaną na parę sekund rozłączone. Z tego powodu warto aktualizować listę wyjątków poza godzinami największego obciążenia.<br>• **Lista wyjątków IP**:Adresy IP (np. 192.168.0.1) wyłączone z weryfikacji usługi Web Reputation i filtrowania adresów URL. Wpisz krytyczne adresy IP, które Twoja organizacja uważa za godne zaufania. |

| SEKCJA | OPIS |
|---|---|
| | • **Wysyłanie dzienników funkcji Web Reputation i Filtrowanie adresów URL do programu Security Server** |
| Lista wyjątków przewidującego uczenia maszynowego | Skonfiguruj wyjątki globalnego mechanizmu przewidywania operacji uczenia maszynowego, aby uniemożliwić wszystkim programom Security Agent wykrycie pliku jako złośliwego. Wpisz wartość skrótu SHA-1 pliku, aby wykluczyć go ze skanowania. Opcjonalnie dodaj notatkę dotyczącą przyczyny wyjątku lub opisz nazwę pliku powiązaną z wartością skrótu. |

3. Kliknij przycisk **Zapisz**.

# Rozdział 12

# Korzystanie z dzienników i raportów

W tym rozdziale opisano sposób korzystania z dzienników i raportów programu do monitorowania systemu i analizy zabezpieczeń.

# Dzienniki

W programie Worry-Free Business Security prowadzone są wszechstronne dzienniki, w których odnotowywane są informacje o przypadkach wykrycia wirusa/złośliwego oprogramowania oraz oprogramowania typu spyware/grayware, zdarzeniach i aktualizacjach. Dzienników tych można użyć do oceny reguł ochrony organizacji, jak również do identyfikacji klientów, które są bardziej narażone na zarażenie, a także sprawdzenia, czy aktualizacje zostały prawidłowo wdrożone.

**Uwaga**

Do przeglądania plików dziennika w formacie CSV służą arkusze kalkulacyjne, takie jak Microsoft Excel.

Program Worry-Free Business Security prowadzi dzienniki w następujących kategoriach:

- Dzienniki zdarzeń konsoli internetowej
- Dzienniki komputerów/serwerów
- Dzienniki serwera Microsoft Exchange (tylko wersja Advanced)

**TABELA 12-1. Typ i zawartość dziennika**

| TYP (OBIEKT, KTÓRY WYGENEROWAŁ WPIS DZIENNIKA) | ZAWARTOŚĆ (TYP DZIENNIKA, Z KTÓREGO POBIERANA JEST ZAWARTOŚĆ) |
|---|---|
| Zdarzenia konsoli zarządzania | • Skanowanie ręczne (uruchamiane za pomocą konsoli internetowej)<br>• Aktualizacja (aktualizacje serwera Security Server)<br>• Zdarzenia konsoli |

| Typ (obiekt, który wygenerował wpis dziennika) | Zawartość (typ dziennika, z którego pobierana jest zawartość) |
|---|---|
| Komputer/serwer | • Dzienniki wirusów<br>  • Skanowanie ręczne<br>  • Skanowanie w czasie rzeczywistym<br>  • Skanowanie zaplanowane<br>• Dzienniki oprogramowania typu spyware/grayware<br>  • Skanowanie ręczne<br>  • Skanowanie w czasie rzeczywistym<br>  • Skanowanie zaplanowane<br>• Dzienniki przewidującego uczenia maszynowego<br>• Dzienniki usługi Web Reputation<br>• Dzienniki filtrowania adresów URL<br>• Dzienniki monitorowania zachowania<br>• Dzienniki aktualizacji<br>• Dzienniki wirusów sieciowych<br>• Dzienniki zdarzeń<br>• Dzienniki kontroli urządzeń<br>• Aktualizuj dzienniki wdrożenia<br>• Dzienniki ataków typu ransomware<br>  • Ochrona antywirusowa<br>  • Monitorowanie zachowania<br>  • Usługa Web Reputation<br>  • Filtrowanie adresów URL<br>  • Przewidujące uczenie maszynowe |

| Typ (obiekt, który wygenerował wpis dziennika) | Zawartość (typ dziennika, z którego pobierana jest zawartość) |
|---|---|
| Serwer Exchange (tylko w wersji Advanced) | • Dzienniki wirusów<br>• Dzienniki blokowania załączników<br>• Dzienniki funkcji Filtrowanie zawartości/Zapobieganie utracie danych<br>• Dzienniki aktualizacji<br>• Dzienniki kopii zapasowych<br>• Dzienniki archiwizacji<br>• Dzienniki zdarzeń skanowania<br>• Dzienniki części wiadomości, których nie można przeskanować<br>• Dzienniki usługi Web Reputation<br>• Dzienniki zdarzeń dotyczące urządzeń mobilnych |

## Korzystanie z kwerendy dziennika

W celu uzyskania informacji z bazy danych dziennika można wykonywać kwerendy dziennika. Do konfigurowania i uruchamiania kwerend można użyć ekranu **Kwerenda dziennika**. Wyniki można następnie wyeksportować do pliku w formacie .CSV lub wydrukować.

Program Messaging Security Agent (tylko wersja Advanced) co pięć minuty wysyła dzienniki do programu Security Server (niezależnie od tego, kiedy generowany jest dziennik).

---

**Procedura**

1. Przejdź do pozycji **Raporty** > **Kwerenda dziennika**.
2. Zmień odpowiednio następujące opcje:

- **Zakres czasu**
  - **Wstępnie skonfigurowany zakres**
  - **Określony zakres**: ogranicza kwerendę do określonych dat.
- **Typ**: zawartość każdego typu dziennika przedstawiono w części *Dzienniki na stronie 12-2*.
  - **Zdarzenia konsoli zarządzania**
  - **Komputer/serwer**
  - **Serwer Exchange** (tylko w wersji Advanced)
- **Zawartość**: dostępne opcje są zależne od **typu** dziennika.

3. Kliknij opcję **Wyświetl dzienniki**.
4. Aby zapisać dziennik jako plik w formacie CSV, kliknij opcję **Eksportuj**. Pliki CSV można przeglądać za pomocą arkusza kalkulacyjnego.

---

# Raporty

Raporty jednorazowe można generować ręcznie, można też skonfigurować program Security Server do generowania raportów zaplanowanych.

Raporty można wydrukować lub wysłać pocztą e-mail do administratora lub innych osób.

Dane dostępne w raporcie zależą od liczby dzienników dostępnych na serwerze Security Server w czasie generowania raportu. Liczba dzienników zmienia się w miarę dodawania nowych i usuwania istniejących dzienników. W sekcji **Raporty** > **Obsługa** można ręcznie usuwać dzienniki albo skonfigurować harmonogram ich usuwania.

# Praca z raportami jednorazowymi

**Procedura**

1. Przejdź do sekcji **Raporty** > **Raporty jednorazowe**.
2. Wykonaj następujące czynności:

| ZADANIE | CZYNNOŚCI |
|---|---|
| Generowanie raportu | a. Kliknij przycisk **Dodaj**.<br>Zostanie wyświetlony nowy ekran.<br>b. Skonfiguruj następujące elementy:<br>• **Nazwa raportu**<br>• **Zakres czasu**: ogranicza raport do określonych dat.<br>• **Zawartość**: aby wybrać wszystkie zagrożenia, zaznacz pole wyboru **Zaznacz wszystko**. Aby wybrać poszczególne zagrożenia, zaznacz odpowiednie pole wyboru. Kliknij ikonę z symbolem znaku plus (+), aby rozwinąć zaznaczenie.<br>• **Wyślij raport do**<br>  • **Odbiorcy**: wpisz adresy e-mail odbiorców, oddzielając je średnikami (;).<br>  • **Format**: wybierz plik PDF albo łącze do raportu w formacie HTML. Jeśli wybierzesz plik PDF, zostanie on załączony do wiadomości e-mail.<br>c. Kliknij przycisk **Dodaj**. |

| ZADANIE | CZYNNOŚCI |
|---|---|
| Wyświetlanie raportu | W kolumnie Nazwa raportu kliknij łącza do raportu. Pierwsze łącze spowoduje otwarcie raportu w formacie PDF, a drugie — w formacie HTML.<br><br>Dane dostępne w raporcie zależą od liczby dzienników dostępnych na serwerze Security Server w czasie generowania raportu. Liczba dzienników zmienia się w miarę dodawania nowych i usuwania istniejących dzienników. W sekcji **Raporty** > **Obsługa** można ręcznie usuwać dzienniki albo skonfigurować harmonogram ich usuwania.<br><br>Szczegółowe informacje dotyczące zawartości raportu zawiera część *Interpretowanie raportów na stronie 12-12*. |
| Usuwanie raportów | a. Wybierz wiersz zawierający łącza do raportu.<br><br>b. Kliknij przycisk **Usuń**.<br><br>**Uwaga**<br><br>Aby automatycznie usuwać raporty, przejdź do karty **Raporty** > **Obsługa** > **Raporty** i ustaw maksymalną liczbę raportów jednorazowych przechowywanych przez program Worry-Free Business Security. Domyślnie liczba raportów jednorazowych wynosi 10. Po jej przekroczeniu program Security Server usunie nadmiarowe raporty, zaczynając od przechowywanego przez najdłuższy czas. |

## Praca z raportami zaplanowanymi

**Procedura**

1. Przejdź do pozycji **Raporty** > **Raporty zaplanowane**.
2. Wykonaj następujące czynności:

| Zadanie | Czynności |
|---|---|
| Tworzenie szablonu raportu zaplanowanego | a. Kliknij przycisk **Dodaj**.<br><br>Zostanie wyświetlony nowy ekran.<br><br>b. Skonfiguruj następujące elementy:<br><br>• **Nazwa szablonu raportu**<br><br>• **Harmonogram**: Codziennie, co tydzień lub co miesiąc oraz godzina generowania raportu<br><br>Jeśli w przypadku raportów miesięcznych wybrana zostanie liczba 31, 30 lub 29, a dany miesiąc ma mniej dni, program WFBS nie wygeneruje raportu w tym miesiącu.<br><br>• **Zawartość**: aby wybrać wszystkie zagrożenia, zaznacz pole wyboru **Zaznacz wszystko**. Aby wybrać poszczególne zagrożenia, zaznacz odpowiednie pole wyboru. Kliknij ikonę z symbolem znaku plus (+), aby rozwinąć zaznaczenie.<br><br>• **Wyślij raport do**<br><br>• **Odbiorcy**: wpisz adresy e-mail odbiorców, oddzielając je średnikami (;).<br><br>• **Format**: wybierz plik PDF albo łącze do raportu w formacie HTML. Jeśli wybierzesz plik PDF, zostanie on załączony do wiadomości e-mail.<br><br>c. Kliknij przycisk **Dodaj**. |

| Zadanie | Czynności |
|---|---|
| Wyświetlanie raportów zaplanowanych | a. W wierszu zawierającym szablon, na podstawie którego generowane są raporty zaplanowane, kliknij pozycję **Historia raportów**.<br><br>Zostanie wyświetlony nowy ekran.<br><br>b. W kolumnie Widok kliknij łącza do raportu. Pierwsze łącze spowoduje otwarcie raportu w formacie PDF, a drugie — w formacie HTML.<br><br>Dane dostępne w raporcie zależą od liczby dzienników dostępnych na serwerze Security Server w czasie generowania raportu. Liczba dzienników zmienia się w miarę dodawania nowych i usuwania istniejących dzienników. W sekcji **Raporty** > **Obsługa** można ręcznie usuwać dzienniki albo skonfigurować harmonogram ich usuwania.<br><br>Szczegółowe informacje dotyczące zawartości raportu zawiera część *Interpretowanie raportów na stronie 12-12*. |
| **Zadania obsługi szablonów** | |
| Edytowanie ustawień szablonów | Kliknij szablon, a następnie zmień ustawienia na wyświetlonym ekranie.<br><br>Nowe ustawienia zostaną wykorzystane w raportach wygenerowanych po zapisaniu wprowadzonych zmian. |
| Włączanie/ wyłączanie szablonu | Kliknij ikonę w kolumnie Włączone.<br><br>Jeśli chcesz czasowo zatrzymać generowanie raportów zaplanowanych, wyłącz odpowiedni szablon. Jeśli raporty będą potrzebne ponownie, włącz szablon. |

| Zadanie | Czynności |
|---|---|
| Usuwanie szablonu | Zaznacz szablon i kliknij przycisk **Usuń**.<br><br>Usunięcie szablonu nie powoduje usunięcia wygenerowanych na jego podstawie raportów zaplanowanych, ale łącza do tych raportów nie będą już dostępne w konsoli internetowej. Dostęp do tych raportów można uzyskać bezpośrednio z komputera z programem Security Server. Raporty zostaną usunięte tylko wtedy, jeśli ręcznie usuniesz je z komputera albo gdy zostaną automatycznie usunięte przez program Security Server zgodnie z ustawieniem automatycznego usuwania raportów zaplanowanych na karcie **Raporty** > **Obsługa** > **Raporty**.<br><br>Aby automatycznie usuwać szablony, przejdź do karty **Raporty** > **Obsługa** > **Raporty** i ustaw maksymalną liczbę szablonów przechowywanych przez program Worry-Free Business Security. Domyślna liczba szablonów wynosi 10. Po jej przekroczeniu program Security Server usunie nadmiarowe szablony, zaczynając od przechowywanego przez najdłuższy czas. |
| **Zadania obsługi raportów** | |

| Zadanie | Czynności |
|---|---|
| Wysyłanie łącza do zaplanowanych raportów | Wyślij łącze do zaplanowanych raportów (w formacie PDF) pocztą elektroniczną. Odbiorcy mogą kliknąć łącze w wiadomości e-mail, aby uzyskać dostęp do pliku PDF. Upewnij się, że odbiorcy mogą łączyć się z komputerem z programem Security Server. W przeciwnym wypadku plik nie zostanie wyświetlony.<br><br>**Uwaga**<br>W wiadomości e-mail podawane jest tylko łącze do pliku PDF. Sam plik PDF nie jest załączany do wiadomości.<br><br>a. W wierszu zawierającym szablon, na podstawie którego generowane są raporty zaplanowane, kliknij pozycję **Historia raportów**.<br><br>Zostanie wyświetlony nowy ekran.<br><br>b. Wybierz raporty, a następnie kliknij przycisk **Wyślij**.<br><br>Otworzy się domyślny program pocztowy z nową wiadomością e-mail zawierającą łącze do raportu. |

| ZADANIE | CZYNNOŚCI |
|---|---|
| Usuwanie raportów zaplanowanych | a. W wierszu zawierającym szablon, na podstawie którego generowane są raporty zaplanowane, kliknij pozycję **Historia raportów**.<br><br>Zostanie wyświetlony nowy ekran.<br><br>b. Zaznacz raporty i kliknij przycisk **Usuń**.<br><br>**Uwaga**<br>Aby automatycznie usuwać raporty, przejdź do karty **Raporty** > **Obsługa** > **Raporty** i dla każdego szablonu ustaw maksymalną liczbę raportów zaplanowanych przechowywanych przez program Worry-Free Business Security. Domyślna liczba raportów zaplanowanych wynosi 10. Po jej przekroczeniu program Security Server usunie nadmiarowe raporty, zaczynając od przechowywanego przez najdłuższy czas. |

## Interpretowanie raportów

Raporty programu Worry-Free Business Security zawierają następujące informacje. Wyświetlone informacje mogą być różne, w zależności od wybranych opcji.

