TREND MICRO

10.0

Worry-Free™ Business Security Standard- und Advanced-Versionen

Service Pack 1

Administratorhandbuch

Securing Your Journey to the Cloud

Protected Cloud

Web Security

Trend Micro Incorporated behält sich das Recht vor, Änderungen an diesem Dokument und den hierin beschriebenen Produkt ohne Vorankündigung vorzunehmen. Lesen Sie vor der Installation und Verwendung von Produkt die Readme-Dateien, die Anmerkungen zu dieser Version und/oder die neueste Version der auf der Trend Micro Website verfügbaren Dokumentation durch:

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

Trend Micro, das Trend Micro T-Ball-Logo, TrendProtect, TrendSecure, Worry-Free, OfficeScan, ServerProtect, PC-cillin, InterScan und ScanMail sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Produkt- oder Firmennamen können Marken oder eingetragene Marken ihrer Eigentümer sein.

Copyright © 2019. Trend Micro Incorporated. Alle Rechte vorbehalten.

Dokument-Nr.: WFEM108677/190617

Release-Datum: Juni 2019

Geschützt durch U.S. Patent-Nr.: 5.951.698 und 7.188.369

Diese Dokumentation enthält eine Beschreibung der wesentlichen Funktionen von Produkt und/oder Installationsanweisungen für eine Produktionsumgebung. Lesen Sie die Dokumentation vor der Installation und Verwendung von Produkt.

Detaillierte Informationen zur Verwendung bestimmter Funktionen in Produkt können Sie in der Trend Micro Online-Hilfe und/oder der Trend Micro Knowledge Base finden.

Trend Micro ist stets bemüht, die Dokumentation zu verbessern. Setzen Sie sich mit uns in Verbindung, wenn Sie Fragen, Kommentare oder Vorschläge zu diesem oder einem anderen Trend Micro Dokument haben: docs@trendmicro.com.

Bewerten Sie diese Dokumentation auf der folgenden Website:

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

Inhaltsverzeichnis

Vorwort

Vorwort xiii
Worry-Free Business Security Dokumentation xiv
Zielpublikum xiv
Textkonventionen xv

Kapitel 1: Einführung in Worry-Free Business Security Standard und Advanced

Übersicht über Trend Micro Worry-Free Business Security ... 1-2
Was ist neu in dieser Version? 1-2
Wichtigste Funktionen und Vorteile 1-3
- Trend Micro Smart Protection Network 1-3
- File-Reputation-Dienste 1-4
- Web Reputation-Dienste 1-4
- Email Reputation (nur Advanced) 1-5
- Smart Feedback 1-6
- URL-Filter 1-7

Vorteile des Schutzes 1-7
Bedrohungen verstehen 1-8
- Viren und Malware 1-9
- Spyware und Grayware 1-11
- Spam 1-12
- Eindringversuche 1-12
- Bösartiges Verhalten 1-12
- Unseriöse Zugangspunkte 1-13
- Phishing-Vorfälle 1-13
- Massenmail-Angriffe 1-14
- Webbedrohungen 1-14

Kapitel 2: Erste Schritte

Das Worry-Free Business Security Netzwerk 2-2

Security Server 2-2
Suchserver 2-2

Agents 2-4

Webkonsole 2-4
Die Webkonsole öffnen 2-5
Navigation auf der Webkonsole 2-9
Symbole auf der Webkonsole 2-11

Kapitel 3: Agents installieren

Security Agent-Installation 3-2
Voraussetzungen für die Installation des Security Agents 3-2
Überlegungen zur Installation des Security Agents 3-2
Verfügbare Security Agent Funktionen 3-3
Installation des Security Agents und IPv6-Unterstützung . 3-5

Installationsmethoden für den Security Agent 3-7
Installation über die interne Webseite 3-9
Mit dem Anmeldeskript-Setup installieren 3-12
Mit Client Packager installieren 3-14
Mit Remote-Installation installieren 3-18
Mit dem Vulnerability Scanner installieren 3-22
Per E-Mail-Benachrichtigung installieren 3-33
Migration zum Security Agent 3-34
Aufgaben nach der Installation auf Security Agents durchführen 3-35

Messaging Security Agent - Installation 3-37
Voraussetzungen für die Installation des Messaging Security Agents 3-38
Messaging Security Agent installieren (nur Advanced) .. 3-38

Agents entfernen 3-40
Agents aus der Webkonsole entfernen 3-41
Agents über die Webkonsole deinstallieren 3-42

Security Agent von Endpunkt deinstallieren 3-43
Messaging Security Agent vom Microsoft Exchange Server deinstallieren (nur Advanced) 3-44

Kapitel 4: Geräte verwalten

Gerätestruktur verwenden 4-2

Gerätebefehle verwenden 4-5

Agents zu Gruppen hinzufügen 4-7

Gruppen hinzufügen 4-9

Spalten der Geräteliste anpassen 4-9

Agents verschieben 4-12
Security Agents zwischen Gruppen verschieben 4-14
Agents mit der Webkonsole zwischen Security Servern verschieben 4-14
Einen Security Agent mit Client Mover zwischen Security Servern verschieben 4-16

Einstellungen replizieren 4-18
Gruppeneinstellungen von Security Agents replizieren . 4-18
Messaging Security Agent-Einstellungen replizieren (nur Advanced) 4-18

Einstellungen von Security Agent Gruppen importieren und exportieren 4-19
Einstellungen exportieren 4-21
Einstellungen importieren 4-21

Kapitel 5: Grundlegende Sicherheitseinstellungen für Security Agents verwalten

Zusammenfassung der grundlegenden Sicherheitseinstellungen für Security Agents 5-2

Suchmethoden 5-3
Suchmethoden konfigurieren 5-5

Echtzeitsuche für Security Agents 5-7
Echtzeitsuche für Security Agents konfigurieren 5-7

Vorausschauendes Maschinenlernen 5-8
Vorausschauendes Maschinenlernen konfigurieren 5-10
Verhaltensüberwachung 5-11
Verhaltensüberwachung konfigurieren 5-12
Vertrauenswürdiges Programm 5-17
Vertrauenswürdiges Programm konfigurieren 5-17
Quarantäne-Ordner 5-18
Den Quarantäne-Ordner konfigurieren 5-22
Web Reputation 5-22
Web Reputation für Security Agents konfigurieren 5-24
URL-Filter 5-25
URL-Filter konfigurieren 5-25
Zulässige/gesperrte URLs 5-27
Zulässige/gesperrte URLs konfigurieren 5-27
Firewall 5-28
Die Firewall konfigurieren 5-31
Mit Firewall-Ausnahmen arbeiten 5-33
Firewall in einer Agents-Gruppe deaktivieren 5-35
Firewall für alle Agents deaktivieren 5-36
Gerätesteuerung 5-36
Gerätesteuerung konfigurieren 5-37
Benutzer-Tools 5-39
Benutzer-Tools konfigurieren 5-40
Agent-Berechtigungen 5-40
Agent-Berechtigungen konfigurieren 5-41

Kapitel 6: Die grundlegenden Sicherheitseinstellungen für Messaging Security Agents (nur Advanced) verwalten

Messaging Security Agents 6-2
So durchsucht der Messaging Security Agent E-Mails 6-3
Standardeinstellungen des Messaging Security Agents 6-4

Echtzeitsuche für Messaging Security Agents 6-5
Die Echtzeitsuche für Messaging Security Agents konfigurieren 6-6

Anti-Spam 6-6
Email Reputation 6-8
Content-Suche 6-10

Content-Filter 6-16
Content-Filter-Regeln verwalten 6-17
Arten von Content-Filter-Regeln 6-21
Content-Filter-Regel für alle Übereinstimmungskriterien hinzufügen 6-22
Content-Filter-Regel für ein beliebiges Übereinstimmungskriterium hinzufügen 6-25
Content-Filter-Überwachungsregel hinzufügen 6-28
Ausnahmen für Content-Filter-Regeln erstellen 6-32

Prävention vor Datenverlust 6-33
Vorbereitung 6-34
Regeln zur Prävention vor Datenverlust verwalten 6-34
Standardregeln der Funktion Prävention vor Datenverlust 6-42
Regeln zur Prävention vor Datenverlust hinzufügen 6-43

Sperren von Anhängen 6-49
Das Sperren von Anhängen konfigurieren 6-50

Web Reputation 6-53
Web Reputation für Messaging Security Agents konfigurieren 6-55

Mobile Security 6-57
Mobile Security-Unterstützung 6-58
Gerätezugriffssteuerung konfigurieren 6-59
Eine ausstehende Gerätezurücksetzung abbrechen 6-60
Geräte manuell zurücksetzen 6-60
Sicherheitsrichtlinien konfigurieren 6-61

Quarantäne für Messaging Security Agents 6-67
Quarantäne-Verzeichnisse abfragen 6-69
Abfrageergebnisse anzeigen und Aktionen ausführen ... 6-70

Quarantäne-Verzeichnisse warten 6-72
Quarantäne-Ordner konfigurieren 6-73

Einstellungen für die Benachrichtigung für Messaging Security Agents 6-74
Einstellungen für die Benachrichtigung für Messaging Security Agents konfigurieren 6-76

Spam-Wartung konfigurieren 6-77
Das Tool End User Quarantine verwalten 6-78

Trend Micro Support und Fehlerbehebung 6-80
Berichte des System-Debuggers erstellen 6-81

Echtzeitmonitor 6-82
Mit dem Echtzeitmonitor arbeiten 6-82

Einen Disclaimer zu ausgehenden E-Mail-Nachrichten hinzufügen 6-83

Kapitel 7: Suche verwalten

Info über Suchtypen 7-2

Echtzeitsuche 7-3

Manuelle Suche 7-3
Manuelle Suche durchführen 7-4

Zeitgesteuerte Suche 7-7
Zeitgesteuerte Suchen konfigurieren 7-7

Suchziele und Aktionen für Security Agents 7-10

Suchziele und Aktionen für Messaging Security Agents 7-18

Kapitel 8: Updates verwalten

Update-Übersicht 8-2

Update-Komponenten 8-4
Info über Hotfixes, Patches und Service Packs 8-10

Security Server-Updates 8-11
Die Update-Adresse des Security Servers konfigurieren . 8-13
Den Security Server manuell aktualisieren 8-14

Zeitgesteuerte Updates für den Security Server konfigurieren 8-15
Rollback für Komponenten durchführen 8-16
Updates für Security Agent und Messaging Security Agent ... 8-17
Automatische Updates 8-17
Manuelles Update ausführen 8-18
Hinweise und Empfehlungen zu Agent-Updates 8-19
Update Agents 8-19
Update Agents konfigurieren 8-22

Kapitel 9: Live-Status verwenden

Live-Status 9-2
Aktionszentrum 9-3
Erkennung von Sicherheitsrisiken im Zeitverlauf 9-8
Ransomware-Übersicht 9-18
Lizenzstatus 9-22
Übersicht zu Exchange Server 9-22
Agent-Status 9-23

Kapitel 10: Benachrichtigungen verwalten

Benachrichtigungen verwenden 10-2
Ereignisse für Benachrichtigungen konfigurieren 10-4
Token-Variablen 10-6

Kapitel 11: Allgemeine Einstellungen verwalten

Allgemeine Einstellungen 11-2
Internet-Proxy-Einstellungen konfigurieren 11-3
Einstellungen des SMTP-Servers konfigurieren 11-4
Desktop-/Server-Einstellungen konfigurieren 11-5
Systemeinstellungen konfigurieren 11-10
Einstellungen für die Ausnahmeliste konfigurieren 11-14

Kapitel 12: Protokolle und Berichte verwenden

Protokolle 12-2
Protokollabfrage verwenden 12-4
Berichte 12-5
Mit Einzelberichten arbeiten 12-6
Mit zeitgesteuerten Berichten arbeiten 12-7
Berichte interpretieren 12-11
Wartungsaufgaben für Berichte und Protokolle durchführen 12-14

Kapitel 13: Administrative Aufgaben durchführen

Das Kennwort der Web-Konsole ändern 13-2
Mit dem Plug-in Manager arbeiten 13-2
Produktlizenz verwalten 13-3
Einstellungen zu Produkt-Updates konfigurieren 13-5
Konfigurieren von Benachrichtigungen über Produkt-Updates 13-6
Am Smart Feedback Programm teilnehmen 13-7
Sprache der Benutzeroberfläche des Agents ändern 13-8
Programmeinstellungen speichern und wiederherstellen 13-8
Den Security Server deinstallieren 13-10

Kapitel 14: Management-Tools verwenden

Tool-Typen 14-2
Trend Micro Remote Manager Agent 14-4
Den Trend Micro Remote Manager Agent installieren (Customer Licensing Portal Benutzer) 14-4
Den Trend Micro Remote Manager Agent installieren (Licensing Management Platform Benutzer) 14-6
Agents über den verwalteten Server verwalten 14-8
Agent-Einstellungen sichern und wiederherstellen 14-12

Festplattenspeicher sparen 14-15
Disk Cleaner auf dem Security Server ausführen 14-15
Disk Cleaner auf dem Security Server mit der Befehlszeilenschnittstelle ausführen 14-16
Festplattenspeicher auf Clients sparen 14-17

Die Scan Server Datenbank verschieben 14-18

Verschlüsselte Dateien wiederherstellen 14-18
Dateien entschlüsseln und auf dem Security Agent wiederherstellen 14-20
Dateien auf dem Security Server, in einem benutzerdefinierten Quarantäne-Verzeichnis oder Messaging Security Agent entschlüsseln und wiederherstellen 14-21
TNEF-Nachrichten (Transport Neutral Encapsulation Format) wiederherstellen 14-23

ReGenID Tool verwenden 14-23

SBS und EBS Add-ins verwalten 14-24
SBS und EBS Add-ins manuell installieren 14-24
SBS oder EBS Add-ins verwenden 14-25

Anhang A: Symbole für Security Agent

Status des Security Agents prüfen A-2

Security Agent-Symbole in der Windows Task-Leiste anzeigen A-4

Auf den Flyover-Bereich der Konsole zugreifen A-5

Anhang B: IPv6-Unterstützung in Worry-Free Business Security

IPv6-Unterstützung für Worry-Free Business Security und Security Agents B-2
IPv6-Voraussetzungen für den Security Server B-2
Voraussetzungen für den Messaging Security Agent B-3
Einschränkungen bei reinen IPv6-Servern B-3
Einschränkungen bei reinen IPv6-Security Agents B-4

IPv6-Adressen konfigurieren B-5

Fenster, auf denen IP-Adressen angezeigt werden B-6

Anhang C: Technischer Support

Ressourcen zur Fehlerbehebung C-2
Support-Portal verwenden C-2
Bedrohungsenzyklopädie C-3

Kontaktaufnahme mit Trend Micro C-3
Problemlösung beschleunigen C-4

Verdächtige Inhalte an Trend Micro senden C-5
Email Reputation Services C-5
File-Reputation-Dienste C-5
Web Reputation-Dienste C-5

Sonstige Ressourcen C-6
Download Center C-6
Anregungen und Kritik C-6

Anhang D: Produktterminologie und Konzepte

Kritischer Patch D-2

Hotfix D-2

IntelliScan D-2

IntelliTrap D-3

Intrusion Detection System D-3

Schlüsselwörter D-5

Patch D-9

Reguläre Ausdrücke D-10

Ausschlussliste für Virensuche D-19

Service Pack D-26

Trojanerports D-26

Dateien, die nicht gesäubert werden können D-27

Stichwortverzeichnis

Stichwortverzeichnis IN-1

Vorwort

Vorwort

Willkommen beim *Administratorhandbuch* von Trend Micro™ Worry-Free™ Business Security. In diesem Dokument finden Sie Informationen über die ersten Schritte, die Verfahren zur Agent-Installation sowie die Verwaltung des Security Servers und die Agent-Verwaltung.