**TABELA 12-2. Zawartość raportu**

| ELEMENT RAPORTU | OPIS |
|---|---|
| Ochrona antywirusowa | **Podsumowanie aktywności wirusów na komputerach/ serwerach**<br><br>Raporty o wirusach zawierają szczegółowe informacje dotyczące liczby i typów złośliwego oprogramowania/wirusów wykrytych przez silnik skanowania oraz operacji wykonanych w celu ich usunięcia. Raport zawiera także spis najczęściej występujących wirusów/złośliwego oprogramowania. Klikając nazwę wirusa/ złośliwego oprogramowania, można otworzyć nową stronę przeglądarki internetowej i przejść do encyklopedii wirusów/ złośliwego oprogramowania firmy Trend Micro w celu uzyskania dodatkowych informacji na temat danego wirusa/złośliwego oprogramowania. |
| | **5 komputerów/serwerów z największą liczbą wykrytych wirusów**<br><br>Wyświetla 5 komputerów lub serwerów najczęściej raportujących wykrycie wirusa/złośliwego oprogramowania. Śledzenie najczęstszych przypadków wirusów/złośliwego oprogramowania na jednym komputerze klienckim może wykazać, że dany klient stanowi duże zagrożenie dla bezpieczeństwa, co może wymagać podjęcia dodatkowych działań. |

| Element raportu | Opis |
|---|---|
| Ochrona antyszpiegowska | **Podsumowanie aktywności spyware/grayware na komputerach/serwerach**<br><br>W raportach dotyczących spyware/grayware przedstawione są szczegółowe informacje o wykrytym na klientach oprogramowaniu spyware/grayware zawierające liczbę wykrytych przypadków i działania podjęte przeciw nim przez program WFBS. Raport zawiera diagram kołowy, pokazujący udział procentowy wszystkich operacji skanowania podjętych przeciw programom spyware. |
| | **5 komputerów/serwerów z największą ilością wykrytego spyware/grayware**<br><br>W raporcie wymieniono też pięć najgroźniejszych wykrytych przypadków spyware/grayware i pięć komputerów/serwerów z największą liczbą wykrytych przypadków spyware/grayware. Aby dowiedzieć się więcej o zagrożeniach ze strony spyware/grayware, kliknij nazwy spyware/grayware. Zostanie otwarta nowa strona przeglądarki internetowej, na której będą wyświetlone informacje o spyware/grayware pochodzące z witryny internetowej firmy Trend Micro. |
| Podsumowanie ochrony przed spamem (tylko w wersji Advanced) | **Podsumowanie działalności spamu**<br><br>Raporty antyspamowe zawierają informacje o liczbie wiadomości typu spam i phishing wykrytych we wszystkich przeskanowanych wiadomościach. Zawierają listę zgłoszonych fałszywych alarmów. |
| Przewidujące uczenie maszynowe | **5 programów najczęściej naruszających reguły przewidujące uczenie maszynowe** |
| | **10 komputerów najczęściej naruszających reguły predyktywnego uczenia maszynowego** |
| Usługa Web Reputation | **10 komputerów najczęściej naruszających reguły usług Web Reputation** |

| Element raportu | Opis |
|---|---|
| Kategoria adresu URL | **5 najczęściej naruszanych reguł kategorii URL**<br>Najczęściej używane kategorie witryn internetowych, związane z naruszeniami reguł. |
| | **10 komputerów najczęściej naruszających reguły kategorii URL** |
| Monitorowanie zachowania | **5 programów najczęściej naruszających reguły monitorowania zachowania** |
| | **10 komputerów najczęściej naruszających reguły monitorowania zachowania** |
| Kontrola urządzeń | **10 komputerów najczęściej naruszających zasady kontroli urządzeń** |
| Podsumowanie filtrowania zawartości (tylko w wersji Advanced) | **Podsumowanie filtrowania zawartości**<br>Raporty filtrowania zawartości zawierają informacje o liczbie wszystkich wiadomości przefiltrowanych przez program Messaging Security Agent. |
| | **10 najczęściej naruszanych reguł filtrowania zawartości**<br>Lista 10 najczęściej naruszanych reguł filtrowania zawartości. Informacje te umożliwiają lepsze dostosowanie reguł filtrowania. |
| Wirus sieciowy | **10 najczęściej wykrywanych wirusów sieciowych**<br>Zawiera listę 10 wirusów sieciowych najczęściej wykrywanych przez ogólny sterownik zapory.<br>Klikając nazwę wirusa, można otworzyć nową stronę przeglądarki internetowej i przejść do encyklopedii wirusów firmy Trend Micro w celu uzyskania dodatkowych informacji na temat danego wirusa. |
| | **10 najczęściej atakowanych komputerów**<br>Lista komputerów w sieci najczęściej zgłaszających przypadki wirusów. |

# Wykonywanie zadań obsługi raportów i dzienników

**Procedura**

1. Przejdź do pozycji **Raporty** > **Obsługa**.
2. Wykonaj następujące czynności:

| ZADANIE | CZYNNOŚCI |
|---|---|
| Ustawianie maksymalnej liczby raportów i szablonów | Istnieje możliwość ograniczenia liczby raportów jednorazowych, raportów zaplanowanych (na szablon) i szablonów dostępnych na serwerze Security Server. Po przekroczeniu tej liczby program Security Server usunie nadmiarowe raporty/szablony, zaczynając od przechowywanych przez najdłuższy czas.<br>a. Kliknij kartę **Raporty**.<br>b. Wpisz maksymalną liczbę zachowywanych raportów jednorazowych, raportów zaplanowanych i szablonów. |
| Konfigurowanie automatycznego usuwania dzienników | a. Kliknij kartę **Automatyczne usuwanie dzienników**.<br>b. Wybierz typy dzienników i określ ich maksymalny wiek. Dzienniki starsze niż określona wartość będą usuwane. |
| Ręczne usuwanie dzienników | a. Kliknij kartę **Ręczne usuwanie dzienników**.<br>b. W przypadku każdego typu dziennika wpisz maksymalny wiek. Dzienniki starsze niż określona wartość będą usuwane. Aby usunąć wszystkie dzienniki, wpisz `0`.<br>c. Kliknij przycisk **Usuń**. |

3. Kliknij przycisk **Zapisz**.

# Rozdział 13

# Wykonywanie zadań administracyjnych

W tym rozdziale opisano sposób wykonywania dodatkowych zadań administracyjnych, takich jak wyświetlanie licencji produktu, praca z Plug-in Manager i odinstalowywanie programu Security Server.

# Zmiana hasła konsoli internetowej

Firma Trend Micro zaleca użycie silnych haseł do konsoli internetowej. Silne hasło ma długość co najmniej ośmiu znaków i zawiera co najmniej jedną wielką literę (A–Z), co najmniej jedną małą literę (a–z), co najmniej jedną cyfrę (0–9), jak również co najmniej jeden znak specjalny lub przestankowy (!@#$%^&,.:;?). Silne hasła nigdy nie powinny być identyczne z nazwą logowania użytkownika, ani zawierać tej nazwy. Nie należy także używać imienia ani nazwiska użytkownika, daty urodzin ani żadnej innej informacji, którą można łatwo utożsamić z użytkownikiem.

---

**Procedura**

1. Przejdź do **Administracja** > **Hasło**.
2. Zmień odpowiednio następujące opcje:
   - **Stare hasło**
   - **Nowe hasło**
   - **Potwierdź hasło**: Wpisz ponownie nowe hasło, aby je potwierdzić.
3. Kliknij przycisk **Zapisz**.

---

# Praca z Plug-in Manager

Menedżer dodatków wyświetla programy przeznaczone dla programu Security Server i agentów w konsoli internetowej zaraz po tym, jak zostaną one udostępnione. Można je instalować i zarządzać nimi za pośrednictwem konsoli internetowej, łącznie z instalowaniem dodatków klienckich w agentach. Menedżer dodatków można pobrać i zainstalować z menu **Administracja** > **Dodatki**. Po zainstalowaniu Menedżera dodatków można sprawdzić dostępność dodatków. Więcej informacji zawiera dokumentacja Plug-in Manager i dodatków.

# Zarządzanie licencją produktu

Na ekranie Licencja produktu można odnowić, zaktualizować albo wyświetlić szczegóły dotyczące licencji produktu.

Na ekranie Licencja produktu wyświetlane są szczegółowe informacje odnośnie licencji. W zależności od opcji wybranych w czasie instalacji może to być wersja z pełną licencją lub wersja próbna. W obu przypadkach licencja upoważnia użytkownika do korzystania z umowy serwisowej. Gdy umowa serwisowa wygaśnie, ochrona komputerów klienckich w sieci stanie się bardzo ograniczona. Na ekranie Licencja produktu można sprawdzić datę wygaśnięcia licencji, tak aby odnowić ją przed upływem tego terminu.

**Uwaga**

Licencje składników produktów firmy Trend Micro mogą różnić się w zależności od regionu. Po zakończeniu instalacji zostanie wyświetlone podsumowanie z informacjami, z jakich składników można korzystać, używając danego klucza rejestracyjnego/kodu aktywacyjnego. Aby zweryfikować składniki, których licencje posiada użytkownik, należy skontaktować się ze sprzedawcą lub dostawcą.

## Odnowienie licencji

Aby odnowić lub uaktualnić posiadany produkt do wersji programu Worry-Free Business Security z pełną licencją, należy wykupić odnowienie usługi. Wersja z pełną licencją wymaga kodu aktywacyjnego.

Licencję produktu można odnowić na dwa sposoby:

- W konsoli internetowej przejdź do ekranu Stan aktywności i wykonuj instrukcje przedstawione na ekranie. Instrukcje te pojawiają się 60 dni przed wygaśnięciem licencji i są widoczne przez 30 dni po jej wygaśnięciu.
- Skontaktuj się z przedstawicielem handlowym lub dystrybutorem oprogramowania firmy Trend Micro w celu odnowienia umowy licencyjnej.

  Sprzedawcy mogą zostawić informacje kontaktowe w pliku w programie Security Server. Sprawdź plik w następującej lokalizacji:

  ```
  {folder instalacji programu Security Server}\PCCSRV\Private
  \contact_info.ini
  ```

**Uwaga**

`{folder instalacji programu Security Server}` to zwykle `C:\Program Files\Trend Micro\Security Server`.

Sprzedawca firmy Trend Micro zaktualizuje informacje rejestracyjne za pomocą funkcji rejestracji produktów firmy Trend Micro.

Program Security Server sprawdza serwer rejestracji produktu i pobiera nową datę wygaśnięcia bezpośrednio z tego serwera. Podczas odnawiania licencji nie jest konieczne ręczne wprowadzanie nowego kodu aktywacyjnego.

## Aktywacja nowej licencji

Od typu licencji zależy kod aktywacyjny programu Worry-Free Business Security.

**TABELA 13-1. Kody aktywacyjne według typu licencji**

| TYP LICENCJI | KOD AKTYWACYJNY |
|---|---|
| Pełna wersja programu Worry-Free Business Security Standard | CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx |
| Pełna wersja programu Worry-Free Business Security Advanced | CM-xxxx-xxxxx-xxxxx-xxxxx-xxxxx |

**Uwaga**

Aby uzyskać odpowiedzi na pytania dotyczące kodu aktywacyjnego, należy odwiedzić witrynę internetową firmy Trend Micro pod następującym adresem:

http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326

Na ekranie Licencja produktu można zmienić typ licencji przez wprowadzenie nowego kodu aktywacyjnego.

1. Przejdź do pozycji **Administracja** > **Licencja produktu**.
2. Kliknij przycisk **Wprowadź nowy kod**.
3. Wpisz nowy kod aktywacyjny w odpowiednim polu.

4. Kliknij przycisk **Aktywuj**.

# Konfigurowanie ustawień aktualizacji produktu

Skonfiguruj program Worry-Free Business Security, aby zautomatyzować aktualizacje produktów.

**Procedura**

1. Przejdź do menu **Administracja** > **Aktualizacja produktu**.

   Zostanie wyświetlona karta **Ustawienia**.

2. W obszarze **Ustawienia aktualizacji** zaznacz opcję **Włącz pobieranie aktualizacji produktu**.

3. Określ działanie do wykonania, gdy nowy pakiet aktualizacji stanie się dostępny.

   - **Pobierz**: Automatycznie pobiera pakiet aktualizacji do folderu pobierania na podstawie skonfigurowanego harmonogramu.
   - **Pobierz i zainstaluj**: Automatycznie pobiera i instaluje pakiet aktualizacji na podstawie skonfigurowanego harmonogramu.

4. Określ, kiedy podjąć działanie.

   **Uwaga**

   Proces instalacji i ponownego uruchomienia serwera Security Server może nieco potrwać. Wybierz czas, gdy instalacja pakietu aktualizacji spowoduje najmniej zakłóceń.

5. Kliknij przycisk **Zapisz**.

# Konfigurowanie powiadomień o aktualizacji produktu

Program Worry-Free Business Security może informować użytkowników o aktualizacjach produktu, gdy dostępna jest nowa wersja, dodatek Service Pack lub poprawka. Można skonfigurować następujące rodzaje powiadomień o aktualizacji produktu:

- Security Agent: Wyświetla powiadomienie w pobliżu obszaru powiadomień na punkcie końcowym.
- E-mail

---

**Procedura**

1. Przejdź do menu **Administracja** > **Aktualizacja produktu**.
2. Kliknij pozycję **Powiadomienia**.
3. Aby otrzymywać powiadomienia agenta Security Agent, skonfiguruj sekcję **Powiadomienie agenta Security Agent**.
   a. Kliknij przycisk **Dodaj**.
   b. Wybierz agenty Security Agent z listy.
   c. Kliknij przycisk **Zapisz**.
4. Aby otrzymywać powiadomienia e-mail o aktualizacjach produktu, określ odbiorców w sekcji **Powiadomienie e-mail**.

   **Uwaga**

   Odbieranie powiadomień e-mail wymaga skonfigurowania karty **SMTP** w **Administracja** > **Ustawienia globalne**.

5. Kliknij przycisk **Zapisz**.

---

# Uczestnictwo w programie Smart Feedback

Szczegółowe informacje dotyczące funkcji Smart Feedback zawiera temat *Smart Feedback na stronie 1-7*.

**Procedura**

1. Przejdź do menu **Administracja** > **Smart Protection Network**.
2. Kliknij opcję **Włącz program Trend Micro Smart Feedback**.
3. Aby wysyłać informacje o potencjalnych zagrożeniach bezpieczeństwa występujących w plikach na komputerach klienckich, zaznacz pole wyboru **Włącz informowanie o podejrzanych plikach programów**.

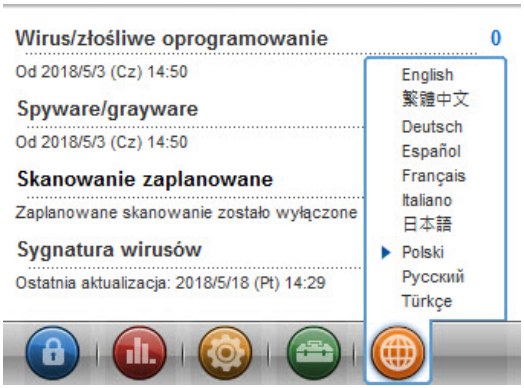
   **Uwaga**

   Pliki przesyłane za pomocą funkcji Smart Feedback nie zawierają danych użytkownika i są wysyłane wyłącznie na potrzeby analizy zagrożeń.

4. Aby poinformować firmę Trend Micro o charakterze prowadzonej działalności, wybierz wartość opcji **Branża**.
5. Kliknij przycisk **Zapisz**.

# Zmiana języka interfejsu agenta

Domyślnie język używany w interfejsie agenta będzie odpowiadał ustawieniom regionalnym skonfigurowanym w systemie operacyjnym klienta. Użytkownicy mogą zmienić język za pomocą interfejsu agenta.




# Zapisywanie i przywracanie ustawień programów

Istnieje możliwość zapisania kopii bazy danych programu Security Server i ważnych plików konfiguracyjnych w celu przywrócenia programu Security Server. Można to zrobić, jeśli występują problemy i konieczna jest ponowna instalacja programu Security Server lub w celu przywrócenia poprzedniej konfiguracji.

**Procedura**

1. Zatrzymaj usługę Trend Micro Security Server Master Service.
2. Ręcznie skopiuj następujące pliki i foldery z folderu w inne miejsce:

   **OSTRZEŻENIE!**

   Do tego zadania nie należy używać narzędzi ani aplikacji do tworzenia kopii zapasowych.

   `<Ścieżka instalacyjna programu Security Server>\PCCSRV`

   - Plik `ofcscan.ini`: zawiera ustawienia globalne.

- `Ous.ini`: zawiera tabelę źródeł aktualizacji dla instalacji składników antywirusowych.
- Folder `Private`: zawiera ustawienia zapory i źródła aktualizacji.
- Plik `Pccnt\Common\OfcPfw.dat`: zawiera ustawienia zapory.
- Plik `Download\OfcPfw.dat`: zawiera ustawienia instalacji zapory.
- Folder `Log`: zawiera zdarzenia systemowe i dziennik sprawdzania połączeń.
- Folder `Virus`: folder, w którym zarażone pliki poddawane są kwarantannie przez program WFBS.
- Folder `HTTDB`: zawiera bazę danych programu WFBS.

3. Dezinstalacja programu Security Server Patrz sekcja *Dezinstalacja programu Security Server na stronie 13-10*.
4. Przeprowadź nową instalację. Informacje na ten temat można znaleźć w *Podręczniku instalacji i uaktualniania* programu Worry-Free Business Security.
5. Kiedy główny program instalacyjny zakończy pracę, zatrzymaj usługę Trend Micro Security Server Master Service na komputerze docelowym.
6. Przeprowadź aktualizację wersji sygnatur wirusów z pliku kopii zapasowej:
   a. Pobierz bieżącą wersję sygnatur wirusów z nowego serwera.

      ```
      <Ścieżka instalacyjna programu Security Server>\PCCSRV
      \Private\component.ini. [6101]

      ComponentName=sygnatura wirusa

      Version=xxxxxx 0 0
      ```

   b. Przeprowadź aktualizację wersji sygnatur wirusów w pliku kopii zapasowej:

      ```
      \Private\component.ini
      ```

> **Uwaga**
>
> W przypadku zmiany ścieżki instalacji programu Security Server zaktualizuj informacje o ścieżce w plikach kopii zapasowej `ofcscan.ini` i `\private\ofcserver.ini`.

7. Używając utworzonych wcześniej kopii zapasowych, zastąp bazę danych programu Worry-Free Business Security oraz odpowiednie pliki i foldery na komputerze docelowym w folderze `PCCSRV`.

8. Uruchom ponownie usługę Trend Micro Security Server Master Service.

---

# Dezinstalacja programu Security Server

Odinstalowanie programu Security Server spowoduje również odinstalowanie serwera skanowania.

Program Worry-Free Business Security korzysta z programu dezinstalacyjnego, aby bezpiecznie usunąć program Trend Micro Security Server z komputera. Przed usunięciem programu Security Server należy usunąć agenta ze wszystkich klientów.

Odinstalowanie programu Trend Micro Security Server nie powoduje dezinstalacji agentów. Przed odinstalowaniem programu Trend Micro Security Server administratorzy muszą odinstalować lub przenieść wszystkie agenty na inny serwer Security Server. Patrz sekcja *Usuwanie agentów na stronie 3-41*.

---

**Procedura**

1. Na komputerze, na którym przeprowadzono instalację programu, kliknij kolejno pozycje **Start** > **Panel sterowania** > **Dodaj lub usuń programy**.

2. Kliknij pozycję **Trend Micro Security Server**, a następnie kliknij opcję **Zmień/usuń**.

   Zostanie wyświetlony ekran potwierdzenia.

3. Kliknij przycisk **Dalej**.

   Dezinstalator serwera poprosi o podanie hasła administratora.

4. W polu tekstowym wpisz hasło administratora i kliknij przycisk **OK**.

   Program odinstalowujący rozpocznie usuwanie plików serwera. Po odinstalowaniu programu Security Server zostanie wyświetlony komunikat potwierdzenia.

5. Kliknij przycisk **OK**, aby zamknąć program odinstalowujący.

# Rozdział 14

# Korzystanie z narzędzi do zarządzania

W tym rozdziale omówiono sposób korzystania z narzędzi i dodatków administracyjnych oraz klienckich.

# Typy narzędzi

Program Worry-Free Business Security zawiera zestaw narzędzi, pozwalających łatwo wykonywać różne zadania, takie jak konfiguracja serwera i zarządzanie klientami.

**Uwaga**

Narzędzi administracyjnych i klienckich nie można uruchamiać z poziomu konsoli internetowej. Z konsoli internetowej można pobierać dodatki.

Aby uzyskać instrukcje na temat uruchamiania narzędzi, należy zapoznać się z poniższymi sekcjami.

Narzędzia te dzielą się na trzy kategorie:

- **Narzędzia administracyjne**
  - **Ustawienia skryptu logowania** (`SetupUsr.exe`): automatyzuje instalację programu Security Agent. Patrz sekcja *Instalowanie za pomocą skryptu logowania na stronie 3-13*.
  - **Narzędzie Vulnerability Scanner** (`TMVS.exe`): wyszukuje niezabezpieczone komputery w sieci. Patrz sekcja *Instalowanie za pomocą narzędzia Vulnerability Scanner na stronie 3-22*.
  - **Program Remote Manager Agent**: umożliwia zarządzanie programem Worry-Free Business Security przez scentralizowaną konsolę internetową. Patrz sekcja *Instalowanie programu Trend Micro Remote Manager Agent (użytkownicy portalu licencjonowania klientów) na stronie 14-4*.
  - **Narzędzie Trend Micro Disk Cleaner**: usuwa niepotrzebne pliki kopii zapasowych, pliki dzienników i nieużywane pliki sygnatur programu Worry-Free Business Security. Patrz sekcja *Oszczędzanie miejsca na dysku na stronie 14-15*.
  - **Narzędzie do przenoszenia bazy danych serwera skanowania**: Służy do bezpiecznego przenoszenia bazy danych serwera skanowania na inny dysk. Patrz sekcja *Przenoszenie bazy danych serwera skanowania na stronie 14-18*.
- **Narzędzia klienckie**

- **Program Client Packager** (`ClnPack.exe`): umożliwia tworzenie samorozpakowujących się plików zawierających program Security Agent i składniki. Patrz sekcja *Instalowanie za pomocą narzędzia Client Packager na stronie 3-15*.
- **Przywracanie zaszyfrowanych wirusów i oprogramowania spyware** (`VSEncode.exe`): umożliwia otwarcie zainfekowanych plików przy użyciu programu Worry-Free Business Security. Patrz sekcja *Przywracanie zaszyfrowanych plików na stronie 14-18*.
- **Narzędzie Client Mover** (`IpXfer.exe`): przenosi agentów między serwerami Security Server. Patrz sekcja *Przenoszenie agentów na stronie 4-11*.
- **Ponowne generowanie identyfikatora klienta programu Security Agent** (`WFBS_WIN_All_ReGenID.exe`): narzędzie ReGenID służy do ponownego generowania identyfikatora klienta programu Security Agent na podstawie tego, czy agent znajduje się na sklonowanym komputerze czy na maszynie wirtualnej. Patrz sekcja *Korzystanie z narzędzia ReGenID na stronie 14-23*.
- **Narzędzie dezinstalacji programu Security Agent** (`SA_Uninstall.exe`): automatycznie usuwa wszystkie składniki programu Security Agent z komputera klienckiego. Patrz sekcja *Używanie narzędzia SA Uninstall na stronie 3-44*.

- **Dodatki**: Pozwalają administratorom wyświetlać bieżące informacje o zabezpieczeniach i systemie z poziomu konsol obsługiwanych systemów operacyjnych Windows. Te same szczegółowe informacje są wyświetlane na ekranie Stan aktywności. Patrz sekcja *Zarządzanie dodatkami SBS i EBS na stronie 14-24*.

**Uwaga**

Niektóre narzędzia dostępne w poprzednich wersjach programu Worry-Free Business Security nie są dostępne w tej wersji. Jeżeli są one potrzebne, należy się skontaktować z pomocą techniczną firmy Trend Micro.

# Trend Micro Remote Manager Agent

Korzystając z programu Trend Micro Remote Manager Agent, sprzedawcy lub partnerzy mogą zarządzać produktem Worry-Free Business Security za pomocą programu Trend

Micro Remote Manager. Po zakończeniu instalacji programu serwera zabezpieczeń Security Server program Remote Manager Agent można od razu zainstalować na tym serwerze lub zrobić to w późniejszym czasie.

Wymagania dotyczące instalacji:

- unikatowy identyfikator globalny (GUID) programu Remote Manager Agent,
- aktywne połączenie internetowe,
- 50 MB wolnego miejsca na dysku.

Postępuj zgodnie z procedurami jednej z następujących opcji:

- *Instalowanie programu Trend Micro Remote Manager Agent (użytkownicy portalu licencjonowania klientów) na stronie 14-4*
- *Instalowanie programu Trend Micro Remote Manager Agent (użytkownicy platformy Licensing Management Platform) na stronie 14-6*

## Instalowanie programu Trend Micro Remote Manager Agent (użytkownicy portalu licencjonowania klientów)

**Procedura**

1. Uzyskaj identyfikator GUID programu Remote Manager Agent.
   a. Na konsoli sieci Web programu Remote Manager przejdź do pozycji **Klienci**.
   b. Kliknij żądanego klienta z kolumny **Firma**.
   c. Wybierz produkt Worry-Free Business Security z karty **Produkty**.
   d. Skopiuj identyfikator GUID.
2. Na serwerze Security Server przejdź do następującego folderu instalacyjnego:`PCCSRV\Admin\Utility\RmAgent` i uruchom aplikację `TMRMAgentforWFBS.exe`.

   Na przykład:`C:\Program Files\Trend Micro\Security Server \PCCSRV\Admin\Utility\RmAgent\TMRMAgentforWFBS.exe`

**Uwaga**

Pomiń ten krok, jeśli uruchamiasz instalację z ekranu instalacji programu Security Server.

3. W kreatorze instalacji programu Trend Micro Remote Manager Agent przeczytaj umowę licencyjną. Jeśli zgadzasz się z jej warunkami, wybierz pozycję **Akceptuję warunki umowy licencyjnej** i kliknij przycisk **Dalej**.

4. Kliknij przycisk **Tak**, aby potwierdzić status certyfikowanego partnera.

5. Wybierz opcję **Mam już konto Trend Micro Remote Manager i chcę zainstalować agenta**, a następnie kliknij przycisk **Dalej**.

6. Wybierz scenariusz.

| SCENARIUSZ | CZYNNOŚCI |
|---|---|
| Nowy klient | a. Wybierz opcję **Powiąż z nowym klientem**.<br>b. Kliknij przycisk **Dalej**. Wprowadź informacje o kliencie.<br>**Uwaga**<br>Jeśli klient już istnieje w konsoli programu TMRM, po wybraniu opcji Powiąż z nowym klientem w drzewie sieci programu TMRM pojawi się dwóch klientów o identycznych nazwach. Aby tego uniknąć, należy wykonać poniższe czynności. |
| Istniejący klient | a. Wybierz opcję **Ten produkt istnieje już na koncie Remote Manager**.<br>**Uwaga**<br>Program WFBS musi być wcześniej dodany do konsoli programu TMRM. Instrukcje znajdują się w dokumentacji programu TMRM.<br>b. Wpisz identyfikator GUID. |

7. Kliknij przycisk **Dalej**.

8. Wybierz **region** i **protokół**, a następnie wprowadź informacje dotyczące serwera proxy, jeżeli jest to wymagane.

9. Kliknij przycisk **Dalej**.

   Zostanie otwarty ekran Installation Location (Lokalizacja instalacji).

10. Aby użyć lokalizacji domyślnej, kliknij przycisk **Dalej**.

11. Kliknij przycisk **Zakończ**.

    Jeżeli instalacja zakończy się powodzeniem i ustawienia będą prawidłowe, program Remote Manager Agent powinien automatycznie zarejestrować się na serwerze Trend Micro Remote Manager. Program Remote Manager Agent powinien wyświetlać się ze stanem Online na konsoli sieci Web programu Remote Manager.

## Instalowanie programu Trend Micro Remote Manager Agent (użytkownicy platformy Licensing Management Platform)

**Procedura**

1. Uzyskaj kod aktywacyjny programu Worry-Free Business Security.

   a. Na konsoli sieci Web programu Remote Manager przejdź do pozycji **Klienci**.

   b. Kliknij żądanego klienta z kolumny **Firma**.

   c. Wybierz produkt Worry-Free Business Security z karty **Produkty**.

   d. Skopiuj kod aktywacyjny.

2. Zaktualizuj informacje dotyczące licencji produktu Worry-Free Business Security.

   a. Na konsoli sieci Web programu Worry-Free Business Security przejdź do pozycji **Administracja** > **Licencja produktu**.

   b. Pod nagłówkiem **Informacje o licencji** kliknij przycisk **Wprowadź nowy kod**.

   c. Wklej kod aktywacyjny w polu **Nowy kod aktywacyjny**.

   d. Kliknij przycisk **Aktywuj**.

e. Kliknij polecenie **Odśwież informacje o licencji**.

3. Na serwerze Security Server przejdź do następującego folderu instalacyjnego:`PCCSRV\Admin\Utility\RmAgent` i uruchom aplikację `TMRMAgentforWFBS.exe`.

   Na przykład:`C:\Program Files\Trend Micro\Security Server \PCCSRV\Admin\Utility\RmAgent\TMRMAgentforWFBS.exe`

   **Uwaga**

   Pomiń ten krok, jeśli uruchamiasz instalację z ekranu instalacji programu Security Server.

4. Wybierz opcję **Mam już konto Trend Micro Remote Manager i chcę zainstalować agenta**, a następnie kliknij przycisk **Dalej**.

5. Wybierz opcję **Powiąż z istniejącą licencją platformy Licensing Management Platform** i kliknij przycisk **Dalej**.

6. Wprowadź poświadczenia konta Remote Manager i kliknij przycisk **Dalej**.

7. W razie potrzeby wprowadź informacje dotyczące serwera proxy i kliknij przycisk **Dalej**.

8. W razie potrzeby wskaż folder instalacji i kliknij przycisk **Dalej**.

9. Kliknij przycisk **Zakończ**.

   Jeżeli instalacja zakończy się powodzeniem i ustawienia będą prawidłowe, program Remote Manager Agent powinien automatycznie zarejestrować się na serwerze Trend Micro Remote Manager. Program Remote Manager Agent powinien wyświetlać się ze stanem Online na konsoli sieci Web programu Remote Manager.

## Zarządzanie agentami serwera zarządzanego

Część ta zawiera informacje dotyczące zarządzania agentami serwera zarządzanego.

## Komunikaty o stanie agenta

Na pasku zadań serwera, którym zarządza agent, wyświetla się jedna z następujących ikon:

**TABELA 14-1. Ikony paska zadań**

| IKONA | OPIS |
|---|---|
| | Zielona ikona oznacza, że agent jest połączony z serwerem komunikacji programu Remote Manager. Agent działa prawidłowo. |
| | Czerwona ikona oznacza, że agent nie jest połączony z serwerem komunikacji programu Remote Manager lub że jego wersja nie jest zgodna z wersją wymaganą przez serwer i wymaga aktualizacji. |
| | Ikona z czerwoną strzałką oznacza, że agent wylogował się z programu Remote Manager |
| | Ikona z czerwonym „X” oznacza, że agent został wyłączony. |

## Zmiana identyfikatora GUID agenta na zarządzanym przez niego serwerze

Jeśli podczas instalacji agenta programu Remote Manager podano nieprawidłowy identyfikator GUID, usuń agenta i zainstaluj ponownie z użyciem właściwego identyfikatora GUID. Jeżeli zastosowanie tej metody nie jest możliwe, wykonaj następujące czynności:

**Procedura**

1. Przejdź do folderu `C:\Program Files\Trend Micro\TMRMAgentForWFBS`.
2. Za pomocą edytora tekstu otwórz plik `AgentSysConfig.xml`.
3. Poszukaj identyfikatora GUID między parametrami `<AgentGUID>` i `</AgentGUID>`.
4. Popraw wartość identyfikatora GUID i zapisz plik.
5. W tym samym folderze za pomocą edytora tekstu otwórz plik `csmSysConfig.xml`.

6. Poszukaj identyfikatora GUID między parametrami `<ProductGUID>` i `</ProductGUID>`.

7. Popraw wartość identyfikatora GUID i zapisz plik.

8. Kliknij prawym przyciskiem myszy ikonę agenta programu Remote Manager na pasku zadań i kliknij **Uruchom ponownie usługę**.

---

## Korzystanie z narzędzia do konfiguracji agenta

Narzędzie do konfiguracji agenta (Agent Configuration Tool) umożliwia zmianę ustawień konfiguracji programu Remote Manager Agent.

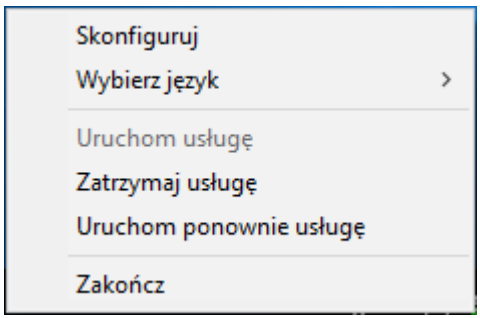
Wybierz kolejno **Start** > **Programy** > **Trend Micro Remote Manager Agent** > **Agent Configuration Tool** lub kliknij prawym przyciskiem myszy ikonę na pasku zadań, a następnie polecenie **Konfiguruj**.

Więcej informacji zawiera część *Konfiguracja agenta na stronie 14-9*.