Worry-Free Business Security Dokumentation

Die Worry-Free Business Security Dokumentation umfasst folgende Komponenten:

Tabelle 1. Worry-Free Business Security Dokumentation

Dokumentation	Beschreibung
Installations- und Upgrade-Handbuch	Ein PDF-Dokument, in dem Anforderungen und Verfahren zum Installieren des Security Servers sowie zum Upgrade des Servers und der Agents beschrieben werden
Administratorhandbuch	Ein PDF-Dokument mit folgenden Inhalten: Informationen über die ersten Schritte, Verfahren zur Client-Installation sowie Security Server- und Client-Verwaltung
Hilfe	Im WebHelp- oder CHM-Format erstellte HTML-Dateien, die Anleitungen, allgemeine Benutzerhinweise und feldspezifische Informationen enthalten.
Readme-Datei	Enthält eine Liste bekannter Probleme und grundlegende Installationshinweise. Die Datei kann auch neueste Produktinformationen enthalten, die noch nicht in der Hilfe oder in gedruckter Form zur Verfügung stehen.
Knowledge Base	Eine Online-Datenbank mit Informationen zur Problemlösung und Fehlerbehebung. Sie enthält die aktuellsten Hinweise zu bekannten Softwareproblemen. Die Knowledge Base finden Sie im Internet unter folgender Adresse: http://esupport.trendmicro.com

Die neuesten Versionen der PDF-Dateien und der Readme-Datei können Sie hier herunterladen:

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

Zielpublikum

Die Worry-Free Business Security Dokumentation richtet sich an folgende Benutzer:

- **Security Administratoren**: Für die Verwaltung von Worry-Free Business Security verantwortlich, einschließlich Security Server und Agent Installation und Verwaltung. Es wird davon ausgegangen, dass diese Benutzer über umfassende Kenntnisse über Netzwerke und Server-Verwaltung verfügen.
- **Endbenutzer**: Benutzer, auf deren Computer der Security Agent installiert ist. Die Computerkenntnisse dieser Benutzergruppe reichen vom Anfänger bis zum erfahrenen Anwender.

Textkonventionen

Damit Sie Informationen leicht finden und einordnen können, werden in der Worry-Free Business Security Dokumentation folgende Konventionen verwendet:

Tabelle 2. Textkonventionen

Konvention	Beschreibung
NUR GROSSBUCHSTABEN	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Befehlsschaltflächen, Registerkarten, Optionen und Tasks
Kursivdruck	Referenzen zu anderen Dokumenten oder neuen technischen Komponenten
<Text>	Text in spitzen Klammern soll durch Benutzerangaben ersetzt werden. Beispiel: `C:\Programme\<Dateiname>` kann `C:\Programme\beispiel.jpg` sein.
Hinweis	Enthält Konfigurationshinweise oder -empfehlungen
Tipp	Enthält Angaben zu bewährten Methoden und Trend Micro Empfehlungen

Konvention	Beschreibung
Warnung!	Enthält Warnungen zu Vorgängen, die Computern im Netzwerk schaden können

Kapitel 1

Einführung in Worry-Free™ Business Security Standard und Advanced

In diesem Kapitel erhalten Sie eine Übersicht über Worry-Free Business Security (Worry-Free Business Security).

Übersicht über Trend Micro Worry-Free Business Security

Trend Micro Worry-Free Business Security (Worry-Free Business Security) schützt die Benutzer und Daten kleiner Unternehmen vor Daten- und Identitätsdiebstahl, gefährlichen Websites und Spam (nur Advanced).

In diesem Dokument finden Sie Informationen für Worry-Free Business Security Standard und Advanced. Die nur für Advanced relevanten Abschnitte und Kapitel sind mit '(nur Advanced)' gekennzeichnet.

Mit der Unterstützung des Trend Micro Smart Protection Network ist Worry-Free Business Security:

- **Sicherer**: Die Lösung stoppt Viren, Spyware, Spam (nur Advanced) und Internet-Bedrohungen, bevor sie Ihre Clients erreichen können. URL-Filter sperren den Zugriff auf gefährliche Websites und helfen, die Benutzerproduktivität zu verbessern.
- **Intelligenter**: Schnelle Suchläufe und kontinuierliche Updates bei minimaler Beeinträchtigung der Clients schützen vor neuen Bedrohungen.
- **Einfacher**: Einfache Verteilung und minimale Administration – Worry-Free Business Security erkennt Bedrohungen noch zuverlässiger, damit Sie sich ganz auf Ihre Geschäfte konzentrieren können, statt auf Sicherheit.

Was ist neu in dieser Version?

Die folgende Tabelle zeigt die neuen Funktionen und Verbesserungen in dieser Version von Worry-Free Business Security an.

Funktion/Verbesserung	Beschreibung
Aggressives Durchsuchen	Worry-Free Business Security umfasst nun die Funktion „Aggressives Durchsuchen“ für erweiterte Suche und Bereinigung infizierter Endpunkte. Weitere Informationen finden Sie unter *Gerätestruktur verwenden auf Seite 4-2* und *Gerätebefehle verwenden auf Seite 4-5*.
Verbesserter Schutz vor dateiloser Malware	Worry-Free Business Security verwendet jetzt die neuesten Technologien zum Schutz vor dateiloser Malware, um Ihre Endpunkte vor dateilosen Angriffen zu schützen.
Unterstützung des Betriebssystems	Worry-Free Business Security unterstützt nun die Installation von Security Server und Agent auf den folgenden Betriebssystemen: • Windows 10. Mai 2019 Update • Windows Server 2019

Wichtigste Funktionen und Vorteile

Worry-Free Business Security bietet die folgenden Funktionen und Vorteile:

Trend Micro™ Smart Protection Network™

Das Trend Micro™ Smart Protection Network™ ist eine Content-Sicherheitsinfrastruktur mit webbasiertem Client der nächsten Generation, die zum Schutz der Kunden vor Sicherheitsrisiken und Internet-Bedrohungen entwickelt wurde. Es unterstützt sowohl lokale als auch von Trend Micro gehostete Lösungen, um Benutzer zu schützen, unabhängig davon, ob sie sich im Netzwerk, zu Hause oder unterwegs befinden. Das Smart Protection Network verwendet leichtgewichtige Agents, um auf seine einzigartige, webbasierte Kombination aus E-Mail-, Web- und File-Reputation-Technologien und Bedrohungsdatenbanken zuzugreifen. Der Kundenschutz wird automatisch aktualisiert und verstärkt, während immer mehr Produkte, Dienste und Benutzer auf das Netzwerk zugreifen. Benutzer werden wie in einer wachsamen Nachbarschaft in Echtzeit geschützt.

Weitere Informationen über das Smart Protection Network finden Sie unter:

http://www.trendmicro.de/technologie-innovationen/technologie/smart-protection-network/

File-Reputation-Dienste

File-Reputation-Dienste überprüft die Vertrauenswürdigkeit jeder einzelnen Datei anhand einer umfangreichen Internet-basierten Datenbank. Da Malware-Informationen im Internet gespeichert werden, sind sie sofort für alle Benutzer zugänglich. Leistungsstarke Content-Netzwerke und lokale Cache-Server gewährleisten minimale Latenzzeiten während der Überprüfung. Die webbasierte Client-Architektur bietet sofortigen Schutz und verringert den Aufwand der Pattern-Verteilung und die Client-Beeinträchtigung insgesamt erheblich.

Security Agents müssen sich im Smart Scan Modus befinden, damit File-Reputation-Dienste angewendet werden kann. Diese Agents werden in diesem Dokument als **Smart Scan Agents** bezeichnet. Agents, die sich nicht im Smart Scan Modus befinden, wenden File-Reputation-Dienste nicht an und heißen **Agents zur herkömmlichen Suche** Worry-Free Business Security Administratoren können den Smart Scan Modus für alle oder mehrere Agents konfigurieren.

Web Reputation-Dienste

Die Web Reputation-Technologie von Trend Micro nutzt eine der größten Domänen-Reputationsdatenbanken der Welt und verfolgt die Glaubwürdigkeit von Webdomänen durch die Zuordnung einer Reputationsbewertung auf Grundlage von Faktoren wie beispielsweise dem Alter einer Website, historischer Änderungen des Speicherorts und Anzeichen von verdächtigen Aktivitäten, die von der Malware-Verhaltensanalyse entdeckt wurden. Anschließend durchsucht Web Reputation Websites und hält Benutzer vom Zugriff auf infizierte Websites ab. Die Web Reputation-Funktionen helfen dabei sicherzustellen, dass die Seiten, auf die die Benutzer zugreifen, sicher und frei von Internet-Bedrohungen wie beispielsweise Malware, Spyware und Phishing-

Nachrichten sind, die Benutzer dazu bringen könnten, persönliche Daten preiszugeben. Um die Genauigkeit zu erhöhen und Fehlalarme zu reduzieren, weist die Web Reputation-Technologie von Trend Micro Reputationsbewertungen bestimmten Webseiten oder Links innerhalb von Websites zu. Dabei wird nicht die gesamte Website klassifiziert oder gesperrt, da oft nur Teile einer legitimen Site gehackt wurden. Außerdem können sich Reputationen dynamisch mit der Zeit ändern.

Agents, die den Web Reputation-Richtlinien unterliegen, benutzen Web Reputation-Dienste. Worry-Free Business Security Administratoren können alle oder mehrere Agents den Richtlinien von Web Reputation unterstellen.

Email Reputation (nur Advanced)

Die Email-Reputation-Technologie von Trend Micro validiert IP-Adressen durch den Abgleich mit einer Reputationsdatenbank, die bekannte Spam-Quellen enthält, und verwendet einen dynamischen Dienst, der die Vertrauenswürdigkeit von E-Mail-Absendern in Echtzeit bewerten kann. Die Bewertungen der Vertrauenswürdigkeit werden durch die kontinuierliche Analyse des Verhaltens, des Aktivitätsumfangs und den bisherigen Verlauf einer IP-Adresse noch weiter verfeinert. Bösartige E-Mails werden anhand der Absender-IP-Adresse im Internet gesperrt, so dass Bedrohungen, wie Zombies oder Botnetze, weder in das Netzwerk noch in den Benutzer-PC eindringen können.

Die Email Reputation-Technologie stuft Spam gemäß der Vertrauenswürdigkeit des sendenden MTAs (Mail Transport Agent) ein. und entbindet dadurch den Security Server von dieser Aufgabe. Bei aktivierter Email Reputation wird der gesamte eingehende SMTP-Datenverkehr von den IP-Datenbanken geprüft, um zu ermitteln, ob die sendende IP-Adresse zulässig ist oder als bekannter Spam-Überträger gelistet ist.

Für Email Reputation gibt es zwei Service-Level:

- **Standard**:Der Service-Level Standard verwendet eine Datenbank, die die Vertrauenswürdigkeit von mehr als zwei Milliarden IP-Adressen nachverfolgt. IP-Adressen, die immer wieder mit Spam-Nachrichten in Verbindung gebracht werden, werden in die Datenbank aufgenommen und nur in seltenen Fällen entfernt.

- **Advanced**: Dieser Service-Level basiert auf DNS und Abfragen, ähnlich dem Service-Level Standard. Das wichtigste Element dieses Service ist die Standard-Reputationsdatenbank, die gemeinsam mit der dynamischen Echtzeit-Reputationsdatenbank Nachrichten bekannter und verdächtiger Spam-Quellen sperrt.

Wird eine E-Mail-Nachricht einer gesperrten oder verdächtigen IP-Adresse gefunden, sperrt die Email Reputation Services (ERS) die Nachricht, bevor diese die Nachrichteninfrastrutur erreicht. Sperrt ERS E-Mail-Nachrichten einer IP-Adresse, die Sie als sicher einstufen, fügen Sie diese IP-Adresse zur Liste der zulässigen IP-Adressen hinzu.

Smart Feedback

Trend Micro Smart Feedback bietet eine ständige Kommunikation zwischen Trend Micro Produkten und den rund um die Uhr verfügbaren Bedrohungsforschungszentren und entsprechenden Technologien. Jede neue Bedrohung, die bei einem Kunden während einer routinemäßigen überprüfung der Reputation erkannt wird, führt zu einer automatischen Aktualisierung der Trend Micro Bedrohungsdatenbanken, wodurch diese Bedrohung für nachfolgende Kunden blockiert wird.

Durch die permanente Weiterentwicklung der Bedrohungsabwehr durch die Analyse der über ein globales Netzwerk von Kunden und Partnern gelieferten Informationen bietet Trend Micro automatischen Schutz in Echtzeit vor den neuesten Bedrohungen sowie Sicherheit durch Kooperation ("Better Together"). Das ähnelt einem "Nachbarschaftsschutz", bei dem in einer Gemeinschaft alle Beteiligten aufeinander aufpassen. Da die gesammelten Bedrohungsdaten auf der Reputation der Kommunikationsquelle und nicht auf dem Inhalt der Kommunikation selbst basieren, ist der Datenschutz der persönlichen oder geschäftlichen Daten eines Kunden jederzeit gewährleistet.

Beispiele der Informationen, die an Trend Micro gesendet werden:

- Datei-Prüfsummen
- Websites, auf die zugegriffen wird

- Dateiinformationen, darunter Größe und Pfade
- Namen von ausführbaren Dateien

Sie können Ihre Teilnahme am Programm jederzeit von der Webkonsole aus beenden.

Weitere Informationen finden Sie unter *Am Smart Feedback Programm teilnehmen auf Seite 13-7*.

Tipp

Sie müssen nicht an Smart Feedback teilnehmen, um Ihre Endpoints zu schützen. Ihre Teilnahme ist optional und kann jederzeit deaktiviert werden. Trend Micro empfiehlt die Teilnahme an Smart Feedback, um allen Trend Micro Kunden einen umfassenderen Schutz zu gewährleisten.

Weitere Informationen über das Smart Protection Network finden Sie unter:

http://www.trendmicro.de/technologie-innovationen/technologie/smart-protection-network/

URL-Filter

URL-Filter unterstützen Sie bei der Vergabe von Zugriffsberechtigungen für Websites, um unproduktive Arbeitszeiten zu reduzieren, Internet-Bandbreite zu schonen und eine sichere Internet-Umgebung zu schaffen. Sie können den gewünschten Grad an URL-Filterschutz auswählen oder selbst definieren, welche Arten von Websites Sie anzeigen möchten.

Vorteile des Schutzes

In der nachfolgenden Tabelle wird beschrieben, wie die verschiedenen Komponenten von Worry-Free Business Security Ihren Computer vor Bedrohungen schützen.

TABELLE 1-1. Vorteile des Schutzes

BEDROHUNG	SCHUTZ
Virus/Malware. Viren, Trojaner, Würmer, Backdoor-Programme und Rootkits **Spyware/Grayware**. Spyware, Dialer, Hacker-Tools, Anwendungen zum Entschlüsseln von Kennwörtern, Adware, Scherzprogramme und Keylogger	Dateibasierte Suchen (Echtzeitsuche, manuelle Suche, zeitgesteuerte Suche)
Sicherheitsbedrohungen, die per E-Mail übertragen werden.	**POP3 Mail Scan** im Security Agent
Netzwerkwürmer/Viren und Eindringlinge	Firewall im Security Agent
Möglicherweise bösartige Websites oder Phishing-Sites	Web Reputation und URL-Filter im Security Agent
Sicherheitsbedrohungen, die über USB- und andere externe Geräte verbreitet werden	Gerätesteuerung im Security Agent
Bösartiges Verhalten	Verhaltensüberwachung im Security Agent
Ransomware-Programme, die auf Dokumente abzielen, die auf Endpunkten ausgeführt werden	Verhaltensüberwachung und Vorausschauendes Maschinenlernen im Security Agent

Bedrohungen verstehen

Unternehmen ohne spezielles Sicherheitspersonal sowie mit weniger strengen Sicherheitsrichtlinien sind immer häufiger Bedrohungen ausgesetzt. Das gilt auch, wenn diese Unternehmen über eine Basissicherheitsinfrastruktur verfügen. Wenn diese Bedrohungen entdeckt werden, können sie sich bereits auf viele Computerressourcen ausgeweitet haben, so dass die vollständige Beseitigung einige Zeit dauert und eines beträchtlichen Aufwands bedarf. Unvorhergesehene Kosten für die Beseitigung von Bedrohungen können sich ansammeln.