## Konfiguracja agenta

### Menu konfiguracji agenta

W celu skonfigurowania agenta kliknij prawym przyciskiem myszy ikonę w pasku zadań, by wywołać poniższe menu:



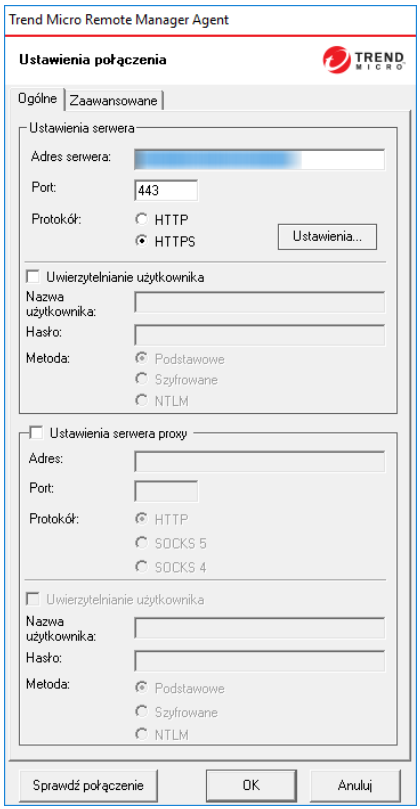

**ILUSTRACJA 14-1. Podręczne menu narzędzia do konfiguracji agenta**

Pojawią się poniższe elementy:

- **Konfiguruj**: otwiera ekran konfiguracji agenta.
- **Wybierz język**: oprócz innych języków do dyspozycji zawsze jest „English” (angielski).
- **Usługa**: Uruchom, Zatrzymaj, Uruchom ponownie
- **Zakończ**: zamknięcie narzędzia nie zatrzymuje usługi programu Remote Manager. Zamyka jedynie Narzędzie do konfiguracji i usuwa jego ikonę z paska zadań. Narzędzie można ponownie uruchomić w dowolnej chwili.

### Główne okno dialogowe Narzędzia do konfiguracji

Kliknij prawym przyciskiem myszy ikonę na pasku zadań i kliknij **Konfiguruj** w menu konfiguracji agenta, aby otworzyć kartę **Ogólne** narzędzia do konfiguracji agenta.




**ILUSTRACJA 14-2. Karta „Ogólne” Narzędzia do konfiguracji agenta**

Poniższe sekcje ekranu konfiguracji agenta są w tej chwili jedynymi dostępnymi funkcjami narzędzia.

- **Ustawienia serwera**: skonfiguruj komunikację z serwerem, ustawiając następujące parametry:

- **Adres serwera**: w pełni kwalifikowana nazwa domeny (FQDN) serwera komunikacji programu Remote Manager. Nazwa FQDN zależy od regionu. Skontaktuj się z przedstawicielem działu wsparcia, jeżeli musisz zmienić informacje o adresie serwera.
- **Port**: port używany przez serwer programu Remote Manager do komunikacji z agentem. Powinien mieć wartość 80 w przypadku protokołu HTTP i 443 dla HTTPS.
- **Protokół**: protokół używany w komunikacji między serwerem i agentem.

**Ważne**

Firma Trend Micro nie zaleca zmiany informacji **Adresu serwera** ani **Portu**, o ile dział wsparcia nie nakazał dokonania tych modyfikacji.

- **Ustawienia serwera proxy**: uaktywnij ten obszar, klikając pole wyboru **Ustawienia serwera proxy**, jeżeli sieć użytkownika wymaga serwera proxy do komunikacji z serwerem programu Remote Manager.
  - **Adres**: adres IP serwera proxy
  - **Port**: port serwera proxy
  - **Protokół**
- **Przycisk Sprawdź połączenie**: Przycisk **Sprawdź połączenie** jest używany do sprawdzenia komunikacji między agentem i serwerem programu Remote Manager. Użyj tej funkcji do sprawdzenia, czy podstawowe połączenie z serwerem komunikacji działa poprawnie. Jeżeli nie zostanie nawiązane (pojawi się okno komunikatu o braku połączenia z serwerem), może to wynikać z prozaicznej przyczyny w rodzaju nieprawidłowego adresu serwera komunikacji i jego portu bądź adresu serwera proxy i jego portu.

## Tworzenie i przywracanie kopii zapasowej ustawień agenta

Jeśli musisz odinstalować agenta i ponownie go zainstalować z użyciem tego samego identyfikatora GUID w ciągu trzech dni, zachowaj ustawienia agenta, aby uniknąć

nałożenia się danych. W tym celu ręcznie wykonaj kopię zapasową plików konfiguracji, a następnie, po zainstalowaniu agenta, zastąp pliki konfiguracji plikami kopii zapasowej.

## Tworzenie kopii zapasowej ustawień

**Procedura**

1. Na serwerze zarządzanym przez agenta kliknij prawym przyciskiem myszy ikonę agenta na pasku zadań i kliknij przycisk **Zatrzymaj usługę** w celu zatrzymania usługi agenta.
2. Skopiuj wszystkie pliki `.xml`, `.dat` oraz `.ini` z foldera instalacyjnego: `C:\Program Files\Trend Micro\TMRMAgentForWFBS` lub `C:\Program Files (x86)\Trend Micro\TMRMAgentForWFBS`.
   - Pliki `.xml`
     - `csmSysConfig.xml`
     - `csmLocalConfig.xml`
     - `csmLogDef.xml`
     - `AgentWorkConfig.xml`
     - `AgentSysConfig.xml`
     - `AgentStatus.xml`
     - `AgentLocalConfig.xml`
   - Pliki `.dat`
     - `MSA.dat`
     - `logBuf.dat`
     - `group.dat`
     - `CSA.dat`
     - `CriticalVA.dat`

- Pliki `.ini`
  - `csmStatusData.ini`

3. Skopiuj wszystkie pliki z foldera `\Cache`.
4. Uruchom ponownie usługę agenta.

## Przywracanie ustawień

**Procedura**

1. Usuń agenta z dysku lokalnego.

**Uwaga**

Przy usuwaniu agenta z dysku lokalnego jest on wyrejestrowywany z programu Remote Manager, co powoduje automatyczne usunięcie wszystkich danych powiązanych z agentem. Aby zapobiec wyrejestrowaniu agenta, przed jego usunięciem należy zmienić wartość ustawienia Adres serwera w interfejsie agenta.

2. Ponownie zainstaluj agenta. Upewnij się, że stosowany jest ten sam identyfikator GUID, co w pliku `agentSysConfig.xml`.
3. Na serwerze zarządzanym przez agenta kliknij prawym przyciskiem myszy ikonę agenta na pasku zadań i kliknij przycisk **Zatrzymaj usługę** w celu zatrzymania usługi agenta.
4. Zastąp pliki konfiguracji plikami kopii zapasowej.
5. Kliknij prawym przyciskiem myszy ikonę agenta na pasku zadań, a następnie kliknij przycisk **Uruchom usługę** w celu ponownego uruchomienia usługi agenta.

# Oszczędzanie miejsca na dysku

Narzędzie Disk Cleaner pozwala oszczędzać miejsce na dysku na serwerze Security Server i klientach.

## Uruchamianie programu Disk Cleaner na serwerze Security Server

### Przed rozpoczęciem

W celu zwiększenia ilości wolnego miejsca na dysku narzędzie czyszczenia dysków (`TMDiskCleaner.exe`) wykrywa i usuwa nieużywane pliki kopii zapasowych, dzienników i sygnatur z następujących katalogów:

- `{Security Agent}\AU_Data\AU_Temp\*`
- `{Security Agent}\Reserve`
- `{Security Server}\PCCSRV\TEMP\*` (z wyjątkiem plików ukrytych)
- `{Security Server}\PCCSRV\Web\Service\AU_Data\AU_Temp\*`
- `{Security Server}\PCCSRV\wss\*.log`
- `{Security Server}\PCCSRV\wss\AU_Data\AU_Temp\*`
- `{Security Server}\PCCSRV\Backup\*`
- `{Security Server}\PCCSRV\Virus\*` (usuwa pliki poddane kwarantannie od ponad dwóch tygodni — z wyjątkiem pliku NOTVIRUS)
- `{Security Server}\PCCSRV\ssaptpn.xxx` (z wyjątkiem tylko najnowszego pliku sygnatur)
- `{Security Server}\PCCSRV\lpt$vpn.xxx` (z wyjątkiem tylko trzech najnowszych plików sygnatur)
- `{Security Server}\PCCSRV\icrc$oth.xxx` (z wyjątkiem tylko trzech najnowszych plików sygnatur)

- `{Security Server}\DBBackup\* (z wyjątkiem tylko dwóch najnowszych podfolderów)`
- `{Messaging Security Agent}\AU_Data\AU_Temp\*`
- `{Messaging Security Agent}\Debug\*`
- `{Messaging Security Agent}\engine\vsapi\latest\pattern\*`

**Procedura**

1. Na Security Server przejdź do następującego katalogu:

   `{folder instalacji serwera}\PCCSRV\Admin\Utility\`

2. Kliknij dwukrotnie plik **TMDiskCleaner.exe**.

   Zostanie otwarte okno narzędzia czyszczenia dysku Trend Micro Worry-Free Business Security Disk Cleaner.

   **Uwaga**

   Plików nie można odzyskać.

3. Kliknij polecenie **Usuń pliki**, aby wyszukać i usunąć nieużywane pliki kopii zapasowych, dzienników i sygnatur.

## Uruchamianie programu Disk Cleaner na serwerze Security Server za pomocą interfejsu wiersza polecenia

**Procedura**

1. Na Security Server otwórz okno wiersza polecenia.
2. W wierszu polecenia wpisz następujące polecenie:

   `TMDiskCleaner.exe [/hide] [/log] [/allowundo]`

   - `/hide`: Powoduje uruchomienie narzędzia w tle.

- `/log`: Włącza rejestrowanie operacji w pliku dziennika DiskClean.log znajdującym się w bieżącym folderze.

**Uwaga**

Opcja `/log` jest dostępna tylko w połączeniu z opcją `/hide`.

- `/allowundo`: Pliki są przenoszone do Kosza systemu Windows, a nie usuwane nieodwracalnie.

3. Jeśli zachodzi potrzeba częstego uruchamiania narzędzia czyszczenia dysków, można skonfigurować nowe zadanie, korzystając z funkcji Harmonogram zadań systemu Windows. Więcej informacji zawiera dokumentacja systemu Windows.

## Oszczędzanie miejsca na dysku klientów

**Procedura**

- Na komputerach/serwerach z programami Security Agent:
  - Wyczyść pliki kwarantanny
  - Wyczyść pliki dziennika
  - Uruchom narzędzie Oczyszczanie dysku systemu Windows
- Na serwerach Microsoft Exchange z programami Messaging Security Agent:
  - Wyczyść pliki kwarantanny
  - Wyczyść pliki dziennika
  - Uruchom narzędzie Oczyszczanie dysku systemu Windows
  - Wyczyść dzienniki archiwum
  - Wyczyść pliki kopii zapasowych
  - Sprawdź rozmiar bazy danych Microsoft Exchange lub dzienników transakcji

# Przenoszenie bazy danych serwera skanowania

Jeśli na dysku, na którym zainstalowany jest serwer skanowania, znajduje się niewystarczająca ilość miejsca, należy skorzystać z narzędzia do przenoszenia bazy danych serwera skanowania, aby bezpiecznie przenieść bazę danych serwera skanowania na inny dysk.

Należy upewnić się, że serwer Security Server jest wyposażony w więcej niż jeden dysk oraz że na nowym dysku znajduje się co najmniej 3 GB wolnego miejsca. Dyski mapowane nie są akceptowane. Nie należy przenosić bazy danych ręcznie ani korzystać z innych narzędzi.

**Procedura**

1. Na komputerze z programem Security Server przejdź do `<folderu instalacji programu Security Server>\PCCSRV\Admin\Utility`.
2. Uruchom plik `ScanServerDBMover.exe`.
3. Kliknij przycisk **Zmień**.
4. Kliknij przycisk **Przeglądaj**, a następnie przejdź do folderu docelowego na drugim dysku.
5. Kliknij przycisk **OK**, a po przeniesieniu bazy danych kliknij przycisk **Zakończ**.

# Przywracanie zaszyfrowanych plików

W celu zapobiegania otwieraniu zarażonych plików program Worry-Free Business Security szyfruje je w następujących przypadkach:

- przed poddaniem pliku kwarantannie,
- podczas tworzenia kopii zapasowej pliku przed jego wyczyszczeniem.

Program Worry-Free Business Security zapewnia narzędzie, które odszyfrowuje, a następnie przywraca plik, gdy jest wymagany dostęp do zapisanych w nim informacji.

Program Worry-Free Business Security można wykorzystywać do szyfrowania i przywracania następujących plików:

**TABELA 14-2. Pliki, które program Worry-Free Business Security może odszyfrowywać i przywracać**

| PLIK | OPIS |
|---|---|
| Pliki poddane kwarantannie na kliencie | Pliki te znajdują się w następujących katalogach:<br>• `<folder instalacji programu Security Agent>\SUSPECT\Backup`<br>lub `<folder instalacji programu Security Agent>\quarantine`, w zależności od tego, która lokalizacja jest dostępna.<br>• `<folder instalacji programu Messaging Security Agent>\storage\quarantine`<br>Te pliki są przesyłane do wyznaczonego katalogu kwarantanny, którym jest zwykle katalog na serwerze Security Server. |
| Pliki poddane kwarantannie w wyznaczonym katalogu kwarantanny | Ten katalog znajduje się zwykle na komputerze serwera Security Server (`<folder instalacji programu >\PCCSRV\Virus`). Aby zmienić katalog, przejdź do karty **Administracja** > **Ustawienia globalne** > **System**, a następnie do sekcji Obsługa kwarantanny. |
| Kopie zapasowe zaszyfrowanych plików | Są to kopie zapasowe zarażonych plików, które agenty były w stanie wyczyścić. Pliki te znajdują się w następujących folderach:<br>• `<folder instalacji programu Security Agent>\Backup`.<br>• `<folder instalacji programu Messaging Security Agent>\storage\backup`<br>By przywrócić te pliki, użytkownicy muszą przenieść je do katalogu kwarantanny na kliencie. |

**OSTRZEŻENIE!**

Przywracanie zarażonego pliku może spowodować rozprzestrzenienie wirusa/złośliwego oprogramowania na inne pliki i klienty. Przed przywróceniem pliku należy odizolować zarażonego klienta i przenieść ważne pliki z tego komputera do lokalizacji zapasowej.

## Odszyfrowywanie i przywracanie plików w programie Security Agent

**Procedura**

1. Otwórz wiersz poleceń i przejdź do lokalizacji `<folder instalacji programu Security Agent>`.
2. Uruchom plik `VSEncode.exe`, wpisując:

   ```
   VSEncode.exe /u
   ```

   Zastosowanie tego parametru powoduje wyświetlenie ekranu z listą plików przechowywanych w lokalizacji `<folder instalacji programu Security Agent>\SUSPECT\Backup`.

   Administratorzy mogą przywrócić pliki zaliczone do oprogramowania spyware/grayware na karcie Spyware/Grayware. Na ekranie wyświetlana jest lista plików znalezionych w folderze: `<folder instalacji programu Security Agent>\BackupAS`.
3. Zaznacz plik przeznaczony do przywrócenia i kliknij polecenie **Przywróć**.

   **Uwaga**

   Narzędzie może jednocześnie przywrócić tylko jeden plik.
4. Na wyświetlonym ekranie określ folder, do którego ma zostać przywrócony plik.
5. Kliknij przycisk **OK**.

**Uwaga**

Może się zdarzyć, że agent ponownie przeskanuje plik i uzna go za zarażony natychmiast po jego przywróceniu. Aby uniemożliwić skanowanie pliku, należy go dodać do listy wykluczeń ze skanowania.

Patrz sekcja *Cele skanowania i operacje dotyczące programów Security Agent na stronie 7-11*.

Plik zostanie przywrócony do wskazanego folderu.

6. Kliknij **Zamknij**.

## Odszyfrowywanie i przywracanie plików na serwerze Security Server, w niestandardowym katalogu kwarantanny lub programie Messaging Security Agent

**Procedura**

1. Jeśli plik znajduje się na komputerze serwera Security Server, otwórz wiersz polecenia i przejdź do lokalizacji `<folder instalacji serwera>\PCCSRV\Admin\Utility\VSEncrypt`.

   Jeśli plik znajduje się na kliencie programu Messaging Security Agent lub w niestandardowym katalogu kwarantanny, przejdź do lokalizacji `<folder instalacji serwera>\PCCSRV\Admin\Utility` i skopiuj folder `VSEncrypt` na klient lub do niestandardowego katalogu kwarantanny.

2. 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 po kwarantannie znajdują się na komputerze serwera Security Server w lokalizacji `<folder instalacji serwera>\PCCSRV\Virus`.

3. Zapisz plik tekstowy z rozszerzeniem `INI` lub `TXT`. Plik można na przykład zapisać na dysku `C:` pod nazwą `DoZaszyfrowania.ini` C:.

4. Otwórz wiersz polecenia i przejdź do katalogu, w którym znajduje się folder `VSEncrypt`.

5. Uruchom plik `VSEncode.exe`, wpisując:

   ```
   VSEncode.exe /d /i <lokalizacja pliku INI lub TXT>
   ```

   Gdzie:

   `<lokalizacja pliku INI lub TXT>` to ścieżka dostępu do utworzonego pliku `INI` lub `TXT` (np. `C:\ForEncryption.ini`).