Trend Micro Netzwerksicherheits- und webbasierte Server, die Teil des Trend Micro Smart Protection Networks sind, erkennen und reagieren auf Bedrohungen der nächsten Generation.

Viren und Malware

Zehntausende von Viren und Malware-Typen sind bereits bekannt, und täglich kommen neue hinzu. Computerviren traten früher vor allem unter DOS oder Windows auf. Heutzutage können Viren verheerenden Schaden anrichten, indem sie die Schwachstellen in Netzwerken, E-Mail-Systemen und Webseiten von Unternehmen ausnutzen.

- **Scherzprogramm**: Virenähnliches Programm, das meist die Anzeige auf dem Computerbildschirm verändert.
- **Mögliche(r) Virus oder Malware**: Verdächtige Dateien, die einige Eigenschaften von Viren/Malware aufweisen. Weitere Informationen finden Sie in der Trend Micro Bedrohungsenzyklopädie:

  http://about-threats.trendmicro.com/threatencyclopedia.aspx
- **Rootkit**: Ein Programm (oder eine Sammlung von Programmen), das Code auf einem System ohne Zustimmung oder Wissen des Endbenutzers installiert und ausführt. Es nutzt die Möglichkeiten des Tarnens, um eine permanente und nicht feststellbare Präsenz auf der Maschine aufrechtzuerhalten. Rootkits infizieren keine Computer, sondern versuchen, eine nicht feststellbare Umgebung für die Ausführung von bösartigem Code bereitzustellen. Rootkits werden auf Systemen über Social Engineering, bei der Ausführung von Malware oder einfach durch das Surfen auf einer bösartigen Website installiert. Einmal installiert, kann ein Angreifer praktisch jede Funktion auf dem System ausführen: Remote-Zugriffe, Abhören und das Verstecken von Prozessen, Dateien, Registrierungsschlüsseln und Kommunikationskanälen.
- **Trojaner**: Diese Art der Bedrohung verwenden oft einen Port, um sich Zugang zu Computern oder ausführbaren Programmen zu verschaffen. Trojaner replizieren sich nicht, sondern nisten sich in einem System ein und lösen unerwünschte Aktionen aus, z. B. indem sie Ports für

Hackerangriffe öffnen. Herkömmliche Antiviren-Software entdeckt und entfernt zwar Viren, aber keine Trojaner. Insbesondere dann nicht, wenn diese bereits aktiv geworden sind.

- **Viren**: Ein Programm, das sich repliziert. Der Virus muss sich dazu an andere Programmdateien anhängen und wird ausgeführt, sobald das Host-Programm ausgeführt wird. Hierzu gehören folgende Typen:
  - **Bösartiger ActiveX-Code**: Code, der sich hinter Webseiten verbirgt, auf denen ActiveX™-Steuerelemente ausgeführt werden.
  - **Bootsektorvirus**: Diese Virenart infiziert den Bootsektor von Partitionen oder Festplatten.
  - **COM- und EXE-Dateiinfektor**: Ausführbares Programm mit der Dateierweiterung `.com` oder `.exe`.
  - **Bösartiger Java-Code**: Virencode, der in Java™ geschrieben oder eingebettet wurde und auf einem beliebigen Betriebssystem ausgeführt werden kann.
  - **Makrovirus**: Diese Virenart ist wie das Makro einer Anwender-Software aufgebaut und verbirgt sich häufig in Dokumenten.
  - **Packer**: Ein komprimiertes und/oder verschlüsseltes ausführbares Windows oder Linux™ Programm; häufig handelt es sich dabei um einen Trojaner. In komprimierter Form ist ein Packer für ein Antiviren-Programm schwieriger zu erkennen.
  - **Testviren**: Eine inaktive Datei, die sich wie ein Virus verhält und von Antiviren-Software erkannt wird. Mit Testviren wie dem EICAR-Testskript können Sie die Funktion Ihrer Antiviren-Software überprüfen.
  - **VBScript**-, **JavaScript**- oder **HTML-Virus**: Ein Virus, der sich auf Websites verbirgt und über einen Browser heruntergeladen wird.
  - **Wurm**: Ein eigenständiges Programm (oder eine Gruppe von Programmen), das funktionsfähige Kopien von sich selbst oder seinen Segmenten an andere Computer (meist per E-Mail) verteilen kann.

- **Andere**: Viren/Malware, die unter keiner der Viren-/Malware-Typen eingestuft wurden.

Spyware und Grayware

Endpunkte werden nicht nur durch Viren oder Malware bedroht. Als Spyware/Grayware werden Anwendungen oder Dateien bezeichnet, die zwar nicht als Viren oder Trojaner eingestuft werden, die Leistung der Clients im Netzwerk jedoch beeinträchtigen und das Unternehmen im Hinblick auf Sicherheit, Geheimhaltung und Haftungsansprüche einem hohen Risiko aussetzen können. Häufig führt Spyware/Grayware eine Vielzahl unerwünschter und bedrohlicher Aktionen durch. Dazu zählen das Öffnen lästiger Popup-Fenster, das Aufzeichnen von Tastatureingaben und das Aufdecken von Sicherheitslücken, durch die der Client angegriffen werden kann.

Senden Sie verdächtige Dateien oder Anwendungen, die Worry-Free Business Security nicht als Grayware erkennen kann, zur Analyse an Trend Micro:

https://success.trendmicro.com/solution/1059565

Typ	Beschreibung
Spyware	Diese Software sammelt Daten, z. B. Benutzernamen und Kennwörter, und leitet sie an Dritte weiter.
Adware	Diese Software blendet Werbebanner ein, zeichnet die Internet-Surf-Gewohnheiten der Benutzer auf und missbraucht die gesammelten Daten, um den Benutzern über einen Browser gezielte Werbung zu senden.
Dialer	Diese Software ändert die Client-Internet-Einstellungen und erzwingt auf dem Client das Wählen von voreingestellten Telefonnummern. Oft handelt es sich um Pay-per-Call oder internationale Rufnummern, die dem Unternehmen beträchtliche Kosten verursachen können.
Scherzprogram m	Diese Software verursacht ungewöhnliches Client-Verhalten, z. B. das Öffnen und Schließen des CD-ROM-Laufwerks oder die Anzeige zahlreicher Nachrichtenfelder.

Typ	Beschreibung
Hacker-Tools	Mit Hilfe solcher Tools verschaffen sich Hacker Zugriff auf Computer.
Tools für den Remote-Zugriff	Mit diesen Tools können Hacker per Fernzugriff in Computer eindringen und sie steuern.
Anwendungen zum Entschlüsseln von Kennwörtern	Hiermit versuchen Hacker, Benutzernamen und Kennwörter zu entschlüsseln.
Andere	Andere Typen potenziell bösartiger Programme.

Spam

Spam besteht aus unerwünschten E-Mails (Junk-Mails), häufig aus Werbemails, die willkürlich an zahlreiche Verteilerlisten, einzelne Personen oder Newsgroups versendet werden. Es gibt zwei Arten von Spam: Unerwünschte Werbe- und unerwünschte Massen-Mails.

Eindringversuche

Eindringversuche bezeichnen den Zugriff auf ein Netzwerk oder Clients ohne (rechtmäßige) Berechtigung. Als Eindringversuch kann auch die Umgehung des Sicherheitssystems eines Netzwerks oder Client bezeichnet werden.

Bösartiges Verhalten

Bösartiges Verhalten bezieht sich auf unbefugte Änderungen durch eine Software, die Betriebssystem, Registrierungseinträge, andere Software oder Dateien und Ordnern modifiziert.

Unseriöse Zugangspunkte

Unseriöse Zugangspunkte, auch bekannt als Evil Twin, sind bösartige WLAN-Zugangspunkte, die sich als rechtmäßige Zugangspunkte tarnen, jedoch durch einen Hacker so konfiguriert wurden, dass die Wireless-Kommunikation ausspioniert werden kann.

Phishing-Vorfälle

Phish oder Phishing ist eine immer häufiger auftretende Betrugsform, bei der Internet-Benutzern durch das Imitieren einer rechtmäßigen Website persönliche Daten entlockt werden sollen.

Ein typisches Beispiel wäre der Fall, in dem ein nichts ahnender Benutzer eine dringend erscheinende (und authentisch aussehende) E-Mail erhält, in der ihm mitgeteilt wird, dass es ein Problem mit seinem Konto gibt, das umgehend behoben werden müsse, da ansonsten das Konto geschlossen werde. Die E-Mail enthält einen Link zu einer täuschend echten Website. Rechtmäßige E-Mails oder Websites können leicht kopiert werden. Es muss darin nur noch der Empfänger der Daten abgeändert werden.

In der E-Mail wird der Benutzer aufgefordert, sich auf der Website anzumelden und einige Kontodaten zu bestätigen. Persönliche Daten, die der Benutzer eingibt, wie Anmeldenamen, Kennwort, Kreditkartennummer, Sozialversicherungsnummer usw., werden dann an einen Hacker weitergeleitet.

Phishing-Mails lassen sich schnell, billig und in großer Zahl umsetzen. Ein Hacker kann mit Phishing-Mails erhebliche finanzielle Gewinne erzielen. Selbst für einen Computerspezialisten sind Phishing-Angriffe nur schwer zu erkennen. Dem Phish-Schreiber rechtlich beizukommen ist ebenfalls nicht einfach, wenn nicht gar unmöglich.

Melden Sie Trend Micro alle Websites, hinter denen Sie Phishing vermuten. Weitere Informationen hierzu finden Sie unter *Verdächtige Inhalte an Trend Micro senden auf Seite C-5*.

Massenmail-Angriffe

E-Mail-basierte Viren und Malware können sich per E-Mail verbreiten, indem sie die infizierten E-Mail-Clients automatisieren oder indem der Virus oder die Malware sich selbst verbreiten. Unter Massenmail-Verhalten versteht man eine Situation, in der sich eine Infektion schnell in einer Microsoft Exchange Umgebung ausbreitet. Die Scan Engine von Trend Micro wurde so konzipiert, dass sie das Verhalten von Massenmail-Angriffen entdeckt. Diese Verhaltensweisen werden in der Viren-Pattern-Datei aufgezeichnet, die über die Trend Micro ActiveUpdate Server aktualisiert wird.

Sie können festlegen, dass der Messaging Security Agent (nur Advanced) bestimmte Aktionen gegen Massenmail-Angriffe durchführt, sobald er einen entsprechenden Hinweis darauf erkennt. Die für das Verhalten bei einem Massenmail-Angriff festgelegte Maßnahme erhält Vorrang vor allen anderen Aktionen. Die Standardaktion bei Massenmail-Angriffen ist "Gesamte Nachricht löschen".

Beispiel: Sie konfigurieren den Messaging Security Agent so, dass Nachrichten, die von einem Trojaner oder einem Wurm infiziert wurden, in Quarantäne verschoben werden. Außerdem aktivieren Sie die Maßnahmen, die bei typischem Massenmail-Verhalten ergriffen werden sollen; der Agent soll Mails mit einem derartigen Verhaltensmuster löschen. Nun empfängt der Agent eine Nachricht, die einen Wurm wie MyDoom enthält. Dieser Wurm verbreitet sich über eine inhärente SMTP-Engine an alle E-Mail-Adressen, die er auf dem infizierten Computer sammelt. Entdeckt der Agent den MyDoom-Wurm und dessen Massenmail-Verhalten, löscht er umgehend diese Mail – entgegen der Quarantäne-Aktion für Würmer ohne Massenmail-Verhalten.

Webbedrohungen

Als Internet-Bedrohungen zählen vielfältige Sicherheitsrisiken, die ihren Ursprung im Internet haben. Sie setzen auf raffinierte Methoden und kombinierte Dateien und Techniken anstelle isolierter Infektionswege. Beispielsweise ändern die Urheber von Internet-Bedrohungen regelmäßig die Version oder die verwendete Variante. Da sich die Internetbedrohung

eher an einem festen Speicherort auf einer Website und nicht auf einem infizierten Client befindet, wird der Code ständig verändert, um einer Entdeckung zu entgehen.

Personen, die in der Vergangenheit als Hacker, Virusautoren, Spammer und Spyware-Hersteller bezeichnet wurden, werden seit einigen Jahren unter der Bezeichnung Cyberkriminelle zusammengefasst. Internet-Bedrohungen helfen diesen Personen eines von zwei Zielen zu verfolgen. Eines dieser Ziele ist es, Informationen zu stehlen, um sie anschließend zu verkaufen. Das Ergebnis ist die Preisgabe vertraulicher Informationen in Form von Identitätsverlust. Infizierte Client können außerdem als Überträger für Phishing-Angriffe eingesetzt oder anderweitig zur Informationsbeschaffung missbraucht werden. Neben weiteren möglichen Auswirkungen birgt diese Bedrohung das Potenzial, das Vertrauen in E-Commerce und damit das Vertrauen, das für Internet-Transaktionen benötigt wird, zu untergraben. Das zweite Ziel ist die Nutzung der Rechenleistung eines fremden Computers für profitorientierte Aktivitäten. Solche Aktivitäten können das Versenden von Spam, Erpressungsversuche in Form verteilter Denial-of-Service-Attacken oder Pay-per-Click-Aktivitäten sein.

Kapitel 2

Erste Schritte

In diesem Kapitel werden die ersten Schritte mit Worry-Free Business Security beschrieben.

Das Worry-Free Business Security Netzwerk

Worry-Free Business Security besteht aus Folgendem:

- *Security Server auf Seite 2-2*
- *Agents auf Seite 2-4*
- *Webkonsole auf Seite 2-4*

Security Server

Die zentrale Komponente von Worry-Free Business Security ist der Security Server. Auf dem Security Server befindet sich die Webkonsole, die zentrale webbasierte Management-Konsole für Worry-Free Business Security. Der Security Server installiert Agents auf den Clients im Netzwerk und stellt eine Agent-Server-Verbindung her. Er ermöglicht das Anzeigen von Informationen über den Sicherheitsstatus und von Agents, das Konfigurieren von Sicherheitsfunktionen und den Komponenten-Download von einem zentralen Speicherort. Außerdem enthält der Security Server die Datenbank, in der Protokolle über die von den Agents berichteten Internet-Bedrohungen gespeichert sind.

Der Security Server hat folgende wichtige Funktionen:

- Er installiert, überwacht und verwaltet die Agents.
- Er lädt von Agents benötigte Komponenten herunter. Standardmäßig lädt der Security Server Komponenten vom Trend Micro ActiveUpdate Server herunter und verteilt diese dann auf die Agents.

Suchserver

Der Sicherheitsserver beinhaltet einen Dienst namens Suchserver, der während der Installation des Security Servers automatisch installiert wird. Daher muss er nicht gesondert installiert werden. Der Suchserver wird unter dem Prozessnamen `iCRCService.exe` ausgeführt und von der Microsoft Management Console als **Trend Micro Smart Scan Service** angezeigt.