6. Użyj innych parametrów do wydawania różnych poleceń.

**TABELA 14-3. Parametry przywracania**

| PARAMETR | OPIS |
|---|---|
| Brak (brak parametru) | Szyfruj pliki |
| `/d` | Odszyfruj pliki |
| `/debug` | Utwórz dziennik diagnostyczny i zapisz go na komputerze. Na kliencie dziennik diagnostyczny `VSEncrypt.log` jest tworzony w lokalizacji `<folder instalacji agenta>`. |
| `/o` | Zastąp zaszyfrowany lub odszyfrowany plik, jeżeli już istnieje |
| `/f <nazwa pliku>` | zaszyfrowanie lub odszyfrowanie pojedynczego pliku |
| `/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 Worry-Free Business Security tworzy zaszyfrowany lub odszyfrowany plik w tym samym katalogu. Przed szyfrowaniem i odszyfrowaniem pliku należy się upewnić, że nie jest on zablokowany.

## Przywracanie wiadomości e-mail w formacie Transport Neutral Encapsulation Format

Format enkapsulacji TNEF jest używany w programach Microsoft Exchange/Outlook. Zazwyczaj jest on dodawany jako załącznik wiadomości e-mail o nazwie `Winmail.dat`, który jest automatycznie ukrywany w programie Outlook Express. Patrz http://support.microsoft.com/kb/241538/en-us.

Jeśli program Messaging Security Agent archiwizuje ten typ wiadomości, a rozszerzenie pliku jest zmieniane na .EML, to w programie Outlook Express jest wyświetlana tylko treść wiadomości.

# Korzystanie z narzędzia ReGenID

Przy każdej instalacji programu Security Agent jest potrzebny unikatowy identyfikator globalny (GUID, Globally Unique Identifier) umożliwiający programowi Security Server identyfikowanie poszczególnych agentów. Zduplikowane identyfikatory GUID występują zwykle w klientach sklonowanych lub maszynach wirtualnych.

Jeśli co najmniej dwa agenty zgłoszą ten sam identyfikator GUID, uruchom narzędzie ReGenID, aby wygenerować unikatowy identyfikator GUID dla każdego klienta.

**Procedura**

1. Na Security Server przejdź do następującego katalogu: `<folder instalacji serwera>\PCCSRV\Admin\Utility`.
2. Skopiuj plik `WFBS_WIN_All_ReGenID.exe` do folderu tymczasowego na komputerze z zainstalowanym programem Security Agent.

   Przykład: `C:\temp`

3. Kliknij dwukrotnie `WFBS_WIN_All_ReGenID.exe` i wykonaj instrukcje wyświetlane na ekranie.

   Narzędzie zatrzyma program Security Agent i usunie identyfikator GUID klienta.

4. Uruchom ponownie program Security Agent.

   Program Security Agent wygeneruje nowy identyfikator GUID klienta.

# Zarządzanie dodatkami SBS i EBS

Program Worry-Free Business Security udostępnia dodatki umożliwiające administratorom wyświetlanie bieżących informacji o zabezpieczeniach i agencie z konsol następujących systemów operacyjnych Windows:

- Windows Small Business Server (SBS) 2008
- Windows Essential Business (EBS) Server 2008
- Windows SBS 2011 Standard/Essentials
- Windows Server 2012 Essentials
- Windows Server 2012 R2 Essentials

## Ręczne instalowanie dodatków SBS i EBS

Dodatek SBS lub EBS instaluje się automatycznie po zainstalowaniu programu Security Server na punkcie końcowym z obsługiwanym systemem operacyjnym. Aby użyć dodatku na innym punkcie końcowym z obsługiwanym systemem operacyjnym, należy zainstalować go ręcznie.

**Procedura**

1. Zaloguj się do konsoli internetowej programu Security Server.
2. Przejdź do menu **Administracja** > **Narzędzia do zarządzania**.

3. Kliknij pozycję **Dodatki**.
4. Kliknij odpowiednie łącze **Pobierz**, aby pobrać program instalacyjny.
5. Skopiuj program instalacyjny na punkt końcowy i uruchom go.

## Korzystanie z dodatków SBS i EBS

**Procedura**

1. Otwórz konsolę SBS lub EBS.
2. Na karcie **Zabezpieczenia**, kliknij program **Trend Micro Worry-Free Business Security**, aby wyświetlić informacje o stanie programu.

# Dodatek A

## Ikony programu Security Agent

W tym dodatku objaśniono znaczenie różnych ikon programu Security Agent, wyświetlanych na klientach.

# Sprawdzanie stanu programu Security Agent

Na poniższej ilustracji przedstawiono konsolę programu Security Agent, gdzie wszystkie składniki są aktualne i działają prawidłowo:

W poniższej tabeli przedstawiono listę ikon interfejsu głównego użytkownika konsoli programu Security Agent wraz z ich znaczeniem:

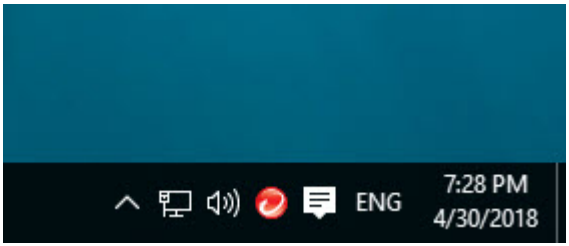
**TABELA A-1. Ikony interfejsu głównego użytkownika konsoli programu Security Agent**

| IKONA | STAN | OBJAŚNIENIE I DZIAŁANIE |
|---|---|---|
| | Ochrona włączona: Komputer jest chroniony a oprogramowanie jest aktualne | Oprogramowanie jest aktualne i działa prawidłowo. Nie są wymagane żadne czynności. |
| | Uruchom ponownie komputer: Ponownie uruchom komputer w celu dokończenia usuwania zagrożeń bezpieczeństwa | Program Security Agent wykrył zagrożenia, których nie można natychmiast usunąć.<br><br>Należy uruchomić ponownie komputer w celu ukończenia usuwania tych zagrożeń. |
| | Ochrona zagrożona: Skontaktuj się z administratorem | Funkcja skanowania w czasie rzeczywistym jest wyłączona lub występuje inne zagrożenie bezpieczeństwa.<br><br>Włącz funkcję skanowania w czasie rzeczywistym, a jeśli nie rozwiąże to problemu, skontaktuj się z pomocą techniczną. |
| | Aktualizuj teraz: Nie odebrano nowej aktualizacji przez (liczba) dni. | Sygnatura wirusów pochodzi sprzed więcej niż 3 dni.<br><br>Niezwłocznie zaktualizuj program Security Agent. |

| Ikona | Stan | Objaśnienie i działanie |
|---|---|---|
| | Usługa Smart Scan jest niedostępna: Sprawdź połączenie internetowe | Program Security Agent nie może uzyskać dostępu do serwera skanowania od co najmniej 15 minut.<br>Sprawdź, czy istnieje połączenie siecią, aby można było przeprowadzać skanowanie z użyciem najnowszych sygnatur. |
| | Uruchom ponownie komputer: Aby ukończyć instalowanie aktualizacji, ponownie uruchom komputer | Aby ukończyć instalowanie aktualizacji, należy ponownie uruchomić komputer. |
| | Aktualizowanie programu: Trwa aktualizacja oprogramowania zabezpieczającego | Aktualizacja jest w toku. Nie odłączaj się od sieci, dopóki nie aktualizacja zostanie zakończona. |

# Wyświetlanie ikon programu Security Agent na pasku zadań systemu Windows

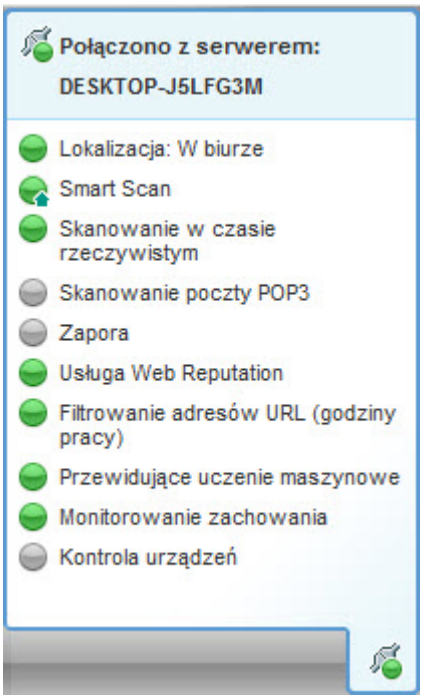
Następujące ikony programu Security Agent są wyświetlane na pasku zadań systemu Windows:



| Ikona | Znaczenie |
|---|---|
| | Stan normalny |
| | (animowane) Uruchomione jest skanowanie ręczne lub skanowanie zaplanowane. Program Security Agent korzysta z ustawienia Skanowanie standardowe lub Smart Scan. |
| | Program Security Agent przeprowadza aktualizację. |
| | Konieczne wykonanie operacji:<br>• Wyłączono skanowanie w czasie rzeczywistym<br>• Aby ukończyć czyszczenie złośliwego oprogramowania, jest wymagane ponowne uruchomienie komputera<br>• Wymagane ponowne uruchomienie komputera z powodu aktualizacji silnika skanowania<br>• Aby przywrócić pliki zaszyfrowane przez oprogramowanie typu ransomware, jest wymagane ponowne uruchomienie komputera<br>• wymagana aktualizacja.<br> **Uwaga**<br>Otwórz konsolę główną programu Security Agent, aby sprawdzić, jaka operacja jest wymagana. |

# Uzyskiwanie dostępu do konsoli Flyover

Konsola Security Agent Flyover zostanie otwarta po ustawieniu wskaźnika myszy nad małą ikoną znajdującą się z prawej strony, u dołu konsoli Security Agent.




W poniższej tabeli przedstawiono listę ikon konsoli Flyover razem z ich znaczeniem:

**TABELA A-2. Ikony konsoli Flyover**

| FUNKCJA | IKONA | ZNACZENIE |
|---|---|---|
| Połączenie | | Połączono z Security Server |
| | | Nie połączono z Security Server, ale skanowanie w czasie rzeczywistym jest nadal uruchomione. Plik sygnatur może być nieaktualny. Kliknij prawym przyciskiem myszy ikonę agenta na pasku zadań systemu Windows i kliknij polecenie **Aktualizuj teraz**. |

| FUNKCJA | IKONA | ZNACZENIE |
|---|---|---|
| Lokalizacja | | W biurze (sieć wewnętrzna) |
| | | Poza biurem (sieć zewnętrzna) |
| Skanowanie w czasie rzeczywistym | | Wł. |
| | | Wył. |
| Skanowanie poczty POP3 | | Wł. |
| | | Wył. |
| Smart Scan | | Połączono z siecią Trend Micro Smart Protection Network |
| | | Nie można nawiązać połączenia z siecią Smart Protection Network; ochrona jest ograniczona, ponieważ programy Security Agent nie mogą wysyłać zapytań dotyczących skanowania.<br><br>**Uwaga**<br>Sprawdź, czy usługa Smart Scan o nazwie TMiCRCScanService jest uruchomiona, a także czy Security Agent są połączone z Security Server. |
| | | Inteligentne Smart Scan jest wyłączone. Używanie tradycyjnego skanowania |

| Funkcja | Ikona | Znaczenie |
|---|---|---|
| • Zapora<br>• Usługa Web Reputation<br>• Filtrowanie adresów URL<br>• Monitorowanie zachowania<br>• Kontrola urządzeń<br>• Przewidujące uczenie maszynowe | | Wł. |
| | | Wył. |

# Dodatek B

# Obsługa protokołu IPv6 w programie Worry-Free Business Security

Ten załącznik stanowi wymaganą lekturę dla użytkowników, którzy planują wdrożenie programu Worry-Free Business Security w środowisku obsługującym adresowanie IPv6. Zawarto tu informacje dotyczące obsługi protokołu IPv6 w programie Worry-Free Business Security.

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 w programie Worry-Free Business Security i Security Agent

Obsługa protokołu IPv6 w programie Worry-Free Business Security pojawiła się po raz pierwszy w wersji 8.0. Wcześniejsze wersje programu Worry-Free Business Security nie obsługiwały adresowania IPv6. Obsługa protokołu IPv6 zostaje włączona automatycznie po zainstalowaniu lub zaktualizowaniu serwera Security Server oraz programów Security Agent i Messaging Security Agent spełniających wymagania protokołu IPv6.

## Wymagania programu Security Server dotyczące protokołu IPv6

Poniżej przedstawiono wymagania protokołu IPv6 dotyczące serwera Security Server:

- Jeśli serwer ma zarządzać agentami wykorzystującymi protokół IPv4 i IPv6, musi on mieć zarówno adres IPv4, jak i IPv6, oraz być identyfikowany nazwą hosta. Jeśli serwer jest identyfikowany adresem IPv4, nie będzie możliwe nawiązanie połączenia między nim i agentami wykorzystującymi protokół IPv6. Taka sama sytuacja zachodzi między klientami z protokołem IPv4 i serwerem identyfikowanym adresem IPv6.

- Jeśli serwer ma zarządzać tylko agentami wykorzystującymi protokół 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.

- Upewnij się, że adres IPv6 lub IPv4 hosta można uzyskać na przykład przy użyciu polecenia „`ping`” lub „`nslookup`”.

- Jeśli instalujesz program Security Server na komputerze z samym protokołem IPv6, skonfiguruj serwer proxy z podwójnym stosem. Umożliwi to zamianę adresów IP (np. DeleGate). Umieść serwer proxy między serwerem Security Server a Internetem, aby umożliwić serwerowi nawiązanie połączenia z usługami

obsługiwanymi przez firmę Trend Micro, takimi jak serwer ActiveUpdate, witryna Online Registration i sieć Smart Protection Network.

## Wymagania dotyczące programu Messaging Security Agent

Program Messaging Security Agent (tylko w wersji Advanced) musi być instalowany na serwerze Microsoft Exchange z dwoma stosami lub wykorzystującym wyłącznie protokół IPv6.

Zaleca się, aby program Messaging Security Agent 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 Security Server, który ma tylko adres IPv6.

**TABELA B-1. Ograniczenia serwera wykorzystującego wyłącznie protokół IPv6**

| ELEMENT | OGRANICZENIE |
|---|---|
| Zarządzanie agentami | Serwer wykorzystujący wyłącznie protokół IPv6 nie może:<br>• Instalować agentów na klientach wykorzystujących tylko protokół IPv4.<br>• Zarządzać agentami wykorzystującymi wyłącznie protokół IPv4. |
| Aktualizacje i scentralizowane zarządzanie | Serwer wykorzystujący wyłącznie protokół IPv6 nie może wykonywać aktualizacji ze źródeł wykorzystujących wyłącznie protokół IPv4, takich jak:<br>• Serwer Trend Micro ActiveUpdate Server<br>• Dowolne niestandardowe źródło aktualizacji wykorzystujące wyłącznie protokół IPv4 |

| Element | Ograniczenie |
|---|---|
| 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:<br>• Agenty lub hosty wykorzystujące wyłącznie protokół IPv4 (ze względu na brak bezpośredniego połączenia).<br>• Agenty 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 Security Server a obiektami, z którymi się łączy lub które obsługuje.

## Ograniczenia Security Agent wykorzystującego wyłącznie protokół IPv6

Poniższa tabela przedstawia ograniczenia klienta Security Agent, który ma tylko adres IPv6.

**Tabela B-2. Ograniczenia Security Agent wykorzystującego wyłącznie protokół IPv6**

| Element | Ograniczenie |
|---|---|
| Nadrzędny serwer Security Server | Agentami wykorzystującymi wyłącznie protokół IPv6 nie można zarządzać za pomocą serwera Security Server, który wykorzystuje wyłącznie protokół IPv4. |

| Element | Ograniczenie |
|---|---|
| Aktualizacje | Klient Security Agent wykorzystujący wyłącznie protokół IPv6 nie może wykonywać aktualizacji ze źródeł wykorzystujących wyłącznie protokół IPv4, takich jak:<br>• Serwer Trend Micro ActiveUpdate Server<br>• Serwer Security Server wykorzystujący wyłącznie protokół IPv4<br>• Agent aktualizacji wykorzystujący wyłącznie protokół IPv4<br>• Dowolne niestandardowe źródło aktualizacji wykorzystujące wyłącznie protokół IPv4 |
| Żądania skanowania i funkcja Smart Feedback | Program Security Agent wykorzystujący wyłącznie protokół IPv6 nie może wysyłać żądań do sieci Trend Micro Smart Protection Network ani używać funkcji Smart Feedback. |
| Rozwiązania dodatków | Agenty wykorzystujące wyłącznie protokół IPv6 nie mogą instalować rozwiązań dodatków, ponieważ żadne rozwiązania dodatków nie obsługują protokołu IPv6. |
| Połączenie proxy | Klient Security Agent 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 Security Agent 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 Worry-Free Business Security 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 Worry-Free Business Security 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 Worry-Free Business Security. Na przykład agenty Security Agent 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 Security Agent, ale agenty Security Agent je zignorują. Jeśli na przykład skonfigurowano listę źródeł Smart Protection i umieszczono na niej Smart Protection Server zidentyfikowany za pomocą adresu IPv6, agenty Security Agent 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.