Wenn Security Agents eine Suchmethode mit dem Namen **Smart Scan** verwenden, hilft der Suchserver diesen Agents dabei, die Suchen effizienter auszuführen. Der Smart Scan-Vorgang kann wie folgt beschrieben werden:

- Der Security Agent durchsucht den Client mit Hilfe des **Agent-Pattern von Smart Scan**, einer abgespeckten Version des herkömmlichen Viren-Pattern, nach Sicherheitsbedrohungen. Das Agent-Pattern von Smart Scan beinhaltet die meisten im Viren-Pattern verfügbaren Bedrohungssignaturen.
- Ein Security Agent, der das Risiko der Datei während der Suche nicht ermitteln kann, überprüft dies, indem er eine Suchabfrage an den Suchserver sendet. Der Suchserver überprüft das Risiko mit Hilfe des **Smart-Scan-Pattern**, der die Bedrohungssignaturen enthält, die auf dem Agent-Pattern von Smart Scan nicht verfügbar sind.
- Der Security Agent legt die Suchabfrageergebnisse des Suchservers zur Verbesserung der Suchleistung in einem Zwischenspeicher ab.

Durch die Bereitstellung einiger Bedrohungsdefinitionen unterstützt der Suchserver die Reduzierung des Bandbreitenverbrauchs des Security Agent beim Herunterladen von Komponenten. Security Agents laden anstatt des Viren-Pattern das Agent-Pattern von Smart Scan herunter, das deutlich kleiner ist.

Wenn Security Agents keine Verbindung zum Suchserver aufbauen können, können sie Suchabfragen an das Trend Micro Smart Protection Network senden, das die gleiche Funktion wie der Suchserver hat.

Es ist nicht möglich, den Suchserver separat vom Security Server zu deinstallieren. Wenn Sie den Suchserver nicht verwenden möchten:

1. Öffnen Sie die Microsoft Management Console im Computer Security Server und deaktivieren Sie **Trend Micro Smart Scan Service**.
2. Ändern Sie in der Webkonsole die Einstellung bei Security Agents in herkömmliche Suche, indem Sie zur Registerkarte **Administration** > **Allgemeine Einstellungen** > **Desktop/Server** navigieren und die Option **Smart Scan Service deaktivieren** auswählen.

Agents

Agents schützen Clients vor Sicherheitsbedrohungen. Clients umfassen Desktops, Server und Microsoft Exchange Server. Es gibt folgende Worry-Free Business Security Agents:

TABELLE 2-1. Worry-Free Business Security Agents

AGENT	BESCHREIBUNG
Security Agent	Schützt Desktops und Server vor Sicherheitsbedrohungen und Eindringversuchen.
Messaging Security Agent (nur Advanced)	Schützt Microsoft Exchange Server vor Sicherheitsbedrohungen in E-Mails.

Der Agent berichtet an den Security Server, von dem aus er installiert wurde. Damit der Security Server stets über die aktuellen Client-Informationen verfügt, sendet der Agent Ereignis- und Statusinformationen in Echtzeit. Agents berichten beispielsweise über Ereignisse wie entdeckte Bedrohungen, das Starten und Herunterfahren, den Startzeitpunkt einer Suche oder einen abgeschlossenen Update-Vorgang.

Webkonsole

Die Webkonsole ist die zentrale Stelle zur Überwachung von Security Agents in Ihrem gesamten Netzwerk. Sie enthält verschiedene Standardeinstellungen und -werte, die Sie entsprechend Ihren Sicherheitsanforderungen und -voraussetzungen konfigurieren können. Die Webkonsole verwendet alle gängigen Internet-Technologien wie Java, CGI, HTML und HTTP.

Verwenden Sie die Webkonsole, um:

- Agents auf Endpunkten zu verteilen.
- Agents zur gleichzeitigen Konfiguration und Verwaltung in logische Gruppen organisieren.

- Produkteinstellungen zu konfigurieren und die manuelle Suche auf Endpunkten zu starten.
- Benachrichtigungen empfangen und Protokolle zu Bedrohungsaktivitäten einsehen.
- Benachrichtigungen zu empfangen und Ausbruchswarnungen per E-Mail zu versenden, wenn Bedrohungen auf Endpunkten entdeckt werden.

Die Webkonsole öffnen

Öffnen Sie mit einem unterstützten Webbrowser die Webkonsole über einen beliebigen Endpunkt im Netzwerk. Weitere Informationen über Browseranforderungen finden Sie im Dokument *Systemvoraussetzungen*.

Prozedur

1. Wählen Sie eine der folgenden Optionen, um die Webkonsole zu öffnen:
   - Navigieren Sie am Endpunkt, auf dem sich der Security Server befindet, zum Desktop und klicken Sie auf die Verknüpfung Worry-Free Business Security.
   - Klicken Sie auf dem Endpunkt, auf dem sich der Security Server befindet, auf **Windows Start-Menü** > **Trend Micro Worry-Free Business Security** > **Worry-Free Business Security**.
   - Öffnen Sie einen Webbrowser auf einem beliebigen Endpunkt in Ihrem Netzwerk und geben Sie eine der folgenden Adressen ein:

     `https://{Name_des_Security_Servers oder IP-Adresse}:{Portnummer}/SMB`

     Beispiel:

     `https://my-test-server:4343/SMB`

     `https://192.168.0.10:4343/SMB`

     `http://my-test-server:8059/SMB`

`http://192.168.0.10:8059/SMB`

Tipp

Wenn Sie nicht SSL verwenden, geben Sie `http` statt `https` in die Adressleiste ein. Der Standardport für HTTP-Verbindungen ist 8059, für HTTPS-Verbindungen 4343.

Wenn die Umgebung Servernamen nicht über DNS auflösen kann, verwenden Sie statt der IP-Adresse den Servernamen.

Im Browser erscheint das Anmeldefenster von Worry-Free Business Security.

2. Geben Sie Ihr Kennwort ein und klicken Sie auf **Anmelden**.

   Im Browser erscheint das Fenster **Live-Status**.

Nächste Maßnahme

Überprüfen Sie Folgendes, wenn Sie nicht auf die Webkonsole zugreifen können.

Zu prüfendes Element	Details
Kennwort	Wenn Sie Ihr Kennwort vergessen haben, können Sie es mit dem Tool zum Zurücksetzen des Konsolenkennworts zurücksetzen. Sie finden dieses Tool auf dem Security Server im Ordner für Trend Micro Worry-Free Business Security im Windows Start-Menü.

Zu prüfendes Element	Details
Zwischenspeicher des Browsers	Nach einem Upgrade von einer Vorgängerversion von Worry-Free Business Security verhindern Dateien des Webbrowsers und des Proxy-Server-Caches möglicherweise das ordnungsgemäße Starten der Webkonsole. Leeren Sie den Zwischenspeicher des Browsers und aller Proxy-Server zwischen dem Trend Micro Security Server und dem Endpunkt, der für den Zugriff auf die Web-Konsole verwendet wird.
SSL-Zertifikat	Überprüfen Sie, ob der Webserver ordnungsgemäß ausgeführt wird. Überprüfen Sie bei Verwendung von SSL, ob das SSL-Zertifikat gültig ist. Weitere Informationen finden Sie in der Dokumentation des Webservers.

Zu prüfendes Element	Details

Einstellungen des virtuellen Verzeichnisses	Eventuell liegt ein Problem mit den Einstellungen des virtuellen Verzeichnisses vor, wenn Sie die Webkonsole auf einem IIS-Server ausführen und die folgende Meldung angezeigt wird:
	`Die Seite kann nicht angezeigt werden.`
	`HTTP-Fehler 403.1 - Verboten: Ausführungszugriff verweigert.`
	`Internet Information Services (IIS)`
	Diese Meldung wird angezeigt, wenn eine der folgenden Adressen für den Zugriff auf die Konsole verwendet wird:
	`http://{server name}/SMB/`
	`http://{server name}/SMB/default.htm`
	Die Konsole kann über die folgende Adresse jedoch problemlos geöffnet werden:
	`http://{server name}/SMB/console/html/cgi/cgichkmasterpwd.exe`
	Um dieses Problem zu lösen, überprüfen Sie die Ausführungsrechte für das virtuelle SMB Verzeichnis.
	Skripte aktivieren:
	1. Öffnen Sie den Internet Information Services (IIS) Manager.
	2. Wählen Sie im virtuellen SMB Verzeichnis die Option **Eigenschaften**.
	3. Wählen Sie die Registerkarte "Virtuelles Verzeichnis" aus und verwenden Sie als Ausführungsrecht `Skripts` anstatt `keine`. Ändern Sie auch die Ausführungsrechte für das virtuelle Verzeichnis der Client-Installation.

Navigation auf der Webkonsole

Die Webkonsole besteht aus folgenden Hauptbereichen:

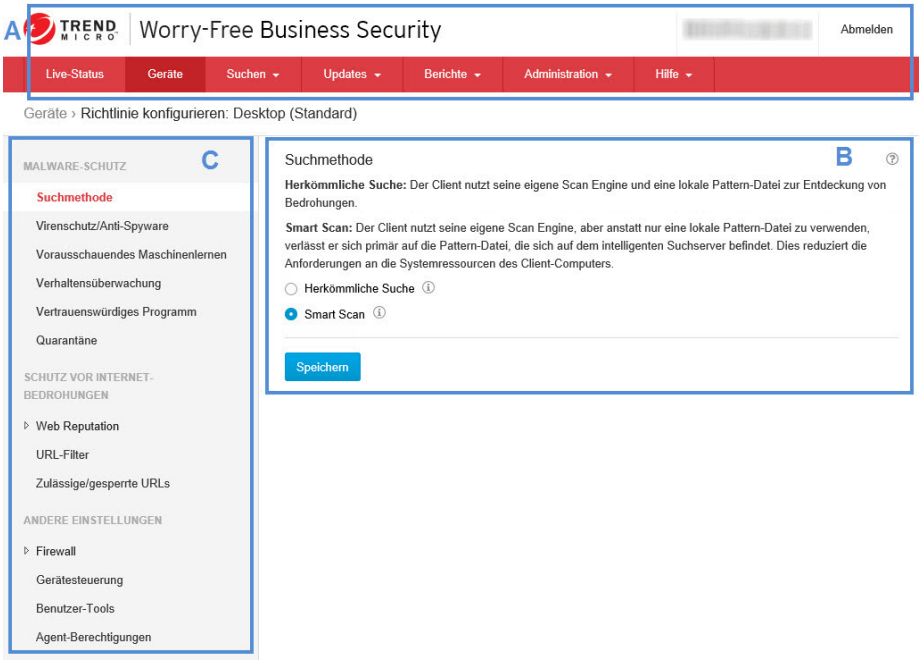


Tabelle 2-2. Hauptbereiche der Webkonsole

Abschnitt	Beschreibung
A. Hauptmenü	Oben an der Webkonsole befindet sich das Hauptmenü. Mit dem Link **Abmelden** können Sie auch Ihre aktuelle Sitzung beenden.
B. Konfigurationsbereich	Unterhalb der Hauptmenüelemente befindet sich der Konfigurationsbereich. In diesem Bereich können Sie Optionen auswählen und Einstellungen entsprechend dem von Ihnen ausgewählten Menüelement konfigurieren.

Abschnitt	Beschreibung
C. Seitenmenü (nicht in allen Fenstern verfügbar)	Wenn Sie eine Security Agent Gruppe im Fenster **Geräte** auswählen und anschließend auf **Richtlinie konfigurieren** klicken, wird ein Seitenmenü angezeigt. Verwenden Sie das Seitenmenü zur Konfiguration der Sicherheitseinstellungen und der Suchaktionen auf den Desktops und Servern der Gruppe. Bei Auswahl eines Messaging Security Agents im Fenster **Geräte** (nur Advanced) können Sie im Seitenmenü Sicherheitseinstellungen und Suchaktionen für Ihre Microsoft Exchange Server konfigurieren.

Tabelle 2-3. Abschnitt Hauptmenü

Menüelement	Description
Live-Status	Überwacht den allgemeinen Sicherheitsstatus von Security Agents und den operativen Status des Security Servers
Geräte	• Passen Sie die Sicherheitseinstellungen für Agents an. • Replizieren Sie die Einstellungen zwischen den Gruppen.
Suchen	• Durchsucht Endpunkte nach Bedrohungen • Legen Sie Zeitpläne für die Suche auf Clients fest.
Updates	• Überprüfen Sie den Trend Micro ActiveUpdate Server (oder eine benutzerdefinierte Update-Adresse) auf neueste Komponenten-Updates, wie z. B. Updates des Viren-Patterns, der Scan Engine, der Säuberungskomponenten und des Agent-Programms. • Konfigurieren Sie Update-Adressen. • Bestimmen Sie Security Agents als Update-Agents.
Berichte	Erzeugen Sie Berichte, um Bedrohungen und andere sicherheitsrelevante Ereignisse zu verfolgen.

Menüelement	Description
Administration	• Erstellen Sie Benachrichtigungen über ungewöhnliche Bedrohungs- oder Systemereignisse. • Verwenden Sie globale Einstellungen, um die Verwaltung zu vereinfachen. • Verwenden Sie Management-Tools für die Sicherheit von Netzwerk und Clients. • Zeigen Sie Informationen über Produktlizenzen an, verwalten Sie das Administratorkennwort und sorgen Sie durch die Teilnahme am Smart Feedback Programm für eine sichere Geschäftsumgebung beim Austausch digitaler Informationen. • Automatisiert Produkt-Updates und benachrichtigt Benutzer, wenn ein neues Update-Paket verfügbar ist.
Hilfe	• Suchen Sie nach speziellen Inhalten und Themen. • Zeigen Sie das Administratorhandbuch an. • Greifen Sie auf aktuelle Informationen aus der Knowledge Base (KB) zu. • Zeigen Sie Informationen zu den Themen Sicherheit, Vertrieb, Support und aktuelle Version an.

Symbole auf der Webkonsole

In der nachfolgenden Tabelle werden die einzelnen Symbole auf der Webkonsole und deren Verwendung beschrieben.

Tabelle 2-4. Symbole auf der Webkonsole

Symbol	Beschreibung
	Hilfe-Symbol. Öffnet die Online-Hilfe.
	Das Symbol Aktualisieren. Aktualisiert die Ansicht des aktuellen Fensters.
	Das Symbol Bereich erweitern/reduzieren. Zeigt Bereiche an oder blendet sie aus. Es kann jeweils nur ein Bereich erweitert werden.

Symbol	Beschreibung
	Das Symbol Information. Zeigt Informationen über ein bestimmtes Element an.
	Das Symbol Benachrichtigungen anpassen. Zeigt verschiedene Benachrichtigungsoptionen an.

Kapitel 3

Agents installieren

In diesem Kapitel werden die erforderlichen Schritte für die Installation von Security Agents und Messaging Security Agents (nur Advanced) beschrieben. Es enthält außerdem Informationen über die Deinstallation dieser Agents.

Security Agent-Installation

Führen Sie eine Neuinstallation des Security Agents auf Windows Clients durch (Desktops und Server). Verwenden Sie die Installationsmethode, die Ihren Anforderungen am besten entspricht.

Schließen Sie vor der Installation des Security Agents alle aktiven Anwendungen auf den Clients. Der Installationsvorgang dauert möglicherweise länger, wenn vor der Installation nicht alle Anwendungen geschlossen werden.

Hinweis

Informationen zum Upgrade der Security Agents auf diese Version finden Sie im *Installations- und Upgrade-Handbuch*.

Voraussetzungen für die Installation des Security Agents

Auf der folgenden Website erhalten Sie eine vollständige Liste der Voraussetzungen für die Installation sowie aller kompatiblen Produkte von Drittanbietern:

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

Überlegungen zur Installation des Security Agents

Beachten Sie vor der Installation von Security Agents folgende Hinweise:

- **Agent-Funktionen:** Einige Security Agent-Funktionen sind auf bestimmten Windows-Plattformen nicht verfügbar. Weitere Informationen finden Sie unter *Verfügbare Security Agent Funktionen auf Seite 3-3*.
- **x64-Plattformen**: Eine Version des Security Agents mit reduzierter Funktionalität ist für x64-Plattformen erhältlich. Die IA-64-Plattform wird jedoch zur Zeit nicht unterstützt.

- **IPv6-Support**: Der Security Agent kann auf Dual-Stack- oder reinen IPv6-Endpoints installiert werden. Einige Installationsmethoden verfügen jedoch möglicherweise über besondere Anforderungen.

  Weitere Informationen finden Sie unter *Installation des Security Agents und IPv6-Unterstützung auf Seite 3-5*.

- **Ausnahmelisten**: Stellen Sie sicher, dass die Ausnahmelisten für die folgenden Funktionen richtig konfiguriert wurden:

  - **Verhaltensüberwachung**: Fügen Sie kritische Client-Programme zur Liste der zulässigen Programme hinzu, um zu verhindern, dass der Security Agent diese Anwendungen sperrt. Weitere Informationen finden Sie unter *Verhaltensüberwachung konfigurieren auf Seite 5-12*.

  - **Web Reputation**: Fügen Sie Websites, die Sie als sicher einstufen, zur Liste der zulässigen URLs hinzu, um zu verhindern, dass der Security Agent den Zugriff auf diese Websites sperrt. Weitere Informationen finden Sie unter *Web Reputation für Security Agents konfigurieren auf Seite 5-24*.

- **Agent-Installationsverzeichnis**: Während der Installation des Security Servers werden Sie über das Setup-Programm aufgefordert, das Installationsverzeichnis für den Agent anzugeben. Dabei handelt es sich standardmäßig um `$ProgramFiles\Trend Micro\Security Agent`. Wenn Sie die Security Agents in einem anderen Verzeichnis installieren möchten, geben Sie das neue Verzeichnis unter **Administration** > **Allgemeine Einstellungen** > **System** > **Security Agent-Installation** an.

Verfügbare Security Agent Funktionen

Die verfügbaren Security Agent Funktionen auf einem Client hängen vom Betriebssystem des Clients ab. Informieren Sie sich über nicht unterstützte Funktionen, wenn Sie einen Agent auf einem bestimmten Betriebssystem installieren.

Tabelle 3-1. Security Agent Funktionen

Funktion	Windows Betriebssystem		
	10	SBS 2011	Server 2012/2012 R2/2016/2019
Manuelle Suche (Normale und Aggressive Suche), Echtzeitsuche und zeitgesteuerte Suche	Ja	Ja	Ja
Firewall	Ja	Ja	Ja
Web Reputation	Ja	Ja	Ja
URL-Filter	Ja	Ja	Ja
Verhaltensüberwachung	Ja	Ja	Ja
Gerätesteuerung	Ja	Ja	Ja
Damage Cleanup Services	Ja	Ja	Ja
Mail Scan (POP3)	Ja	Ja	Ja
Manuelle und zeitgesteuerte Updates	Ja	Ja	Ja
Update Agent	Ja	Ja	Ja
Agent Plug-in Manager	Ja	Ja	Ja
Smart Feedback	Ja	Ja	Ja
Trend Micro Anti-Spam Symbolleiste	Ja Unterstützte E-Mail-Clients (32 und 64 Bit): • Outlook 2010 • Outlook 2013 • Outlook 2016	Nein	Nein

Funktion	Windows Betriebssystem		
	10	SBS 2011	Server 2012/2012 R2/2016/2019
HouseCall	Ja	Ja	Ja
Case Diagnostic Tool	Ja	Ja	Ja
Wi-Fi Advisor	Ja	Nein	Nein

Installation des Security Agents und IPv6-Unterstützung

In diesem Thema werden Fragen zur Installation des Security Agents auf einem Dual-Stack- oder einem reinen IPv6-Client behandelt.

Betriebssystem

Der Security Agent kann nur auf folgenden Betriebssystemen, die IPv6-Adressierung unterstützen, installiert werden:

- Windows SBS 2011
- Windows 10 (alle Editionen)
- Windows Server 2012/2012 R2 (alle Editionen)
- Windows Server 2016 (Standard, Datacenter, Essentials)
- Windows Server 2019 (Standard, Datacenter, Essentials)

Eine vollständige Liste der Systemvoraussetzungen finden Sie auf der folgenden Website:

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

Unterstützte Installationsmethoden

Alle verfügbaren Installationsmethoden können zur Installation des Security Agents auf reinen IPv6- oder Dual-Stack-Clients verwendet werden. Bei einigen Installationsmethoden gibt es besondere Voraussetzungen für die erfolgreiche Installation des Security Agents.

Tabelle 3-2. Installationsmethoden und IPv6-Unterstützung

Installationsmethode	Voraussetzungen/Überlegungen
Installation über die interne Website und Installation per E-Mail-Benachrichtigung	Die Installation des Security Servers auf einem reinen IPv6-Client setzt einen Dual-Stack- oder reinen IPv6-Server voraus, und sein Host-Name oder seine IPv6-Adresse müssen in der URL enthalten sein. Bei Dual-Stack-Clients hängt die im Installationsstatusfenster angezeigte IPv6-Adresse von der Option ab, die im Abschnitt **Bevorzugte IP-Adresse** auf der Registerkarte **Administration** > **Allgemeine Einstellungen** > **Desktop/Server** ausgewählt wurde.
Installation mit Vulnerability Scanner und Remote-Installation	Ein reiner IPv6-Security Server kann den Security Agent nicht auf reinen IPv4-Clients installieren. Ebenso kann ein reiner IPv4-Security Server den Agent nicht auf reinen IPv6-Clients installieren.

IP-Adressen des Security Agents

Ein Security Server in einer Umgebung, die IPv6-Adressierung unterstützt, kann folgende Security Agents verwalten:

- Ein Security Server, der auf einem reinen IPv6-Client installiert ist, kann reine IPv6-Security Agents verwalten.
- Ein Security Server auf einem Dual-Stack-Client, dem sowohl IPv4- als auch IPv6-Adressen zugewiesen wurden, kann reine IPv6-, Dual-Stack- und reine IPv4-Security Agents verwalten.

Nach der Installation oder dem Upgrade von Security Agents, registrieren sich die Agents über eine IP-Adresse am Security Server.

- Reine IPv6-Security Agents registrieren sich mit ihrer IPv6-Adresse.
- Reine IPv4-Security Agents registrieren sich mit ihrer IPv4-Adresse.
- Dual-Stack-Security Agents registrieren sich entweder mit ihrer IPv4- oder mit ihrer IPv6-Adresse. Sie können im Bereich **Bevorzugte IP-Adresse** auf der Registerkarte **Administration** > **Allgemeine**

Einstellungen > **Desktop/Server** die IP-Adresse auswählen, die von diesen Agents verwendet wird.

Installationsmethoden für den Security Agent

In diesem Abschnitt finden Sie eine Zusammenfassung der verschiedenen Methoden für eine Neuinstallation des Security Agents. Für alle Installationsmethoden sind lokale Administratorrechte auf den Zielendpunkten erforderlich.

Wenn Sie bei der Installation der Security Agents die IPv6-Unterstützung aktivieren wollen, lesen Sie die Richtlinien unter *Installation des Security Agents und IPv6-Unterstützung auf Seite 3-5*.

Tabelle 3-3. Installationsmethoden

Installationsmethode/ Betriebssystemunterstützung	Überlegungen zur Verteilung					
	WAN-Verteilung	Zentrale Verwaltung	Erfordert Eingreifen durch den Benutzer	Erfordert IT-Ressource	Verteilung in hoher Anzahl	Verbrauchte Bandbreite
Interne Webseite Wird auf allen Betriebssystemen unterstützt	Ja	Ja	Ja	Nein	Nein	Gering, wenn zeitgesteuert
E-Mail-Benachrichtigung Wird auf allen Betriebssystemen unterstützt	Ja	Ja	Ja	Nein	Nein	Hoch, wenn die Installationen gleichzeitig gestartet werden

Installationsmethode/ Betriebssystemunterstützung	Überlegungen zur Verteilung					
	WAN-Verteilung	Zentrale Verwaltung	Erfordert Eingreifen durch den Benutzer	Erfordert IT-Ressource	Verteilung in hoher Anzahl	Verbrauchte Bandbreite
Remote-Installation Wird auf allen Betriebssystemen unterstützt	Nein	Ja	Nein	Ja	Ja	Gering, wenn zeitgesteuert
Anmeldeskript-Setup Wird auf allen Betriebssystemen unterstützt	Nein	Ja	Nein	Ja	Ja	Hoch, wenn die Installationen gleichzeitig gestartet werden
Client Packager Wird auf allen Betriebssystemen unterstützt	Ja	Nein	Ja	Ja	Nein	Gering, wenn zeitgesteuert
Trend Micro Vulnerability Scanner (TMVS) Wird auf allen Betriebssystemen unterstützt, ausgenommen Windows 10	Nein	Ja	Nein	Ja	Ja	Gering, wenn zeitgesteuert

Bei der Verteilung an einem einzelnen Standort und in Unternehmen, in denen IT-Richtlinien strikt durchgesetzt werden, kann der IT-Administrator

entscheiden, ob er die Verteilung über die **Remote-Installation** oder das **Anmeldeskript-Setup** vornehmen möchte.

In Unternehmen, in denen IT-Richtlinien weniger strikt durchgesetzt werden, empfiehlt Trend Micro, Security Agents über die **interne Webseite** zu installieren. Zur Verwendung dieser Methode benötigen Endbenutzer, die den Security Agent installieren, jedoch Administratorrechte.

Die **Remote-Installation** eignet sich für Netzwerke mit Active Directory. Wenn Ihr Netzwerk kein Active Directory verwendet, sollte die Installation über die interne Website vorgenommen werden.

Installation über die interne Webseite

Vorbereitungen

Für die Installation über die interne Webseite sind folgende Voraussetzungen erforderlich:

Zu prüfendes Element	Voraussetzung
Security Server	Der Security Server muss auf einem der folgenden Betriebssysteme installiert sein: • Windows 7, 8.1, 10, Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019 oder SBS 2008, 2011 • mit Internet Information Server (IIS) 7.0, 7.5, 8.0, 8.5, 10 oder Apache 2.4

Zu prüfendes Element	Voraussetzung
Zielendpunkt	• Der Zielendpunkt muss auf Windows 10, Server 2012, 2012 R2, 2016, 2019 oder SBS 2011 installiert sein. • Auf dem Zielendpunkt muss Internet Explorer 9.0 oder höher installiert sein. • Benutzer müssen für die Anmeldung beim Endpunkt ein Administratorkonto verwenden. **Hinweis** Wenn der Zielendpunkt auf einem Desktop-Betriebssystem ausgeführt wird, aktivieren Sie zuerst das integrierte Administratorkonto. Weitere Informationen finden Sie auf der Support-Website von Microsoft (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account).
Sicherheitseinstellungen für Internet Explorer	Benutzer müssen die folgenden Schritte durchführen: 1. Öffnen Sie den Internet Explorer, und fügen Sie die URL des Security Servers (z. B. `https://<Name des Security Servers>:4343/SMB/console/html/client`) zur Liste der vertrauenswürdigen Websites hinzu. Greifen Sie auf die Liste zu, indem Sie zu **Tools** > **Internetoptionen** > **Sicherheit** navigieren, das Symbol **Vertrauenswürdige Sites** auswählen und auf **Sites** klicken. 2. Ändern Sie die Sicherheitseinstellung des Internet Explorers, um die Option **Automatische Eingabeaufforderung für ActiveX-Steuerelemente** zu aktivieren. Navigieren Sie zu **Tools** > **Internetoptionen** > **Sicherheit** und klicken Sie auf **Stufe anpassen**.
IPv6	Falls Sie in einer gemischten Umgebung aus reinen IPv4-, reinen IPv6- und Dual-Stack-Endpunkten arbeiten, benötigt der Security Server IPv4- und IPv6-Adressen, damit sich alle Endpunkte mit der internen Website auf dem Security Server verbinden können.

Senden Sie die folgenden Anweisungen zur Installation des Security Agent von der internen Website an die Benutzer. Weitere Informationen zur

Versendung der Installationsbenachrichtigung per E-Mail finden Sie unter *Per E-Mail-Benachrichtigung installieren auf Seite 3-33*.

Prozedur

1. Melden Sie sich über ein Administratorkonto beim Endpunkt an.
2. Öffnen Sie Internet Explorer und geben Sie eine der folgenden Adressen ein:
   - Security Server mit SSL:

     ```
     https://<Name oder IP-Adresse des Security
     Servers>:4343/SMB/console/html/client
     ```

   - Security Server ohne SSL:

     ```
     http://<Name oder IP-Adresse des Security
     Servers>:8059/SMB/console/html/client
     ```

3. Klicken Sie auf **Jetzt installieren**, um die Installation des Security Agents zu starten.

   Die Installation wird gestartet. Lassen Sie die Installation des ActiveX-Steuerelements zu, wenn Sie dazu aufgefordert werden. Nach der Installation wird das Security Agent Symbol in der Windows Task-Leiste angezeigt.

   Hinweis

   Eine Liste der Symbole in der Windows Task-Leiste finden Sie unter *Status des Security Agents prüfen auf Seite A-2*.

Nächste Maßnahme

Versuchen Sie Folgendes, falls Benutzer Sie benachrichtigen, dass die Installation über die interne Website nicht möglich ist.

- Überprüfen Sie mithilfe von Ping und Telnet, ob Endpunkt und Server miteinander kommunizieren können.

- Überprüfen Sie, ob auf dem Endpunkt TCP/IP aktiviert und ordnungsgemäß konfiguriert ist.
- Überprüfen Sie bei Verwendung eines Proxy-Servers für die Endpunkt/Serverkommunikation, ob die Proxy-Einstellungen ordnungsgemäß konfiguriert sind.
- Löschen Sie im Webbrowser die Trend Micro Add-Ons und den Browser-Verlauf.

Mit dem Anmeldeskript-Setup installieren

Mit dem Anmeldeskript-Setup können Sie die Installation des Security Agents auf ungeschützten Clients automatisieren, wenn diese sich am Netzwerk anmelden. Das Anmeldeskript-Setup fügt zum Anmeldeskript des Servers das Programm `AutoPcc.exe` hinzu.

`AutoPcc.exe` installiert den Security Agent auf nicht geschützten Clients und aktualisiert Programmdateien und Komponenten. Die Clients müssen zur Domäne gehören, um AutoPcc über das Anmeldeskript zu nutzen.

Wenn bereits ein Anmeldeskript vorhanden ist, fügt das Anmeldeskript-Setup einen Befehl hinzu, der `AutoPcc.exe` ausführt. Andernfalls wird eine Batch-Datei mit dem Namen `ofcscan.bat` erstellt, die den Befehl zur Ausführung von `AutoPcc.exe` enthält.

Das Anmeldeskript-Setup fügt die folgenden Informationen am Ende des Skripts hinzu:

```
\\<Servername>\ofcscan\autopcc
```

Wobei gilt:

- `<Servername>` ist der Computername oder die IP-Adresse des Security Server Computers.
- ‘`ofcscan`’ ist der Name des Freigabeordners auf dem Security Server.
- ‘`autopcc`’ ist der Link zu der ausführbaren Datei ‘autopcc’, die den Security Agent installiert.