- Drzewo Grupy zabezpieczeń

  We wszystkich miejscach, w których pojawia się drzewo grup zabezpieczeń, adresy IPv6 agentów wykorzystujących wyłącznie protokół IPv6 są wyświetlane w kolumnie **Adres IP**. W przypadku agentów z dwoma stosami ich adresy IPv6 są wyświetlane, jeśli do rejestracji na serwerze użyto adresu IPv6.

  **Uwaga**

  Adres IP używany przez agenty z dwoma stosami podczas rejestrowania się na serwerze można ustawić w części **Preferowany adres IP** na karcie **Administracja** > **Ustawienia globalne** > **Komputer/serwer**.

  Podczas eksportowania ustawień agenta do pliku adresy IPv6 są także widoczne w wyeksportowanym pliku.

- Dzienniki

  Adresy IPv6 agentów z dwoma stosami i agentów wykorzystujących wyłącznie protokół IPv6 są wyświetlane w dziennikach.

# Dodatek C

## 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 **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

Z przedstawicielami firmy Trend Micro można skontaktować się telefonicznie lub pocztą e-mail:

| | |
|---|---|
| Adres | Trend Micro (EMEA) Limited - Central Eastern Europe, Office in Warsaw<br>Warsaw Trade Tower<br>Floor 30, Chłodna 51<br>00-867 Warszawa |
| Telefon | +48 (22)486 34 50 |
| Witryna internetowa | http://www.trendmicro.pl |

| | |
|---|---|
| Adres e-mail | biuro@trendmicro.com |

- Lista biur pomocy technicznej na całym świecie:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Kontakt z firmą Trend Micro:

  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.

## Email Reputation Services

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

# Dodatek D

## Terminologia i pojęcia związane z produktami

Pozycje tego dodatku zawierają dalsze informacje na temat produktów i technologii firmy Trend Micro.

# Poprawka krytyczna

Poprawka krytyczna koncentruje się na problemach zabezpieczeń i nadaje się do instalacji na wszystkich klientach. Poprawki krytyczne dla systemu Windows zawierają program instalacyjny, poprawki dla pozostałych systemów zazwyczaj zawierają skrypt instalacyjny.

# 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.

# 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

Mechanizm IntelliTrap jest heurystyczną technologią firmy Trend Micro służącą do wykrywania zagrożeń wykorzystujących kompresję w czasie rzeczywistym oraz inne charakterystyczne cechy złośliwego oprogramowania, na przykład samorozpakowujące się archiwa. Obejmuje to wirusy, programowanie typu malware, robaki, trojany, samorozpakowujące się archiwa oraz boty. Autorzy wirusów/złośliwego oprogramowania często podejmują próby ominięcia zabezpieczeń antywirusowych, stosując różne schematy kompresji. Technologia IntelliTrap to oparty na regułach i działający w czasie rzeczywistym silnik skanowania i rozpoznawania sygnatur, który wykrywa i usuwa znane wirusy / złośliwe oprogramowanie z plików o nawet 17 warstwach kompresji, generowanej za pomocą jednego z 16 popularnych typów kompresji.

**Uwaga**

Mechanizm IntelliTrap korzysta z tego samego silnika skanowania, co używany podczas skanowania w poszukiwaniu wirusów. W związku z tym reguły obsługi i skanowania plików mechanizmu IntelliTrap będą identyczne z regułami określonymi przez administratora dla skanowania w poszukiwaniu wirusów.

Agent zapisuje przypadki wykrycia botów i innego złośliwego oprogramowania do dziennika mechanizmu IntelliTrap. Zawartość dziennika mechanizmu IntelliTrap może być eksportowana w celu włączenia do raportów.

Mechanizm IntelliTrap używa następujących elementów podczas sprawdzania w poszukiwaniu botów i innego złośliwego oprogramowania:

- Silnik skanowania antywirusowego
- Sygnatura IntelliTrap
- Sygnatura wyjątków IntelliTrap

# System wykrywania włamań (IDS)

System wykrywania włamań (IDS) pomaga identyfikować sygnatury w pakietach sieciowych, które mogą wskazywać na atak na punkt końcowy.

System wykrywania włamań (IDS) umożliwia zapobieganie następującym znanym typom ataków:

| Atak | Opis |
|---|---|
| **Zbyt duży fragment** | Atak typu Denial of Service, w którym haker kieruje do zaatakowanego punktu końcowego ponadwymiarowy pakiet TCP/UDP. Może to spowodować przepełnienie bufora, co w efekcie może zablokować punkt końcowy lub spowodować ponowne jego uruchomienie. |
| **Atak Ping of Death** | Atak typu Denial of Service, w którym haker kieruje do zaatakowanego punktu końcowego ponadwymiarowy pakiet ICMP/ICMPv6. Może to spowodować przepełnienie bufora, co w efekcie może zablokować punkt końcowy lub spowodować ponowne jego uruchomienie. |
| **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 punktu końcowego. Zaatakowany punkt końcowy nieprzerwanie wysyła odpowiedź ARP (własny adres MAC) do samego siebie, co powoduje awarie oraz blokowanie punktu końcowego. |
| **Atak typu SYN flood** | Atak typu Denial of Service, w którym program wysyła do punktu końcowego wiele pakietów synchronizacji TCP (SYN), powodując nieprzerwane wysyłanie przez punkt końcowy odpowiedzi oznaczających potwierdzenie synchronizacji (SYN/ACK). Może to wyczerpać pamięć punktu końcowego i doprowadzić do jego awarii. |
| **Nakładające się fragmenty** | Podobnie jak w przypadku ataku typu Teardrop, w tym ataku typu Denial of Service do zaatakowanego punktu końcowego 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 zaatakowanego punktu końcowego następujących po sobie fragmentów ze złośliwym kodem. |

| Atak | Opis |
|---|---|
| **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 odbierającego punktu końcowego 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 zaatakowanego punktu końcowego, który nie jest w stanie poprawnie ich przetworzyć. Może to spowodować zablokowanie punktu końcowego lub spowolnienie jego pracy. |
| **Atak typu LAND** | Typ ataku, w którym do zaatakowanego punktu końcowego wysyłane są pakiety synchronizacji IP (SYN) o takim samym adresie źródłowym i docelowym, powodując wysyłanie przez punkt końcowy odpowiedzi oznaczających potwierdzenie synchronizacji (SYN/ACK) do samego siebie. Może to spowodować zablokowanie punktu końcowego lub spowolnienie jego pracy. |

# Słowa kluczowe

Poniżej przedstawiono słowa kluczowe, które są używane w programie Worry-Free Business Security do filtrowania wiadomości:

- słowa (pistolety, bomby itd.);
- cyfry (1, 2, 3 itd.);
- znaki specjalne (&, #, + itd.);
- krótkie frazy (niebieska ryba, czerwony telefon, duży dom itd.);

- słowa lub frazy połączone operatorami logicznymi (jabłka .AND. pomarańcze);
- słowa lub frazy oparte na wyrażeniach regularnych (na przykład wzorzec .REG. a.*e spowoduje trafienie w przypadku słów „ale”, „ave” i „apanaże”, ale nie „akt”, „aby” czy „antywirus”);

Program Worry-Free Business Security umożliwia importowanie istniejącej listy słów kluczowych z pliku tekstowego (`.txt`). Zaimportowane słowa kluczowe pojawiają się na liście.

### Operatory dotyczące słów kluczowych

Operatory to polecenia łączące wiele słów kluczowych. Operatory mogą rozszerzać lub zawężać wyniki dla danych kryteriów. Operatory należy otoczyć kropkami (.). Na przykład:

```
jabłka .AND. pomarańcze lub jabłka .NOT. pomarańcze
```

**Uwaga**

Bezpośrednio przed i za operatorem występuje kropka. Między kropką kończącą a słowem kluczowym znajduje się znak spacji.

**TABELA D-1. Korzystanie z operatorów**

| OPERATOR | SPOSÓB DZIAŁANIA | PRZYKŁAD |
|---|---|---|
| dowolne słowo kluczowe | Program Messaging Security Agent wyszukuje zawartość pasującą do słowa. | Wpisz słowo i dodaj je do listy słów kluczowych. |

| Operator | Sposób działania | Przykład |
|---|---|---|
| OR | Program Messaging Security Agent będzie szukał zawartości, w której występuje którekolwiek ze słów kluczowych rozdzielonych operatorem OR.<br><br>Na przykład: jabłka OR pomarańcze. Agent wyszuka zawartość, w której występuje słowo „jabłka” bądź „pomarańcze”. Jeśli treść zawiera któreś z nich, zgłaszane jest dopasowanie. | Wpisz „.OR.” między wszystkimi słowami, które mają zostać uwzględnione.<br><br>Na przykład:<br><br>„jabłka .OR. pomarańcze” |
| AND | Program Messaging Security Agent będzie szukał zawartości, w której występują wszystkie słowa kluczowe rozdzielone operatorem AND.<br><br>Na przykład: jabłka AND pomarańcze. Agent wyszuka zawartość, w której występuje zarówno słowo „jabłka”, jak i „pomarańcze”. Jeśli treść nie zawiera obydwu słów, nie ma dopasowania. | Wpisz operator „.AND.” między wszystkimi słowami, które mają zostać uwzględnione.<br><br>Na przykład:<br><br>„jabłka .AND. pomarańcze” |
| NOT | Słowa kluczowe poprzedzone operatorem NOT są wykluczane z wyszukiwania w programie Messaging Security Agent.<br><br>Na przykład zapis „.NOT. duże” powoduje, że agent wyszuka zawartość bez słowa „duże”. Jeśli w wiadomości obecny jest tekst „dojrzałe pomarańcze”, to dopasowanie istnieje; jeśli jednak obecny jest tekst „duże pomarańcze”, to dopasowanie nie istnieje. | Wpisz „.NOT.” przed słowem, które ma zostać wykluczone.<br><br>Na przykład:<br><br>„.NOT. duże” |

| Operator | Sposób działania | Przykład |
|---|---|---|
| WILD | Symbol wieloznaczny zastępuje brakującą część słowa. Zwracane są wszystkie wpisane słowa z dowolnymi znakami odpowiadającymi symbolowi wieloznacznemu.<br><br>**Uwaga**<br>Program Messaging Security Agent nie umożliwia stosowania znaku „?” w poleceniu symbolu wieloznacznego „.WILD.”. | Wpisz „`.WILD.`” przed częściami słów, które mają zostać uwzględnione.<br><br>Na przykład aby dopasować wszystkie słowa zawierające ciąg „wart”, wpisz „`.WILD.valu`”. Pasować będą wszystkie słowa spośród: Wartburg, wartko i wartownicy. |
| REG | Aby określić wyrażenie regularne, należy przed wzorcem dodać operator .REG. (na przykład, .REG. a.*e).<br><br>Patrz sekcja *Wyrażenia regularne na stronie D-11*. | Wpisz operator „`.REG.`” przed wzorcem słowa, który ma zostać wykryty.<br><br>Na przykład do wzorca „.REG. a.*e” pasują: „ale”, „ave” i „apanaże”, ale nie „akt”, „aby” czy „antywirus”. |

## Efektywne korzystanie ze słów kluczowych

Program Messaging Security Agent zawiera proste w użyciu i rozbudowane funkcje tworzenia wysoce wyspecjalizowanych filtrów. Podczas tworzenia reguł filtrowania zawartości należy uwzględnić następujące uwagi:

- Program Messaging Security Agent domyślnie wyszukuje dokładnie dopasowane słowa kluczowe. Aby wyszukać słowa częściowo pasujące do słów kluczowych, należy użyć wyrażeń regularnych. Patrz sekcja *Wyrażenia regularne na stronie D-11*.
- Program Messaging Security Agent inaczej analizuje wiele słów kluczowych umieszczonych w jednym wierszu, wiele słów kluczowych umieszczonych w oddzielnych wierszach oraz wiele słów kluczowych rozdzielonych przecinkami, kropkami, dywizami lub innymi znakami interpunkcyjnymi. Więcej informacji na temat używania słów kluczowych w wielu wierszach zawiera tabela poniżej.

- Program Messaging Security Agent można skonfigurować tak, aby wyszukiwał synonimy słów kluczowych.

**TABELA D-2. Sposób korzystania ze słów kluczowych**

| SYTUACJA | PRZYKŁAD | DOPASOWANIE/NIEDOPASOWANIE |
|---|---|---|
| Dwa słowa w jednym wierszu | pistolety bomby | Dopasowanie:<br>„Kliknij tutaj, aby kupić pistolety bomby i inną broń.”<br>Brak dopasowania:<br>„Kliknij tutaj, aby kupić pistolety i bomby.” |
| Dwa słowa rozdzielone przecinkiem | pistolety, bomby | Dopasowanie:<br>„Kliknij tutaj, aby kupić pistolety, bomby i inną broń.”<br>Brak dopasowania:<br>„Kliknij tutaj, aby kupić używane pistolety, nowe bomby i inną broń.” |

| SYTUACJA | PRZYKŁAD | DOPASOWANIE/NIEDOPASOWANIE |
|---|---|---|
| Wiele słów w kilku wierszach | pistolety<br>bomby<br>broń i amunicja | Po wybraniu opcji **Którekolwiek z podanych słów kluczowych**<br>Dopasowanie:<br>„Pistolety na sprzedaż”<br>Pasuje też:<br>„Do kupienia pistolety, bomby i inna broń”<br>Po wybraniu opcji **Wszystkie podane słowa kluczowe**<br>Dopasowanie:<br>„Do kupienia pistolety bomby broń i amunicja”<br>Brak dopasowania:<br>„Do kupienia pistolety bomby broń amunicja”<br>Nie pasuje też:<br>„Do kupienia pistolety, bomby, broń i amunicja” |
| Wiele słów kluczowych w jednym wierszu | pistolety bomby broń amunicja | Dopasowanie:<br>„Do kupienia pistolety bomby broń amunicja”<br>Brak dopasowania:<br>„Do kupienia amunicja do pistoletów oraz broń i nowe bomby” |

# 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.

# Wyrażenia regularne

Wyrażenia regularne służą do dopasowywania łańcuchów znaków. Niektóre typowe przykłady wyrażeń regularnych podano w następujących tabelach. Aby określić wyrażenie regularne, podany wzorzec należy poprzedzić operatorem „.REG.”.

W sieci jest dostępnych wiele witryn i przewodników. Jedną z takich witryn jest PerlDoc, dostępna pod adresem:

http://www.perl.com/doc/manual/html/pod/perlre.html

**OSTRZEŻENIE!**

Wyrażenia regularne to bardzo skuteczne narzędzie służące do dopasowywania łańcuchów znaków. Dlatego też firma Trend Micro zaleca, aby administratorzy decydujący się na korzystanie z nich, znali dobrze ich składnię. Błędnie napisane wyrażenia regularne mogą znacznie obniżyć wydajność. Firma Trend Micro zaleca stosowanie na początku prostych wyrażeń regularnych, które nie mają skomplikowanej składni. Wprowadzając nowe reguły, należy korzystać z funkcji archiwizacji i obserwować, jak program Messaging Security Agent zarządza wiadomościami przy użyciu tych reguł. Gdy okaże się, że reguła nie wprowadza żadnych nieoczekiwanych zmian, można zmienić akcję.

## Przykłady wyrażeń regularnych

Niektóre typowe przykłady wyrażeń regularnych podano w następujących tabelach. Aby określić wyrażenie regularne, podany wzorzec należy poprzedzić operatorem „.REG.”.