Speicherort des Anmeldeskripts auf allen Windows Server Versionen (durch ein über die Netzwerkanmeldung freigegebenes Verzeichnis):

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

Prozedur

1. Öffnen Sie `<Security Server-Installationsordner>\PCCSRV\Admin` auf dem Computer, den Sie zur Ausführung der Server-Installation verwendet haben.

2. Doppelklicken Sie auf `SetupUsr.exe`.

   Das Dienstprogramm **Anmeldeskript-Setup** wird gestartet. Die Konsole zeigt eine Ansicht aller Domänen im Netzwerk.

3. Suchen Sie nach dem Server, dessen Anmeldeskript Sie ändern möchten, wählen Sie ihn aus, und klicken Sie dann auf **Auswählen**. Stellen Sie sicher, dass es sich beim Server um einen primären Domänencontroller handelt und Sie Administratorzugriff auf den Server haben.

   Das Anmeldeskript-Setup fordert Sie zur Angabe eines Benutzernamens und eines Kennworts auf.

4. Geben Sie den Benutzernamen und das Kennwort ein. Klicken Sie auf **OK**, um den Vorgang fortzusetzen.

   Das Fenster **Benutzer auswählen** wird angezeigt. Die Liste **Benutzer** enthält die Profile der Benutzer, die sich an dem Server anmelden. Die Liste **Ausgewählte Benutzer** enthält die Benutzerprofile, deren Anmeldeskript geändert werden soll.

5. Um das Anmeldeskript für ein Benutzerprofil zu ändern, wählen Sie aus der Liste ‘Benutzer’ das Benutzerprofil aus, und klicken Sie anschließend auf **Hinzufügen**.

6. Um das Anmeldeskript aller Benutzer zu ändern, klicken Sie auf **Alle hinzufügen**.

7. Um ein zuvor ausgewähltes Benutzerprofil auszuschließen, wählen Sie den Namen aus der Liste **Ausgewählte Benutzer** aus, und klicken Sie auf **Löschen**.

8. Um die Auswahl aufzuheben, klicken Sie auf **Alle löschen**.

9. Klicken Sie auf **Übernehmen**, wenn alle gewünschten Benutzerprofile in der Zielliste **Ausgewählte Benutzer** enthalten sind.

   Eine Meldung informiert Sie über die erfolgreiche Änderung der Anmeldeskripts des Servers.

10. Klicken Sie auf **OK**.

    Der Eingangsbildschirm des Anmeldeskript-Setups wird wieder angezeigt.

11. Um das Anmeldeskript-Setup zu schließen, klicken Sie auf **Beenden**.

Mit Client Packager installieren

Client Packager erstellt ein Installationspaket, das Sie per CD-ROM oder sonstigen herkömmlichen Medien an die Benutzer versenden können. Benutzer führen das Paket auf dem Client aus, um den Security Agent sowie die Update-Komponenten zu installieren oder zu aktualisieren.

Client Packager ist in folgenden Fällen besonders nützlich:

- Bei der Verteilung und Installation des Security Agents oder der Komponenten auf externen Clients an Standorten mit geringer Bandbreite.
- Bei eingeschränkter Internet-Konnektivität, z. B. aufgrund eines geschlossenen LAN oder eines fehlenden Internet-Zugangs.

Security Agents, die mit Client Packager installiert werden, berichten an den Server, auf dem das Paket erstellt wurde.

Prozedur

1. Navigieren Sie auf dem Security Server Computer zu `<Server-Installationsordner>\PCCSRV\Admin\Utility\ClientPackager`.

2. und doppelklicken Sie auf `ClnPack.exe`.

   Die Client Packager Konsole wird geöffnet.

3. Wählen Sie das Betriebssystem, für das Sie das Paket erstellen möchten. Verteilen Sie das Paket nur an Clients, die unter diesem Betriebssystem laufen. Erstellen Sie ein anderes Paket, um es an ein anderes Betriebssystem zu verteilen.

4. Wählen Sie für das Paket die Suchmethode aus.

   Weitere Informationen über Suchmethoden finden Sie unter *Suchmethoden auf Seite 5-3*.

   Welche Komponenten im Paket enthalten sind, hängt von der ausgewählten Suchmethode ab. Bei der intelligenten Suche (Smart Scan) werden alle Komponenten mit Ausnahme des Viren-Patterns gefunden. Bei der herkömmlichen Suche sind alle Komponenten außer Agent-Pattern von Smart Scan eingeschlossen.

5. Wählen Sie aus, welche Art von Paket Sie erstellen möchten.

TABELLE 3-4. Client-Paketarten

PACKETTYP	BESCHREIBUNG
Setup	Wählen Sie **Setup**, um das Paket als MSI-Datei zu erstellen, die dem Paketformat von Microsoft Installer entspricht. Das Paket installiert das Security Agent Programm mit den Komponenten, die gegenwärtig auf dem Security Server verfügbar sind. Falls eine vorherige Version des Security Agents auf dem Ziel-Client installiert ist und Sie ein Upgrade durchführen möchten, erstellen Sie die MSI-Datei über den Security Server, der den Agent verwaltet. Andernfalls wird kein Upgrade für den Agent ausgeführt.

Packettyp	Beschreibung
Update	Wählen Sie **Update**, um ein Paket zu erstellen, das die Komponenten enthält, die gegenwärtig auf dem Security Server verfügbar sind. Das Paket wird anschließend als ausführbare Datei erstellt. Verwenden Sie dieses Paket, falls Probleme beim Upgrade der Komponenten auf dem Client auftauchen, auf dem der Security Agent installiert ist.

6. Klicken Sie auf **Unbeaufsichtigter Modus**, um ein Paket zu erstellt, das im Hintergrund für den Benutzer unsichtbar auf dem Client installiert wird. Der Installationsfortschritt wird nicht angezeigt. Aktivieren Sie diese Option, wenn Sie planen, das Paket remote auf den Client zu verteilen.

7. Klicken Sie auf **Virensuche vor Installation deaktivieren (Neuinstallation)**, falls der Client vor der Installation des Security Agents nicht auf Viren durchsucht werden soll. Wählen Sie diese Vorgehensweise nur, wenn Sie sicher sind, dass der Client bedrohungsfrei ist.

   Wenn die Virensuche vor der Installation aktiviert ist, führt Setup eine Suche nach Viren/Malware in den anfälligsten Bereichen des Computers durch. Dazu gehört das Folgende:

   - der Boot-Bereich und das Boot-Verzeichnis (Suche nach Boot-Viren)
   - Windows Ordner
   - Programme-Ordner

8. Stellen Sie im Feld neben **Quelldatei** sicher, dass der Speicherort der Datei `ofcscan.ini` richtig angegeben wurde. Zum Ändern des Pfads klicken Sie auf (...), um die Datei `ofcscan.ini` zu suchen. Standardmäßig befindet sich diese Datei im `<Installationsordner des Servers>\PCCSRV`.

9. Klicken Sie unter Ausgabedatei auf (...), um anzugeben, wo das Paket erstellt werden soll, und geben Sie den Namen der Paketdatei an (z. B. `ClientSetup.exe`)

10. Klicken Sie auf **Erstellen**.

    Nach der Erstellung des Pakets wird die Meldung „Das Paket wurde erstellt“ angezeigt. Suchen Sie das Verzeichnis, das Sie im vorhergehenden Schritt angegeben haben.

Nächste Maßnahme

Verteilen Sie das Paket an die Clients.

Client-Voraussetzungen:

- Festplattenspeicher
  - Herkömmliche Suche: mindestens 1,5 GB (2 GB empfohlen)
  - Smart Scan: 500 MB

  1 GB freier Speicherplatz, falls für das Paket die herkömmliche Suche festgelegt wurde, 500 MB für Smart Scan.
- Windows Installer 4.5 oder später (zur Ausführung eines MSI-Pakets)

Richtlinien für die Paketverteilung:

- Senden Sie das Paket an die Benutzer, und fordern Sie sie auf, es mit einem Doppelklick auf die Datei (`.MSI` oder `.EXE`) auszuführen.

  Hinweis

  Senden Sie das Paket nur an die Benutzer, deren Security Agent an den Server berichtet, auf dem das Paket erstellt wurde.

- Leiten Sie Benutzer an, mit der rechten Maustaste auf die Paketdatei zu klicken und **Als Administrator ausführen** auszuwählen.
- Falls Sie ein Active Directory verwenden, können Sie den Security Agent mit der `.MSI`-Datei automatisch an alle Clients gleichzeitig verteilen, statt jeden Benutzer aufzufordern, den Security Agent selbst zu installieren. Verwenden Sie **Computer-Konfiguration** statt **Benutzerkonfiguration**, damit der Security Agent unabhängig von dem Benutzer installiert werden kann, der sich beim Client anmeldet.

- Falls ein neuinstallierter Security Agent keine Verbindung zum Security Server herstellen kann, behält der Security Agent die Standardeinstellungen bei. Wenn der Security Agent mit dem Security Server verbunden wird, erhält er die Einstellungen für seine Gruppe, die in der Webkonsole festgelegt wurden.
- Wenn beim Upgrade des Security Agents mit Client Packager Probleme auftreten, empfiehlt Trend Micro, zunächst die vorherige Version des Security Agents zu deinstallieren und dann die neue Version zu installieren. Hinweise zur Deinstallation finden Sie unter *Agents entfernen auf Seite 3-40*.

Mit Remote-Installation installieren

Vorbereitungen

Installieren Sie den Security Agent remote auf einem oder mehreren mit dem Netzwerk verbundenen Endpunkten.

Zur Remote-Installation müssen folgende Voraussetzungen erfüllt sein:

Zu prüfendes Element	Voraussetzung
Zielendpunkt	• Melden Sie sich über ein Administratorkonto bei den einzelnen Zielendpunkten an. **Hinweis** • Wenn der Zielendpunkt auf einem Desktop-Betriebssystem ausgeführt wird, aktivieren Sie zuerst das integrierte Administratorkonto. Weitere Informationen finden Sie auf der Support-Website von Microsoft (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account). • Beim Ausführen der Remote-Installation auf Windows 10 kann das Microsoft-Konto nicht für die Anmeldung beim Ziel-Client verwendet werden

Zu prüfendes Element	Voraussetzung
	• Auf dem Zielendpunkt darf kein Security Server installiert sein. Über die Remote-Installation wird der Security Agent nicht auf Endpunkten installiert, die den Security Server bereits ausführen.
Datei- und Druckfreigaben	Aktivieren Sie auf dem Endpunkt vorübergehend Datei- und Druckerfreigaben. **Hinweis** Falls die unternehmensinterne Sicherheitsrichtlinie die Deaktivierung der Windows Firewall vorsieht, fahren Sie mit dem Abschnitt für die Remote-Registrierung fort. 1. Öffnen Sie in der Systemsteuerung die Windows Firewall. 2. Klicken Sie auf **Ein Programm über die Windows Firewall zulassen**. Geben Sie auf die entsprechende Aufforderung hin entweder ein Administratorkennwort ein, oder bestätigen Sie das Kennwort. Das Fenster der Windows Firewall-Einstellungen wird angezeigt. 3. Aktivieren Sie in der Liste **Programm oder Port** auf der Registerkarte **Ausnahmen** das Kontrollkästchen **Datei- und Druckerfreigaben**. 4. Klicken Sie auf **OK**. 5. Falls nötig, stellen Sie nach der Installation von Security Agents die ursprünglichen Einstellungen wieder her.
Benutzerkontensteuerung	Deaktivieren Sie die Benutzerkontensteuerung. **Hinweis** Ändern Sie den folgenden Registrierungsschlüssel, um die Benutzerkontensteuerung zu deaktivieren: `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] “EnableLUA”=dword:00000000`. Falls nötig, stellen Sie nach der Installation von Security Agents die ursprünglichen Einstellungen wieder her.

Zu prüfendes Element	Voraussetzung
Remote-Registrierung	Starten Sie vorübergehend den Remote-Registrierungsdienst. 1. **Hinweis** Geben Sie im Fenster "Ausführen..." `services.msc` ein, um die Microsoft Management Console zu öffnen. 2. Klicken Sie mit der rechten Maustaste auf **Remote-Registrierung**, und wählen Sie **Starten**. 3. Falls nötig, stellen Sie nach der Installation von Security Agents die ursprünglichen Einstellungen wieder her.
IPv6	Ein Dual-Stack-Security Server kann den Security Agent auf einem beliebigen Endpunkt installieren. Ein reiner IPv6-Security Server kann den Security Agent nur auf reinen IPv6- oder Dual-Stack-Endpunkten installieren.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Klicken Sie auf **Geräte hinzufügen**.
3. Wählen Sie unter **Computertyp** die Option **Desktop oder Server** aus.
4. Wählen Sie im Bereich **Methode** die Option **Remote-Installation** aus.
5. Klicken Sie auf **Weiter**.

   Ein neues Fenster wird angezeigt.
6. Wählen Sie aus der Liste der Clients im Fenster **Gruppen und Computer** einen Client, und klicken Sie anschließend auf **Hinzufügen**. Sie werden aufgefordert, einen Benutzernamen und ein Kennwort für den Client einzugeben.
7. Geben Sie Ihren Benutzernamen und das Kennwort ein, und klicken Sie dann auf **Anmelden**. Der Client wird in der Liste **Ausgewählte Computer** angezeigt.

8. Wiederholen Sie diese Schritte, bis alle Clients in der Liste **Ausgewählte Computer** angezeigt werden.

9. Klicken Sie auf **Installieren**.

   Ein Bestätigungsfenster wird angezeigt.

10. Klicken Sie auf **Ja**, um die Installation des Agents auf den Clients zu bestätigen.

    Während das Programm die Security Agent Dateien auf alle Clients kopiert, wird ein Fortschrittsfenster angezeigt.

    Wenn der Security Server die Installation auf einem Client abgeschlossen hat, wird der Installationsstatus im Feld **Status** in der Liste **Ausgewählte Computer** angezeigt, und der Client-Name wird mit einem grünen Häkchen versehen.

Nächste Maßnahme

Führen Sie folgende Aufgaben durch, falls die Remote-Installation fehlschlägt.

- Überprüfen Sie mit Hilfe von Ping und Telnet, ob Client und Server miteinander kommunizieren können.
- Überprüfen Sie, ob auf dem Client TCP/IP aktiviert und ordnungsgemäß konfiguriert ist.
- Überprüfen Sie bei Verwendung eines Proxy-Servers für die Client-Server-Kommunikation, ob die Proxy-Einstellungen richtig konfiguriert sind.
- Löschen Sie im Webbrowser die Trend Micro Add-Ons und den Browser-Verlauf.

Mit dem Vulnerability Scanner installieren

Vorbereitungen

Vulnerability Scanner erkennt, ob Antiviren-Lösungen installiert sind, sucht nach ungeschützten Clients im Netzwerk und installiert auf diesen Security Agents.

Zur Installation mit Vulnerability Scanner müssen folgende Voraussetzungen erfüllt sein:

Zu prüfendes Element	Voraussetzung
Starten von Vulnerability Scanner	Sie können Vulnerability Scanner auf dem Security Server oder auf einem beliebigen Client im Netzwerk starten. Der Client sollte Terminal Server nicht ausführen.
Ziel-Client	• Auf dem Ziel-Client darf kein Security Server installiert sein. Vulnerability Scanner installiert den Security Agent nicht auf Clients, die den Security Server bereits ausführen. • Benutzer müssen für die Anmeldung beim Client ein Administratorkonto verwenden. **Hinweis** Wenn der Ziel-Client auf einem Desktop-Betriebssystem ausgeführt wird, aktivieren Sie zuerst das integrierte Administratorkonto. Weitere Informationen finden Sie auf der Support-Website von Microsoft (https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-and-disable-the-built-in-administrator-account).

Vulnerability Scanner kann auf verschiedene Art durchgeführt werden.

- *Eine manuelle Schwachstellensuche ausführen auf Seite 3-23*
- *Eine DHCP-Suche ausführen auf Seite 3-24*
- *Eine zeitgesteuerte Schwachstellensuche konfigurieren auf Seite 3-27*

Eine manuelle Schwachstellensuche ausführen

Vulnerability Scanner bei Bedarf ausführen

Prozedur

1. Vulnerability Scanner starten

Vulnerability Scanner über folgende Orte starten:	Schritte
Security Server	a. Navigieren Sie zu `<Server-Installationsordner>\PCCSRV\Admin\Utility\TMVS`. b. Doppelklicken Sie auf `TMVS.exe`.
Einem Client im Netzwerk	a. Navigieren Sie auf dem Security Server zu `<Server-Installationsordner>\PCCSRV\Admin\Utility`. b. Kopieren Sie den Ordner `TMVS` auf den anderen Client. c. Öffnen Sie auf dem anderen Client den Ordner `TMVS` und doppelklicken Sie auf `TMVS.exe`.

2. Gehen Sie zum Abschnitt **Manuelle Suche**.
3. Geben Sie den IP-Adressbereich der Clients ein, die Sie überprüfen möchten.
   a. Geben Sie einen IPv4-Adressbereich ein.

   Hinweis

   Vulnerability Scanner kann IPv4-Adressbereiche nur dann abfragen, wenn das Tool auf einem reinen IPv4- oder Dual-Stack-Client ausgeführt wird. Der Vulnerability Scanner unterstützt nur einen IP-Adressbereich der Klasse B, z. B. 168.212.1.1 bis 168.212.254.254.

   b. Geben Sie bei einem IPv6-Adressbereich das IPv6-Präfix und die Länge ein.

Hinweis

Vulnerability Scanner kann IPv6-Adressbereiche nur dann abfragen, wenn das Tool auf einem reinen IPv6- oder Dual-Stack-Client ausgeführt wird.

4. Klicken Sie auf **Einstellungen**.

   Das Fenster **Einstellungen** wird angezeigt.

5. Konfigurieren Sie die Einstellungen des Vulnerability Scanners. Weitere Informationen finden Sie unter *Einstellungen für die Suche nach Schwachstellen auf Seite 3-29*.

6. Klicken Sie auf **OK**.

   Das Fenster mit den Einstellungen wird geschlossen.

7. Klicken Sie auf **Start**.

   Die Ergebnisse der Suche des Vulnerability Scanners werden in der Tabelle **Ergebnisse** auf der Registerkarte **Manuelle Suche** angezeigt.

   Hinweis

   Wenn auf dem Computer Windows Server 2008 ausgeführt wird, werden in der Tabelle **Ergebnisse** keine Informationen über die MAC-Adresse angezeigt.

8. Um die Ergebnisse in einer komma-separierte Datei im CSV-Format zu speichern, klicken Sie auf **Exportieren**, navigieren Sie zu dem Ordner, in dem die Datei gespeichert werden soll, geben Sie den Dateinamen ein, und klicken Sie auf **Speichern**.

Eine DHCP-Suche ausführen

Vulnerability Scanner auf Clients ausführen, die IP-Adressen von einem DHCP-Server anfordern.

Vulnerability Scanner horcht auf Port 67, dem Listening-Port des DHCP-Servers für DHCP-Anfragen. Wenn er eine DHCP-Anforderung von einem Client entdeckt, läuft Vulnerability Scanner auf dem Client.

Hinweis

Vulnerability Scanner kann keine DHCP-Anforderungen entdecken, wenn er auf Windows Server 2008 oder Windows 7 gestartet wird.

Prozedur

1. Konfigurieren Sie die DHCP-Einstellungen in der Datei `TMVS.ini`, die sich im folgenden Ordner befindet: `<Installationsordner des Servers>\PCCSRV\Admin\Utility\TMVS`.

TABELLE 3-5. DHCP-Einstellungen in der Datei `TMVS.ini`

EINSTELLUNG	BESCHREIBUNG
DhcpThreadNum=x	Geben Sie die Thread-Nummer für den DHCP-Modus ein. Der Minimalwert ist 3, der Maximalwert ist 100. Der Standardwert ist 3.
DhcpDelayScan=x	Dabei handelt es sich um die Verzögerung in Sekunden, bevor überprüft wird, ob auf dem anfragenden Computer bereits eine Antiviren-Software installiert ist. Der Minimalwert ist 0 (keine Wartezeit) und der Maximalwert ist 600. Der Standardwert ist 60.
LogReport=x	0 deaktiviert die Protokollierung, 1 aktiviert die Protokollierung. Vulnerability Scanner versendet die Ergebnisse der Suche an den Worry-Free Business Security Server. Protokolle werden im Fenster **Systemereignisprotokolle** der Webkonsole angezeigt.
OsceServer=x	Das ist die IP-Adresse oder der DNS-Name des Worry-Free Business Security Servers.
OsceServerPort=x	Das ist der Webserver-Port auf dem Worry-Free Business Security Server.

2. Vulnerability Scanner starten

Vulnerability Scanner über folgende Orte starten:	Schritte
Security Server	a. Navigieren Sie zu `<Server-Installationsordner>\PCCSRV\Admin\Utility\TMVS`. b. Doppelklicken Sie auf `TMVS.exe`.
Einem Client im Netzwerk	a. Navigieren Sie auf dem Security Server zu `<Server-Installationsordner>\PCCSRV\Admin\Utility`. b. Kopieren Sie den Ordner `TMVS` auf den anderen Client. c. Öffnen Sie auf dem anderen Client den Ordner `TMVS` und doppelklicken Sie auf `TMVS.exe`.

3. Klicken Sie im Abschnitt **Manuelle Suche** auf **Einstellungen**.

   Das Fenster **Einstellungen** wird angezeigt.

4. Konfigurieren Sie die Einstellungen des Vulnerability Scanners. Weitere Informationen finden Sie unter *Einstellungen für die Suche nach Schwachstellen auf Seite 3-29*.

5. Klicken Sie auf **OK**.

   Das Fenster mit den Einstellungen wird geschlossen.

6. Klicken Sie in der Tabelle **Ergebnisse** auf die Registerkarte **DHCP-Suche**.

   Hinweis

   Die Registerkarte **DHCP-Suche** ist auf Computern unter Windows Server 2008 und Windows 7 nicht verfügbar.

7. Klicken Sie auf **DHCP Start**.

   Vulnerability Scanner wartet nun auf DHCP-Anfragen und untersucht dann alle Clients, die sich im Netzwerk anmelden.

8. Um die Ergebnisse in einer komma-separierte Datei im CSV-Format zu speichern, klicken Sie auf **Exportieren**, navigieren Sie zu dem Ordner, in dem die Datei gespeichert werden soll, geben Sie den Dateinamen ein, und klicken Sie auf **Speichern**.

Eine zeitgesteuerte Schwachstellensuche konfigurieren

Schwachstellensuchen werden automatisch nach einem Zeitplan ausgeführt.

Prozedur

1. Vulnerability Scanner starten

Vulnerability Scanner über folgende Orte starten:	Schritte
Security Server	a. Navigieren Sie zu `<Server-Installationsordner>\PCCSRV\Admin\Utility\TMVS`. b. Doppelklicken Sie auf `TMVS.exe`.
Einem Client im Netzwerk	a. Navigieren Sie auf dem Security Server zu `<Server-Installationsordner>\PCCSRV\Admin\Utility`. b. Kopieren Sie den Ordner `TMVS` auf den anderen Client. c. Öffnen Sie auf dem anderen Client den Ordner `TMVS` und doppelklicken Sie auf `TMVS.exe`.

2. Gehen Sie zum Abschnitt **Zeitgesteuerte Suche**.
3. Klicken Sie auf **Hinzufügen/Bearbeiten**.

   Das Fenster **Zeitgesteuerte Suche** wird angezeigt.
4. Geben Sie einen Namen für die zeitgesteuerte Schwachstellensuche ein.
5. Geben Sie den IP-Adressbereich der Computer ein, die Sie überprüfen möchten.

a. Geben Sie einen IPv4-Adressbereich ein.

Hinweis

Vulnerability Scanner kann IPv4-Adressbereiche nur dann abfragen, wenn das Tool auf einem reinen IPv4- oder Dual-Stack-Host-Rechner mit verfügbarer IPv4-Adresse ausgeführt wird. Der Vulnerability Scanner unterstützt nur einen IP-Adressbereich der Klasse B, z. B. 168.212.1.1 bis 168.212.254.254.

b. Geben Sie bei einem IPv6-Adressbereich das IPv6-Präfix und die Länge ein.

Hinweis

Vulnerability Scanner kann IPv6-Adressbereiche nur dann abfragen, wenn das Tool auf einem reinen IPv6- oder Dual-Stack-Host-Rechner mit verfügbarer IPv6-Adresse ausgeführt wird.

6. Geben Sie die Startzeit im 24-Stunden-Format an, und wählen Sie, wie oft die Suche durchgeführt werden soll. Zur Auswahl stehen "Täglich", "Wöchentlich" oder "Monatlich".

7. Wählen Sie **Aktuelle Einstellungen verwenden**, wenn Sie manuelle Einstellungen für die Schwachstellensuche konfiguriert haben und diese verwenden wollen. Weitere Informationen zur manuellen Suche nach Schwachstellen finden Sie unter *Eine manuelle Schwachstellensuche ausführen auf Seite 3-23*.

   Wenn Sie keine manuellen Einstellungen für die Schwachstellensuche konfiguriert haben oder wenn Sie eine andere Reihe von Einstellungen verwenden wollen, wählen Sie **Einstellungen ändern** und klicken dann auf **Einstellungen**. Das Fenster **Einstellungen** wird angezeigt. Konfigurieren Sie die Sucheinstellungen und klicken Sie auf **OK**. Weitere Informationen finden Sie unter *Einstellungen für die Suche nach Schwachstellen auf Seite 3-29*.

8. Klicken Sie auf **OK**.

   Das Fenster **Zeitgesteuerte Suche** wird geschlossen. Die zeitgesteuerte Schwachstellensuche, die Sie erstellt haben, wird im Abschnitt

Zeitgesteuerte Suche angezeigt. Wenn Sie Benachrichtigungen aktiviert haben, erhalten Sie von Vulnerability Scanner die Suchergebnisse der zeitgesteuerten Schwachstellensuche.

9. Um die zeitgesteuerte Schwachstellensuche sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

   Die Ergebnisse der Schwachstellensuche werden in der Tabelle **Ergebnisse** auf der Registerkarte **Zeitgesteuerte Suche** angezeigt.

   Hinweis

   Wenn auf dem Computer Windows Server 2008 ausgeführt wird, werden in der Tabelle **Ergebnisse** keine Informationen über die MAC-Adresse angezeigt.

10. Sollen die Ergebnisse in einer komma-separierten Datei (`CSV`-Format) gespeichert werden, klicken Sie auf **Exportieren**, navigieren Sie zu dem Ordner, in dem die Datei gespeichert werden soll, geben Sie den Dateinamen ein, und klicken Sie auf **Speichern**.

11. Gehen Sie in den Bereich **Zeitgesteuerte Suchen**, wählen Sie die zeitgesteuerte Suche und klicken Sie auf **Löschen**, um geplante Schwachstellensuchen zu verwerfen.

Einstellungen für die Suche nach Schwachstellen

Konfigurieren Sie die folgenden Einstellungen, wenn Sie Vulnerability Scanner ausführen. Weitere Informationen zu den verschiedenen Arten von Schwachstellensuchen finden Sie unter *Mit dem Vulnerability Scanner installieren auf Seite 3-22*.

Einstellungen	Beschreibung und Anweisungen
Produktabfrage	Vulnerability Scanner kann feststellen, ob auf den Ziel-Clients Sicherheitssoftware vorhanden ist. 1. Wählen Sie die Sicherheitssoftware, die geprüft werden soll. 2. Vulnerability Scanner verwendet zum Prüfen der Software die Standard-Ports, die im Fenster angezeigt werden. Falls der Software-Administrator die Standard-Ports ändert, nehmen Sie die erforderlichen Änderungen vor, damit Vulnerability Scanner die Software erkennt. 3. Für Norton Antivirus Corporate Edition können Sie die Einstellungen für die Zeitüberschreitung ändern, indem Sie auf **Einstellungen** klicken.
	Sonstige Einstellungen zur Überprüfung von Produkten Anzahl der Clients festlegen, auf denen Vulnerability Scanner gleichzeitig nach Sicherheitssoftware sucht: 1. Navigieren Sie zu `<Installationsordner des Servers>\PCCSRV\Admin\Utility\TMVS` und öffnen Sie `TMVS.ini` mit Hilfe eines Texteditors, z. B. Notepad. 2. Anzahl der geprüften Clients festlegen: • Ändern Sie den Wert für `ThreadNumManual` für die Suche von manuellen Schwachstellen. Geben Sie einen Wert zwischen 8 und 64 an. Geben Sie zum Beispiel `ThreadNumManual=60` ein, wenn Vulnerability Scanner 60 Clients gleichzeitig überprüfen soll. • Ändern Sie den Wert für `ThreadNumSchedule` für die Suche nach zeitgesteuerte Schwachstellen. Geben Sie einen Wert zwischen 8 und 64 an. Geben Sie zum Beispiel `ThreadNumSchedule=50` ein, wenn Vulnerability Scanner 50 Clients gleichzeitig überprüfen soll. 3. Speichern Sie die Datei `TMVS.ini`.

Einstellungen	Beschreibung und Anweisungen
Einstellungen der Beschreibungsabfrage	Wenn Vulnerability Scanner die Clients ‘anpingen’ kann, kann er zusätzliche Informationen über die Clients abfragen. Es gibt zwei Methoden zur Abfrage von Informationen: • **Normale Abfrage**: Fragt Informationen über die Domäne und den Computer ab. • **Schnellabfrage**: Bei der Schnellabfrage wird nur der Computer-Name abgefragt.
Warneinstellungen	Die Ergebnisse der Schwachstellensuche automatisch an Sie selbst oder an andere Administratoren in Ihrem Unternehmen senden: 1. Wählen Sie **Email results to the system administrator**. 2. Klicken Sie auf **Konfigurieren**, um die E-Mail-Einstellungen festzulegen. 3. Geben Sie in das Feld **To** die E-Mail-Adresse des Empfängers ein. 4. Geben Sie in das Feld **An** die E-Mail-Adresse des Empfängers ein. 5. Geben Sie in das Feld **SMTP-Server** die Adresse des SMTP-Servers ein. Die Adresse hat das Format `smtp.firma.com`. Die Angabe des SMTP-Servers ist unbedingt erforderlich. 6. Geben Sie unter **Subject** einen Betreff für die Nachricht ein, oder übernehmen Sie den Standardbetreff. 7. Klicken Sie auf **OK**. Die Benutzer darüber informieren, dass auf ihren Computern keine Sicherheitssoftware installiert ist: 1. Wählen Sie **Display a notification on unprotected computers**. 2. Klicken Sie auf **Anpassen**, um die Benachrichtigung zu konfigurieren. 3. Geben Sie im Fenster **Benachrichtigung** eine eigene Meldung ein, oder verwenden Sie den Standardtext. 4. Klicken Sie auf **OK**.