**TABELA D-3. Zliczanie i grupowanie**

| ELEMENT | ZNACZENIE | PRZYKŁAD |
|---|---|---|
| . | Znak kropki reprezentuje dowolny znak, z wyjątkiem znaku nowej linii. | Ciąg pie. powoduje dopasowanie słowa pies, piec itd.<br>Ciąg za.p powoduje dopasowanie słowa zakup, zakop itd. |
| * | Znak gwiazdki oznacza zero lub więcej wystąpień elementu poprzedzającego. | Ciąg do* powoduje dopasowanie ciągów znaków d, do, doo, dooo itd. |

| Element | Znaczenie | Przykład |
|---|---|---|
| + | Znak plus oznacza jedno lub więcej wystąpień elementu poprzedzającego. | Ciąg do+ powoduje dopasowanie ciągów znaków do, doo, dooo itd., ale nie d. |
| ? | Znak zapytania oznacza zero lub jedno wystąpienie elementu poprzedzającego. | Ciąg wie?lki powoduje dopasowanie słów wilki i wielki, ale nie wieelki, wieeelki itd. |
| ( ) | Nawiasy służą do łączenia wzorca znajdującego się między nimi w jedną grupę, która jest następnie traktowana jak pojedynczy element. | Ciąg j(eleń)+ powoduje dopasowanie słowa jeleń, jeleńeleń lub jeleńeleńeleń itd. Znak + odnosi się do ciągu ujętego w nawiasy, więc funkcja dopasowuje znak j, po którym następuje jedno lub więcej wystąpień ciągu „eleń”. |
| [ ] | Nawiasy kwadratowe wskazują zbiór lub zakres znaków. | Ciąg d[aeiouy]+ powoduje dopasowanie ciągów znaków da, de, di, do, du, dy, daa, dae, dai itd. Znak + odnosi się do zbioru wskazanego w nawiasach, więc funkcja dopasowuje znak d, po którym następuje jeden lub więcej znaków ze zbioru [aeiouy].<br><br>Do d[A-Z] pasują: dA, dB, dC itd. aż do dZ. Zestaw w nawiasach kwadratowych reprezentuje przedział złożony ze wszystkich wielkich liter: od A do Z. |
| [ ^ ] | Znak daszka w nawiasach kwadratowych logicznie neguje określony zbiór lub zakres. Funkcja dopasuje więc każdy znak, który nie znajduje się w zbiorze lub zakresie. | Do d[^aeiouy] pasują: db, dc lub dd, d9, d#, czyli litera d, po której następuje dowolny pojedynczy znak, z wyjątkiem samogłoski nienosowej. |

| Element | Znaczenie | Przykład |
|---|---|---|
| { } | Nawiasy klamrowe określają konkretną liczbę wystąpień elementu poprzedzającego. Pojedyncza wartość w nawiasach spowoduje dopasowanie dokładnie takiej liczby wystąpień. Para liczb rozdzielonych przecinkiem reprezentuje zbiór właściwych liczb wystąpień poprzedniego znaku. Pojedyncza cyfra, po której następuje przecinek, oznacza brak górnej granicy. | Do da{3} pasuje daaa, czyli litera d, po której następują dokładnie 3 wystąpienia litery „a”. Do da{2,4} pasują: daa, daaa, daaaa, and daaaa (ale nie: daaaaa), czyli litera d, po której następują 2, 3 lub 4 wystąpienia litery „a”. Do da{4,} pasują: daaaa, daaaaa, daaaaaa itd., czyli litera d, po której następują nie mniej niż 4 wystąpienia litery „a”. |

**Tabela D-4. Klasy znaków (zapis skrótowy)**

| Element | Znaczenie | Przykład |
|---|---|---|
| \d | Dowolny znak cyfry. Zapis ten jest równoważny oznaczeniu [0-9] i [[:digit:]]. | Do \d pasują: 1, 12, 123 itd., ale nie 1b7, czyli przynajmniej jedna cyfra. |
| \D | Dowolny znak oprócz cyfr. Zapis ten jest równoważny oznaczeniu [^0-9] i [^[:digit:]]. | Ciąg \D powoduje dopasowanie ciągów a, ab, ab&, ale nie 1 — czyli jednego lub więcej wystąpień dowolnego znaku oprócz 0, 1, 2, 3, 4, 5, 6, 7, 8 lub 9. |
| \w | Dowolny znak „słowa”, tzn. dowolny znak alfanumeryczny; funkcjonalny odpowiednik zapisu [_A-Za-z0-9] lub [_[:alnum:]] | Ciąg \w powoduje dopasowanie zwrotów a, ab, a1, ale nie !& — czyli jednej lub więcej małych bądź wielkich liter lub cyfr, ale nie znaków interpunkcyjnych ani innych znaków specjalnych. |
| \W | Dowolny znak niealfanumeryczny; funkcjonalny odpowiednik zapisu [^_A-Za-z0-9] lub [^_[:alnum:]] | Ciąg \W powoduje dopasowanie zwrotów *, &, ale nie as czy a1 — czyli jednego lub więcej dowolnych znaków z wyjątkiem małych i wielkich liter oraz cyfr. |

| Element | Znaczenie | Przykład |
|---|---|---|
| \s | Dowolny znak odstępu: znak spacji, nowego wiersza, tabulatora, spacji nierozdzielającej itd. Ten zapis jest równoważny oznaczeniu [[:space:]]. | Ciąg por\s odpowiada zwrotowi „por”, po którym następuje dowolny znak niewidoczny. Zatem na frazę „Lubię por w zupie” funkcja regex zareagowałaby, ale na frazę „Lubię pory w zupie” już nie. |
| \S | Dowolny znak inny niż odstęp: wszystko oprócz znaku spacji, nowego wiersza, tabulatora, spacji nierozdzielającej itd. Ten zapis jest równoważny oznaczeniu [^[:space:]]. | Ciąg por\S odpowiada zwrotowi „por”, po którym następuje dowolny znak widoczny. Zatem na frazę „Lubię pory w zupie” funkcja regex zareagowałaby, ale na frazę „Lubię por w zupie” już nie. |

**Tabela D-5. Klasy znaków**

| Element | Znaczenie | Przykład |
|---|---|---|
| [:alpha:] | Dowolny znak alfabetyczny | .REG. [[:alpha:]] powoduje dopasowanie ciągów znaków abc, def, xxx, ale nie 123 ani @# $. |
| [:digit:] | Dowolna cyfra; funkcjonalny odpowiednik zapisu \d | .REG. [[:digit:]] powoduje dopasowanie ciągów znaków 1, 12, 123 itd. |
| [:alnum:] | Dowolny znak „słowa”, tzn. dowolny znak alfanumeryczny; funkcjonalny odpowiednik zapisu \w. | .REG. [[:alnum:]] powoduje dopasowanie ciągów znaków abc, 123, ale nie ~!@. |
| [:space:] | Dowolny znak biały: znak odstępu, nowej linii, tabulacji, odstępu nierozdzielającego itd. Zapis ten jest równoważny oznaczeniu \s. | .REG. (por)[[:space:]] powoduje dopasowanie słowa „por”, po którym następuje dowolny znak niewidoczny. Zatem na frazę „Lubię por w zupie” funkcja regex zareagowałaby, ale na frazę „Lubię pory w zupie” już nie. |

| Element | Znaczenie | Przykład |
|---|---|---|
| [:graph:] | Dowolne znaki z wyjątkiem znaku odstępu, znaków sterujących itp. | .REG. [[:graph:]] pasują: 123, abc, xxx, ><", ale nie spacja ani znaki sterujące. |
| [:print:] | Dowolne znaki (podobnie jak [:graph]), ale obejmuje także znak odstępu. | .REG. [[:print:]] pasują 123, abc, xxx, ><" i spacje. |
| [:cntrl:] | Dowolne znaki sterujące (np. CTRL+C, CTRL+X) | .REG. [[:cntrl:]] powoduje dopasowanie ciągów znaków 0x03, 0x08, ale nie abc, 123, ! @#. |
| [:blank:] | Znaki odstępu i tabulacji | .REG. [[:blank:]] powoduje dopasowanie znaków odstępu i tabulacji, ale nie ciągów znaków 123, abc, !@#. |
| [:punct:] | Znaki interpunkcyjne | .REG. [[:punct:]] powoduje dopasowanie znaków ; : ? ! ~ @ # $ % & * ' " itd., ale nie ciągów 123, abc. |
| [:lower:] | Dowolne małe litery. (Uwaga: musi być włączona opcja „Dopasuj z uwzględnieniem wielkości liter", bo w przeciwnym razie będzie funkcjonować jako [:alnum:]). | .REG. [[:lower:]] powoduje dopasowanie ciągów znaków abc, Def, sTres, Do itp., ale nie ABC, DEF, STRES, DO, 123, ! @#. |
| [:upper:] | Dowolne wielkie litery. (Uwaga: musi być włączona opcja „Dopasuj z uwzględnieniem wielkości liter", bo w przeciwnym razie będzie funkcjonować jako [:alnum:]). | .REG. [[:upper:]] powoduje dopasowanie ciągów znaków ABC, DEF, STRES, DO itp., ale nie abc, Def, Stres, Do, 123, ! @#. |
| [:xdigit:] | Cyfry dozwolone w liczbach szesnastkowych (0-9a-fA-F). | .REG. [[:xdigit:]] powoduje dopasowanie ciągów znaków 0a, 7E, 0f itd. |

**TABELA D-6. Punkty zaczepienia wzorców**

| ELEMENT | ZNACZENIE | PRZYKŁAD |
|---|---|---|
| ^ | Wskazuje początek ciągu znaków. | Ciąg ^(mimo wszystko) powoduje dopasowanie dowolnego bloku tekstu zaczynającego się słowami „mimo wszystko”. Zatem na frazę „mimo wszystko faktycznie lubię pory w zupie” funkcja regex zareagowałaby, ale na frazę „faktycznie lubię pory w zupie mimo wszystko” już nie. |
| $ | Wskazuje koniec ciągu znaków. | Ciąg (mimo wszystko)$ powoduje dopasowanie dowolnego bloku tekstu kończącego się słowami „mimo wszystko”. Zatem na frazę „mimo wszystko faktycznie lubię pory w zupie” funkcja regex nie zareagowałaby, ale na frazę „faktycznie lubię pory w zupie mimo wszystko” — tak. |

**TABELA D-7. Sekwencje specjalne i łańcuchy literałowe**

| ELEMENT | ZNACZENIE | PRZYKŁAD |
|---|---|---|
| \ | Służy do dopasowywania znaków mających specjalne znaczenie w wyrażeniu regularnym (na przykład „+”). | (1) Do .REG. C\\C\+\+ powoduje dopasowanie ciągów znaków C \C++.<br>(2) Do .REG. * pasuje znak *.<br>(3) Do .REG. \? pasuje znak ?. |
| \t | Oznacza znak tabulatora. | Ciąg (stres)\t powoduje dopasowanie dowolnego bloku tekstu zawierającego podłańcuch „stres”, po którym bezpośrednio następuje tabulator (znak 0x09 w kodzie ASCII). |

| Element | Znaczenie | Przykład |
|---|---|---|
| \n | Oznacza znak nowego wiersza.<br><br>**Uwaga**<br>Znak nowego wiersza różni się w zależności od platformy. W systemie Windows jest to para znaków: znak powrotu karetki, po którym występuje znak wysuwu wiersza. W systemach Unix i Linux nowy wiersz jest oznaczany samym znakiem przejścia do nowego wiersza, natomiast w systemie Macintosh nowy wiersz jest oznaczany samym znakiem powrotu karetki. | Ciąg (stres)\n\n powoduje dopasowanie dowolnego bloku tekstu zawierającego podciąg stres, bezpośrednio po którym występują dwa znaki nowego wiersza (kod ASCII 0x0A). |
| \r | Oznacza znak powrotu karetki. | Ciąg (stres)\r powoduje dopasowanie dowolnego bloku tekstu zawierającego podłańcuch „stres”, po którym bezpośrednio następuje jeden znak powrotu karetki (znak 0x0D w kodzie ASCII). |

| Element | Znaczenie | Przykład |
|---|---|---|
| \b | Oznacza znak cofania.<br>OR<br>Oznacza granice. | Ciąg (stres)\b powoduje dopasowanie dowolnego bloku tekstu zawierającego podciąg „stres”, po którym bezpośrednio następuje jeden znak cofania (kod ASCII 0x08).<br>Granica słowa (\b) to punkt między dwoma znakami, gdzie po jednej stronie znajduje się ciąg \w, a po drugiej ciąg \W (w dowolnej kolejności), zliczający znaki pozorne od końca i od początku ciągu zgodnego z \W. (W klasach znaków \b oznacza znak cofania, a nie granicę słowa).<br>Przykładowo poniższe wyrażenie regularne pasuje do numeru ubezpieczenia społecznego: .REG. \b\d{3}-\d{2}-\d{4}\b |
| \xhh | Oznacza znak w kodzie ASCII o podanym numerze szesnastkowym (hh reprezentuje dowolną dwucyfrową liczbę szesnastkową). | Ciąg \x7E(\w){6} powoduje dopasowanie dowolnego bloku tekstu zawierającego „słowo” składające się z dokładnie sześciu znaków alfanumerycznych poprzedzonych znakiem tyldy (~). Zatem pasowałyby słowa „~ab12cd”, „~Pa3499”, ale słowo „~ojej” już nie. |

## Generator wyrażeń regularnych

Przy podejmowaniu decyzji o konfiguracji reguł funkcji zapobiegania utracie danych należy pamiętać, że generator wyrażeń regularnych służy wyłącznie do tworzenia prostych wyrażeń zgodnie z poniższymi regułami i ograniczeniami:

- zmiennymi mogą być wyłącznie znaki alfanumeryczne;

- wszystkie pozostałe znaki, takie jak [-], [/] itp., mogą być wyłącznie stałymi;
- można używać wyłącznie przedziałów zmiennych A-Z i 0-9, nie można ograniczać przedziałów do, przykładowo, zakresu A-D;
- w wyrażeniach regularnych generowanych przez to narzędzie nie rozpoznaje się wielkości liter;
- Wyrażeń regularnych generowanych przez to narzędzie można używać tylko w pozytywnych warunkach wyszukiwania, a nie negatywnych („jeżeli nie jest zgodne").
- Wyrażenia oparte na przykładzie umożliwiają tylko wyszukiwanie dokładnie takiej samej liczby znaków i spacji, jak w przykładzie; to narzędzie nie generuje wzorców, dla których istnieje „jeden lub kilka" odpowiedników danego znaku lub łańcucha.

### Składnia wyrażeń złożonych

Wyrażenie słowa kluczowego złożone jest z tokenów, które są najmniejszą jednostką używaną do dopasowania wyrażenia do treści. Tokenem może być operator, symbol logiczny lub operant tj. argument lub wartość, na której działa operator.

Operatory obejmują .AND., .OR., .NOT., .NEAR., .OCCUR., .WILD., ".(." i " .)." Operant i operator muszą być oddzielone spacją. Operant może również zawierać kilka tokenów. Patrz sekcja *Słowa kluczowe na stronie D-5*.

### Wyrażenia regularne w praktyce

Następujący przykład opisuje jak działa filtr numeru ubezpieczenia społecznego, jeden z domyślnych filtrów:

[Format] .REG. \b\d{3}-\d{2}-\d{4}\b

Powyższe wyrażenie wykorzystuje przełącznik \b (znak cofania), następnie przełącznik \d (dowolna cyfra), następnie {x} (liczba cyfr), a na końcu - (łącznik). To wyrażenie powoduje dopasowanie numeru ubezpieczenia społecznego. Następująca tabela opisuje ciągi tekstowe które pasują do przykładowego wyrażenia regularnego:

**TABELA D-8. Numery pasujące do wyrażenia regularnego numeru ubezpieczenia społecznego**

| .REG. \b\d{3}-\d{2}-\d{4}\b |
|---|

| | |
|---|---|
| 333-22-4444 | Dopasowanie |
| 333224444 | Brak dopasowania |
| 333 22 4444 | Brak dopasowania |
| 3333-22-4444 | Brak dopasowania |
| 333-22-44444 | Brak dopasowania |

Jeśli zmienisz wyrażenie następująco,

[Format] .REG. \b\d{3}\x20\d{2}\x20\d{4}\b

to nowe wyrażenie pasować będzie do następującej sekwencji:

333 22 4444

# Listy wyłączeń ze skanowania

## Listy wyłączeń ze skanowania dla programów Security Agent

Ta lista wyłączeń obejmuje wszystkie produkty Trend Micro, które są domyślnie wykluczone ze skanowania.

**TABELA D-9. Lista wyłączeń programu Security Agent**

| NAZWA PRODUKTU | LOKALIZACJA ŚCIEŻKI INSTALACJI |
|---|---|
| InterScan eManager 3.5x | `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan eManager\CurrentVersion`<br><br>`ProgramDirectory=` |
| ScanMail eManager (ScanMail for Microsoft Exchange eManager) 3.11, 5.1, 5.11, 5.12 | `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange eManager\CurrentVersion`<br><br>`ProgramDirectory=` |

| Nazwa produktu | Lokalizacja ścieżki instalacji |
|---|---|
| ScanMail for Lotus Notes (SMLN) eManager NT | HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Lotus Notes\CurrentVersion<br><br>AppDir=<br><br>DataDir=<br><br>IniDir= |
| InterScan Web Security Suite (IWSS) | HKEY_LOCAL_MACHINE\Software\TrendMicro\Interscan Web Security Suite<br><br>Program Directory= C:\Program Files\Trend Micro\IWSS |
| InterScan WebProtect | HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\InterScan WebProtect\CurrentVersion<br><br>ProgramDirectory= |
| InterScan FTP VirusWall | HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan FTP VirusWall\CurrentVersion<br><br>ProgramDirectory= |
| InterScan Web VirusWall | HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan Web VirusWall\CurrentVersion<br><br>ProgramDirectory= |
| InterScan E-Mail VirusWall | HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall\CurrentVersion<br><br>ProgramDirectory={Installation Drive}:\INTERS~1 |
| Dodatek InterScan NSAPI | HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan NSAPI Plug-In\CurrentVersion<br><br>ProgramDirectory= |
| InterScan E-Mail VirusWall | HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall \CurrentVersion<br><br>ProgramDirectory= |

| NAZWA PRODUKTU | LOKALIZACJA ŚCIEŻKI INSTALACJI |
|---|---|
| IM Security (IMS) | HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IM Security \CurrentVersion<br><br>HomeDir=<br><br>VSQuarantineDir=<br><br>VSBackupDir=<br><br>FBArchiveDir=<br><br>FTCFArchiveDir= |

| Nazwa produktu | Lokalizacja ścieżki instalacji |
|---|---|
| ScanMail for Microsoft Exchange (SMEX) | HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion<br><br>TempDir=<br><br>DebugDir=<br><br><br>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption<br><br>BackupDir=<br><br>MoveToQuarantineDir=<br><br><br>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption\Advance<br><br>QuarantineFolder=<br><br><br>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption<br><br>BackupDir=<br><br>MoveToQuarantineDir=<br><br><br>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption \Advance<br><br>QuarantineFolder= |

| NAZWA PRODUKTU | LOKALIZACJA ŚCIEŻKI INSTALACJI |
|---|---|
| ScanMail for Microsoft Exchange (SMEX) | HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\ManualScan\ScanOption<br><br>BackupDir=<br><br>MoveToQuarantineDir=<br><br>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\QuarantineManager<br><br>QMDir=<br><br>Pobierz ścieżkę do pliku exclusion.txt z lokalizacji HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion\HomeDir<br><br>Przejdź do ścieżki (na przykład C:\Program Files \Trend Micro\Messaging Security Agent\)<br><br>Otwórz plik exclusion.txt<br><br>C:\Program Files\Trend Micro\Messaging Security Agent\Temp\<br><br>C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\<br><br>C:\Program Files\Trend Micro\Messaging Security Agent\storage\backup\<br><br>C:\Program Files\Trend Micro\Messaging Security Agent\storage\archive\<br><br>C:\Program Files\Trend Micro\Messaging Security Agent\SharedResPool |

### Listy wyłączeń skanowania dla programu Messaging Security Agent (tylko w wersji Advanced)

Jeśli program Messaging Security Agent jest zainstalowany na serwerze Microsoft Exchange (2000 lub nowszym), domyślnie nie będą skanowane bazy danych i pliki

dziennika serwera Microsoft Exchange ani foldery serwera wirtualnego lub dysku M. Lista wykluczeń jest zapisywana w:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp
\CurrentVersion\Misc.

ExcludeExchangeStoreFiles=C:\Program Files\Exchsrvr\mdbdata\

priv1.stm|C:\Program Files\Exchsrvr\mdbdata\

priv1.edb|C:\Program Files\Exchsrvr\mdbdata\

pub1.stm|C:\Program Files\Exchsrvr\mdbdata\pub1.edb

ExcludeExchangeStoreFolders=C:\Program Files\Exchsrvr\mdbdata\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\Queue\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\PickUp\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\BadMail\
```

Inne zalecane foldery Microsoft Exchange należy dodać ręcznie do listy wykluczeń ze skanowania. Patrz http://support.microsoft.com/kb/245822/.

### Wyłączenia w środowisku SBS 2003

W środowisku SBS 2003 należy dodać ręcznie następujące pozycje:

| Wyłączenia programu Microsoft Exchange | |
|---|---|
| Baza danych programu Microsoft Exchange Server | `C:\Program Files\Exchsrvr\MDBDATA` |
| Pliki MTA programu Microsoft Exchange | `C:\Program Files\Exchsrvr\Mtadata` |
| Pliki dziennika śledzenia wiadomości programu Microsoft Exchange | `C:\Program Files\Exchsrvr\server_name.log` |
| Katalog główny poczty SMTP programu Microsoft Exchange | `C:\Program Files\Exchsrvr\Mailroot` |

| | |
|---|---|
| Pliki robocze programu Microsoft Exchange | `C:\Program Files\Exchsrvr\MDBDATA` |
| Usługa replikacji witryn | `C:\Program Files\Exchsrvr\srsdata`<br>`C:\Program Files\Exchsrvr\conndata` |
| | |
| **Wykluczenia programu IIS** | |
| Pliki systemowe programu IIS | `C:\WINDOWS\system32\inetsrv` |
| Folder kompresji programu IIS | `C:\WINDOWS\IIS Temporary Compressed Files` |
| | |
| **Wykluczenia kontrolera domeny** | |
| Pliki bazy danych usługi Active Directory | `C:\WINDOWS\NTDS` |
| Wolumin systemowy | `C:\WINDOWS\SYSVOL` |
| Pliki bazy danych NTFRS | `C:\WINDOWS\ntfrs` |
| | |
| **Wykluczenia programu Windows SharePoint Services** | |
| Folder tymczasowy środowiska SharePoint | `C:\windows\temp\FrontPageTempDir` |
| | |
| **Wykluczenia folderów komputera klienckiego** | |
| Magazyn usługi Windows Update | `C:\WINDOWS\SoftwareDistribution\DataStore` |
| | |
| **Dodatkowe wykluczenia** | |

| | |
|---|---|
| Baza danych magazynu wymiennego (używana przez mechanizm wykonywania kopii zapasowej w środowisku SBS) | `C:\Windows\system32\NtmsData` |
| Łącznik niedostarczonej poczty w protokole POP3 SBS | `C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Failed Mail` |
| Łącznik poczty przychodzącej w protokole POP3 SBS | `C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Incoming Mail` |
| Magazyn usługi Windows Update | `C:\WINDOWS\SoftwareDistribution\DataStore` |
| Magazyn bazy danych serwera DHCP | `C:\WINDOWS\system32\dhcp` |
| Magazyn bazy danych serwera WINS | `C:\WINDOWS\system32\wins` |

# 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.

# Porty trojanów

Porty trojanów są często używane przez programy typu „koń trojański" w celu połączenia się z urządzeniem typu klienty. W przypadku epidemii program Worry-Free Business Security blokuje następujące numery portów, z którym mogą korzystać konie trojańskie.

**TABELA D-10. 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 |
| 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 |

| Numer portu | Program typu koń trojański | Numer portu | Program typu koń trojański |
|---|---|---|---|
| 7300 | Net Spy | 1234 | Valvo line |

# Pliki, których nie można wyczyścić

Silnik skanowania antywirusowego nie czyści następujących plików:

**Tabela D-11. 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.<br><br>Rozwiązanie: Silnik usług Damage Cleanup i szablon usług Damage Cleanup 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 klient. Rozpowszechnianie zazwyczaj ma miejsce przez połączenia sieciowe lub przez załączniki wiadomości e-mail. Robaków nie można wyczyścić, ponieważ ich pliki są samodzielnymi programami.<br><br>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. |

| Pliki, których nie można wyczyścić | Wyjaśnienie i rozwiązanie |
|---|---|
| | 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.<br><br>Rozwiązanie: Jeśli program pomyślnie wyczyści zarażony plik, zachowanie kopii zapasowej nie jest konieczne. Jeżeli urządzenie typu klient działa prawidłowo, kopię zapasową można usunąć. |
| Zarażone pliki w Koszu | System może nie zezwalać na usunięcie zarażonych plików z Kosza, ponieważ system jest uruchomiony.<br><br>Rozwiązanie:<br><br>1. Uruchom ponownie urządzenie typu klient w trybie MS-DOS.<br><br>2. Otwórz wiersz polecenia.<br><br>3. Wpisz następujące polecenia w celu usunięcia tych plików:<br><br>`cd \`<br><br>`cd recycled`<br><br>`del *.* /S`<br><br>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 klient z nich korzysta. Pliki do wyczyszczenia mogą być plikami tymczasowymi potrzebnymi do działania systemu Windows.<br><br>Rozwiązanie:<br><br>1. Uruchom ponownie urządzenie typu klient w trybie MS-DOS.<br><br>2. Jeśli zarażony plik znajduje się w folderze Temp systemu Windows: |

| Pliki, których nie można wyczyścić | Wyjaśnienie i rozwiązanie |
|---|---|
| | a. Otwórz wiersz polecenia i przejdź do folderu plików tymczasowych systemu Windows (domyślna ścieżka to `C:\Windows\Temp`).<br>b. Wpisz następujące polecenia w celu usunięcia tych plików:<br>`cd temp`<br>`attrib -h`<br>`del *.* /S`<br>Ostatnie polecenie usuwa wszystkie pliki z folderu Temp systemu Windows.<br>c. Ponownie uruchom urządzenie typu klient w zwykłym trybie.<br>3. Jeśli zarażony plik znajduje się w folderze plików tymczasowych programu Internet Explorer:<br>a. Otwórz wiersz polecenia i przejdź do folderu plików tymczasowych programu Internet Explorer (domyślna ścieżka to `C:\Użytkownicy\<Twoja nazwa użytkownika>\AppData\Local\Microsoft\Windows\Temporary Internet Files`).<br>b. Wpisz następujące polecenia w celu usunięcia tych plików:<br>`cd tempor~1`<br>`attrib -h`<br>`del *.* /S`<br>Ostatnie polecenie usuwa wszystkie pliki z folderu plików tymczasowych programu Internet Explorer.<br>c. Ponownie uruchom urządzenie typu klient w zwykłym trybie. |
| Pliki skompresowane za | Rozwiązanie: rozpakuj pliki. |

| Pliki, których nie można wyczyścić | Wyjaśnienie i rozwiązanie |
|---|---|
| pomocą nieobsługiwanego formatu kompresji. | |
| Pliki zablokowane lub pliki, które są obecnie uruchomione. | Rozwiązanie: odblokuj pliki lub poczekaj, aż ich wykonywanie się zakończy. |
| Uszkodzone pliki | Rozwiązanie: usuń pliki. |

# Indeks


**A**

ActiveAction, 7-17
Agent aktualizacji, 3-5
aktualizacja serwera
    aktualizacja ręczna, 8-15
    duplikacja składników, 8-13
    zaplanowana aktualizacja, 8-16
Atak Ping of Death, D-4
Atak typu LAND, D-5
Atak typu SYN flood, D-4
Atak typu Teardrop, D-5
AutoPcc.exe, 3-8, 3-9, 3-13, 3-14

**C**

Client Packager, 3-9, 3-15, 3-17
    ustawienia, 3-16
    wdrażanie, 3-18

**D**

dezinstalacja
    używanie programu dezinstalacji klienta, 3-43
dokumentacja, xiv
duplikacja składników, 8-13

**E**

Encyklopedia wirusów, 1-10

**F**

file reputation, 1-5

**G**

Główna usługa monitorowania zachowania, 8-10

**I**

IDS, D-3
instalacja klienta
    Client Packager, 3-15
    Ustawienia skryptu logowania, 3-13
    używanie narzędzia Vulnerability Scanner, 3-22
Instalacja programu Security Agent
    z konsoli Web, 3-19
instalacja zdalna, 3-9

**K**

katalog kwarantanny, 5-18, 14-19
konsola internetowa, 2-4, 2-5
    informacje, 2-4
    wymagania, 2-5

**M**

Mechanizm obsługi zapytań analizy kontekstowej, 8-8
Menedżer dodatków, 3-5
metoda skanowania, 3-16
Metody instalacji programu Security Agent, 3-7
Możliwy wirus/złośliwe oprogramowanie, 1-10

**N**

Nakładające się fragmenty, D-4
narzędzie do kompresji, 1-11
Niewielki fragment, D-5
nowe funkcje, 1-2

**O**

Obsługa IPv6, B-2
    ograniczenia, B-3, B-4
    wyświetlanie adresów IPv6, B-7

ochrona urządzeń zewnętrznych, 8-10
Ogólna sygnatura zapory, 8-9
operacje skanowania
    spyware/grayware, 7-16
opinie o dokumentacji, C-6

**P**

pakiety hot fix, 8-11
plik testowy EICAR, 1-11
Pofragmentowany IGMP, D-5
pomoc
    szybsze rozwiązywanie problemów, C-4
poprawki, 8-11
poprawki zabezpieczeń, 8-11
programy, 8-4
Programy typu „koń trojański”, 1-10, 8-7
Program-żart, 1-10
przyrostowe wzorce sygnatur, 8-13

**R**

Robak, 1-11

**S**

Silnik analizy kontekstowej, 8-8
Silnik skanowania antywirusowego, 8-6
Silnik skanowania spyware/grayware, 8-9
Silnik skanowania w poszukiwaniu zagrożeń zaawansowanych, 8-8
Silnik usługi Usuwania Szkód, 8-7
Skanowanie standardowe, 5-4, 5-5
skanowanie w poszukiwaniu spyware/grayware
    operacje, 7-16
składniki, 8-4
Skonfliktowane ARP, D-4
smart protection, 1-4, 1-5
    Smart Protection Network, 1-4
Smart Protection
    Usługi File Reputation Services, 1-5
    Usługi Web Reputation Services, 1-5
Smart Protection Network, 1-4
smart scan, 5-4, 5-5
spyware/grayware, 1-12, 1-13
    adware, 1-12
    aplikacje do łamania haseł, 1-13
    dialery, 1-12
    narzędzia hakerskie, 1-12
    narzędzie dostępu zdalnego, 1-13
    programy-żarty, 1-12
    spyware, 1-12
Sterownik funkcji monitorowania zachowania, 8-10
Sterownik wczesnego czystego rozruchu, 8-9
strona instalacyjna w sieci Web, 3-7, 3-8
Sygnatura analizy kontekstowej, 8-8
Sygnatura IntelliTrap, 8-5
Sygnatura konfiguracji monitorowania zachowania, 8-10
Sygnatura monitorowania inspekcji programów, 8-11
Sygnatura naprawiania uszkodzeń, 8-10
Sygnatura niedopuszczenia do wykorzystania luki w przeglądarce, 8-11
Sygnatura oprogramowania spyware/grayware, 8-9
Sygnatura podpisu cyfrowego, 8-10
Sygnatura stosowania zasad, 8-11
Sygnatura wirusa, 8-5
Sygnatura wirusów, 8-17
Sygnatura wyjątków IntelliTrap, 8-5
Sygnatura wykrywania monitorowania zachowania, 8-10
System wykrywania włamań (IDS), D-3

Szablon usługi Usuwania Szkód, 8-7
Szyfrowane pliki, 14-18

## T

typy skanowania, 3-4

## U

Ujednolicona sygnatura analizatora skryptów, 8-11
Usługa Web Reputation, 1-5, 3-4, 5-2
Usługi Damage Cleanup Services, 3-4
Ustawienia DHCP, 3-26
Ustawienia skryptu logowania, 3-8, 3-9, 3-13, 3-14

## V

Vulnerability Scanner, 3-10, 3-22
    pobieranie opisu komputera, 3-32
    Ustawienia DHCP, 3-26
    ustawienia polecenia ping, 3-33

## W

WFBS
    dokumentacja, xiv
wirus HTML, 1-11
wirus JavaScript, 1-11
Wirus sektora rozruchowego, 1-11
wirus sieciowy, 5-29
Wirus testowy, 1-11
wirus VBScript, 1-11
Wirusy/złośliwe oprogramowanie, 1-10, 1-11
    Możliwy wirus/złośliwe oprogramowanie, 1-10
    narzędzie do kompresji, 1-11
    Programy typu „koń trojański”, 1-10
    Program-żart, 1-10
    Robak, 1-11
    typy, 1-10, 1-11
    Wirus sektora rozruchowego, 1-11
    Wirus testowy, 1-11
    Wirus VBScript, JavaScript lub HTML, 1-11
    Wirusy makr, 1-11
    Zarażający plik COM i EXE, 1-11
    złośliwy kod Java, 1-11
    Złośliwy kod w formancie ActiveX, 1-11
Wirusy makr, 1-11
wstępne czynności instalacyjne, 3-11, 3-19, 3-23
wykrywanie rootkitów, 8-10
Wzorzec korelacji zagrożeń zaawansowanych, 8-8

## Z

zagrożenia bezpieczeństwa, 1-12, 1-13
    spyware/grayware, 1-12, 1-13
zapora
    korzyści, 5-29
zarażający plik COM, 1-11
zarażający plik EXE, 1-11
zasady bezpieczeństwa
    złożoność hasła
        wymagania, 6-60
Zbyt duży fragment, D-4
złośliwy kod Java, 1-11
Złośliwy kod w formancie ActiveX, 1-11
złożoność hasła, 6-60

**TREND MICRO INCORPORATED**

Trend 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  info@trendmicro.com

www.trendmicro.com

Item Code: WFPM108197/180326