Einstellungen	Beschreibung und Anweisungen
Als CSV-Datei speichern	Speichern Sie die Ergebnisse der Schwachstellensuche in einer komma-separierten Datei (CSV). Die Datei wird auf dem Client gespeichert, auf dem Vulnerability Scanner gestartet wurde. Akzeptieren Sie den standardmäßigen Dateipfad oder legen Sie einen neuen fest.
Ping-Einstellungen	Verwenden Sie die 'Ping'-Einstellungen, um das Vorhandensein eines Clients zu überprüfen und sein Betriebssystem festzustellen. Wenn diese Einstellungen deaktiviert sind, durchsucht Vulnerability Scanner alle IP-Adressen innerhalb des vorgegebenen IP-Adressbereichs, sogar solche, die auf keinem Client verwendet werden. Dadurch wird der Suchvorgang länger als er sein sollte. 1. Übernehmen oder ändern Sie die Standardwerte in den Feldern **Packet size** und **Timeout**. 2. Wählen Sie **Detect the type of operating system using ICMP OS fingerprinting**. Wenn Sie diese Option wählen, bestimmt Vulnerability Scanner, ob auf einem Client Windows oder ein anderes Betriebssystem läuft. Bei Clients mit Windows kann Vulnerability Scanner die Version von Windows feststellen.
	Weitere Ping-Einstellungen Anzahl der Clients festlegen, an die Vulnerability Scanner gleichzeitig Pings sendet: 1. Navigieren Sie zu `<Installationsordner des Servers>\PCCSRV\Admin\Utility\TMVS` und öffnen Sie `TMVS.ini` mit Hilfe eines Texteditors, z. B. Notepad. 2. Ändern Sie den Wert für `EchoNum`. Geben Sie einen Wert zwischen 1 und 64 an. Geben Sie zum Beispiel `EchoNum=60` ein, wenn Vulnerability Scanner Pings an 60 Clients gleichzeitig senden soll. 3. Speichern Sie die Datei `TMVS.ini`.

Einstellungen	Beschreibung und Anweisungen
Einstellungen des Security Servers	1. Wählen Sie **Security Agent automatisch auf ungeschützten Computern installieren**, um den Security Agent auf Clients zu installieren, die von Vulnerability Scanner durchsucht werden. 2. Geben Sie den Security Server Host-Namen oder die IPv4-/IPv6-Adresse und die Portnummer an. Security Agents, die von Vulnerability Scanner installiert wurden, berichten an diesen Server. 3. Konfigurieren Sie die Anmeldedaten , die zur Anmeldung bei den Clients verwendet werden sollen, indem Sie auf **Konto installieren** klicken. Geben Sie im Fenster **Kontoinformationen** einen Benutzernamen und ein Kennwort ein und klicken Sie auf **OK**.

Per E-Mail-Benachrichtigung installieren

Wählen Sie diese Installationsmethode, um eine E-Mail mit einem Link zum Installationsprogramm zu senden.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Klicken Sie auf **Geräte hinzufügen**.
3. Wählen Sie unter **Computertyp** die Option **Desktop oder Server** aus.
4. Wählen Sie im Bereich **Methode** die Option **Installation über E-Mail-Benachrichtigung** aus.
5. Klicken Sie auf **Weiter**.

   Ein neues Fenster wird angezeigt.
6. Geben Sie einen Betreff und die Empfänger der E-Mail ein.
7. Klicken Sie auf **Übernehmen**. Der Standard-Mail-Client wird geöffnet mit Empfängern, Betreff und dem Link zum Installer.

Migration zum Security Agent

Bei der Installation des Security Agents wird geprüft, ob auf dem Client Endpunkt-Sicherheitssoftware von Trend Micro oder Fremdherstellern installiert ist.

Folgende Aktionen können durchgeführt werden:

- Andere Endpunkt-Sicherheitssoftware entfernen, die aktuell auf dem Client installiert ist, und sie mit dem Security Agent ersetzen.
- Andere Endpunkt-Sicherheitssoftware erkennen, aber nicht entfernen.

Eine vollständige Liste der Endpunkt-Sicherheitssoftware finden Sie auf der folgenden Website:

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

Falls die Software auf dem Client nicht automatisch entfernt oder nur erkannt, aber nicht entfernt werden kann, müssen Sie sie zunächst manuell deinstallieren. Je nach Deinstallationsverfahren der Software muss der Client nach der Deinstallation unter Umständen neu gestartet werden.

Migrationsprobleme und Lösungsmöglichkeiten

Auf folgenden Gründen kann die automatische Deinstallation von Endpunkt-Sicherheitssoftware von Fremdherstellern möglicherweise fehlschlagen:

- Die Versionsnummer oder der Produktschlüssel der Software des anderen Anbieters ist ungültig.
- Das Deinstallationsprogramm für die Software des anderen Anbieters funktioniert nicht.
- Bestimmte Dateien der Software des anderen Anbieters fehlen oder sind beschädigt.
- Der Registrierungsschlüssel für die Software des anderen Anbieters kann nicht gelöscht werden.
- Es gibt kein Deinstallationsprogramm für die Software des anderen Anbieters.

Lösungsmöglichkeiten für diese Probleme:

- Entfernen Sie die Software des anderen Anbieters manuell.
- Beenden Sie den Dienst für die Software des anderen Anbieters.
- Beenden Sie den Dienst oder den Prozess für die Software des anderen Anbieters.

Aufgaben nach der Installation auf Security Agents durchführen

Prozedur

1. Überprüfen Sie Folgendes:
   - Die Security Agent-Verknüpfungen werden im Windows Start-Menü auf dem Endpunkt angezeigt.
   - **Trend Micro Worry-Free Business Security Agent** wird in der Liste Software in der Systemsteuerung auf dem Endpunkt aufgeführt.
   - Der Security Agent wird auf der Webkonsole im Fenster **Geräte** angezeigt und in der Gruppe **Server (Standard)** oder **Desktops (Standard)** gruppiert, je nach Betriebssystemtyp des Endpunkts.

     Hinweis

     Wenn der Security Agent nicht angezeigt wird, führen Sie unter **Administration** > **Allgemeine Einstellungen** > **System (Registerkarte)** > **Agentenverbindungsüberprüfung** eine Verbindungsüberprüfung durch.

   - Die folgenden Security Agent Dienste werden in der **Microsoft Management Console** aufgeführt:
     - Trend Micro Security Agent Listener (`tmlisten.exe`)
     - Trend Micro Security Agent RealTime Scan (`ntrtscan.exe`)

- Trend Micro Security Agent Firewall (`TmPfw.exe`), wenn die Firewall bei der Installation aktiviert wurde
- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`), wenn die Verhaltensüberwachung oder Gerätesteuerung während der Installation aktiviert wurde
- Trend Micro Common Client Solution Framework (`TmCCSF.exe`)

2. Wenn der Security Agent nicht auf der Webkonsole erscheint, konnte er seinen Status möglicherweise nicht an den Server senden. Führen Sie einen der folgenden Schritte durch:

- Öffnen Sie einen Webbrowser auf dem Client, geben Sie `https://{Name des Trend Micro Security Servers}:{Portnummer}/SMB/cgi/cgionstart.exe` in das Adressfeld ein, und drücken Sie dann die Eingabetaste.

  Wenn im nächsten Fenster -2 angezeigt wird, kann der Agent mit dem Server kommunizieren. Daran lässt sich auch erkennen, dass das Problem möglicherweise an der Serverdatenbank liegt, wenn darin kein Eintrag für den Agent erstellt wurde.

- Überprüfen Sie mit Hilfe von Ping und Telnet, ob Client und Server miteinander kommunizieren können.
- Falls Sie nur über eine begrenzte Bandbreite verfügen, sollten Sie überprüfen, ob dadurch eine Verbindungszeitüberschreitung zwischen Server und Client verursacht wird.
- Überprüfen Sie, ob die Berechtigungen für den Ordner `\PCCSRV` auf dem Server freigegeben wurden und ob allen Benutzern Vollzugriff erteilt wurde.
- Überprüfen Sie die Proxy-Einstellungen des Trend Micro Security Servers auf ihre Richtigkeit.

3. Testen Sie den Security Agent mit dem EICAR-Testskript.

Das Europäische Institut für Computervirenforschung (EICAR) hat einen Testvirus entwickelt, mit dem Sie Ihre Installation und Konfiguration

testen können. Bei dieser Datei handelt es sich um eine inaktive Textdatei, deren Binär-Pattern in den Viren-Pattern-Dateien der meisten Hersteller von Antiviren-Software enthalten ist. Diese Datei ist kein Virus und enthält keinen Programmcode.

Sie können den EICAR-Testvirus über einen der folgenden Links herunterladen:

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

Sie können den EICAR-Testvirus auch selbst erstellen, indem Sie den folgenden Text in eine Textdatei eingeben und die Datei "eicar.com" nennen:

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

Hinweis

Leeren Sie den Zwischenspeicher des Proxy-Servers und des lokalen Browsers, bevor Sie den Test ausführen.

Messaging Security Agent - Installation

Sie können Messaging Security Agents nur mit der Advanced-Version von Worry-Free Business Security installieren.

Führen Sie eine Neuinstallation des Messaging Security Agents auf Microsoft Exchange Servern durch.

Hinweis

Informationen zum Upgrade der Messaging Security Agents finden Sie im Installations- und Upgrade-Handbuch.

Voraussetzungen für die Installation des Messaging Security Agents

Eine vollständige Liste der Voraussetzungen für die Installation finden Sie auf der folgenden Website:

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

Messaging Security Agent installieren (nur Advanced)

Vorbereitungen

Hinweise zur Installation und Erinnerung:

- Die Microsoft Exchange-Dienste müssen weder vor noch nach der Installation angehalten oder neu gestartet werden.
- Der Messaging Security Agent kann nicht erfolgreich installiert werden, wenn auf dem Endpunkt Informationen zu einer vorherigen Messaging Security Agent-Installation vorhanden sind. Mit der Windows-Systemsteuerung können Sie Überreste einer früheren Installation entfernen.

  Weitere Informationen hierzu finden Sie unter *Messaging Security Agent vom Microsoft Exchange Server deinstallieren (nur Advanced) auf Seite 3-44*.
- Bei Installation des Messaging Security Agent auf einem Server, auf dem Lockdown-Tools ausgeführt werden, entfernen Sie das Lockdown-Tool, damit es den IIS Dienst nicht deaktiviert und die Installation nicht fehlschlägt.
- Der Messaging Security Agent kann außerdem während der Installation des Security Servers installiert werden. Weitere Informationen finden Sie im Installations- und Upgrade-Handbuch.
- Der Messaging Security Agent unterstützt einige Funktionen von Microsoft Exchange Server Enterprise nicht, wie beispielsweise die Datenverfügbarkeitsgruppe (Data Availability Group, DAG).

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Klicken Sie auf **Geräte hinzufügen**.
3. Wählen Sie **Exchange Server** aus.
4. Geben Sie unter **Exchange Server Daten** folgende Daten ein:
   - **Server name**: Der Name des Microsoft Exchange Servers, auf dem Sie den Agent installieren wollen.
   - **Konto**: Der Benutzername des integrierten Domänenadministratorkontos.
   - **Kennwort**: Das Kennwort des integrierten Domänenadministratorkontos.
5. Klicken Sie auf **Weiter**.

   Je nach erforderlicher Installationsart zeigt der Installationsassistent ein entsprechendes Fenster an.

   - **Erstinstallation**: Der Agent ist nicht auf dem Microsoft Exchange Server vorhanden und wird installiert.
   - **Upgrade**: Eine frühere Version des Agents ist auf dem Microsoft Exchange Server vorhanden und es wird ein Upgrade auf die aktuelle Version durchgeführt.
   - **Keine Installation erforderlich**: Die aktuelle Version des Microsoft Exchange Servers ist auf dem Agent vorhanden. Falls der Agent zurzeit nicht in der Sicherheitsgruppenansicht angezeigt wird, wird er automatisch hinzugefügt.
   - **Ungültig**: Es liegt ein Problem mit der Installation des Agents vor.

   Hinweis

   Für die **Art der Spam-Verwaltung** wird die **End User Quarantine** verwendet.

6. Ändern oder akzeptieren Sie unter **Verzeichnisse** das Standardzielverzeichnis und die Standardfreigabeverzeichnisse für die Messaging Security Agent Installation. Das Standardzielverzeichnis und die Standardfreigabeverzeichnisse sind `C:\Programme\Trend Micro\Messaging Security Agent` oder `C$`.
7. Klicken Sie auf **Weiter**.

   Es öffnet sich ein neues Fenster.
8. Bestätigen Sie die Einstellungen des Microsoft Exchange Servers, die Sie in den vorherigen Fenstern eingegeben haben, und klicken Sie dann auf **Weiter**, um die Installation zu starten.
9. Um den Status der Installation anzuzeigen, klicken Sie auf die Registerkarte **Live-Status**.

Agents entfernen

Der Befehl **Agent deinstallieren** bietet die folgenden Möglichkeiten, Security Agents und Messaging Security Agents (nur Advanced) zu entfernen:

- *Agents aus der Webkonsole entfernen auf Seite 3-41*

  Verwenden Sie diese Option für inaktive Agents. Ein inaktiver Agent wird in der Webkonsole ständig als offline angezeigt, da der Client, auf dem der Agent installiert ist, ggf. für längere Zeit ausgeschaltet oder neu formatiert wurde, bevor der Agent deinstalliert werden konnte.

  Wenn Sie Agents über die Webkonsole entfernen, beachten Sie Folgendes:

  - Der Agent, falls dieser auf dem Client noch vorhanden ist, wird nicht nicht deinstalliert.
  - Der Server verwaltet den Agent nicht mehr.
  - Wenn der Agent wieder mit dem Server kommuniziert (z. B. nach dem Einschalten des Clients), wird der Agent wieder in der

Webkonsole hinzugefügt. Ein Security Agent übernimmt die Einstellungen seiner ursprünglichen Gruppe. Wenn die Gruppe nicht mehr besteht, wird der Agent je nach Betriebssystem des Clients unter **Server (Standard)** oder **Desktops (Standard)** eingeordnet und übernimmt die Einstellungen dieser Gruppe.

Tipp

WFBS bietet eine weitere Funktion, die nach inaktiven Agents in der Webkonsole sucht und diese entfernt. Verwenden Sie diese Funktion, um das Entfernen von Agents zu automatisieren. Um diese Funktion zu verwenden, navigieren Sie zur Registerkarte **Administration** > **Allgemeine Einstellungen** > **System** und wählen Sie den Bereich 'Inaktive Security Agents entfernen' aus.

- *Agents über die Webkonsole deinstallieren auf Seite 3-42*

  Sie können den Agent deinstallieren (und somit aus der Webkonsole entfernen), wenn Probleme mit dem Agent-Programm auftreten. Trend Micro empfiehlt eine sofortige Neuinstallation des Agents, um den Client weiterhin vor Bedrohungen zu schützen.

Agents aus der Webkonsole entfernen

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Um Security Agents zu entfernen, wählen Sie eine Gruppe und anschließend die Agents aus. Um einen Messaging Security Agent zu entfernen, wählen Sie ihn aus.

Tipp

Um mehrere aufeinanderfolgende Security Agents auszuwählen, klicken Sie auf den ersten Agent des Bereichs. Halten Sie die Umschalttaste gedrückt und klicken Sie dann auf den letzten Agent des Bereichs. Um mehrere nicht unmittelbar aufeinanderfolgende Agents auszuwählen, klicken Sie auf den ersten Agent des Bereichs. Halten Sie die STRG-Taste gedrückt und klicken Sie dann auf die Agents, die Sie auswählen möchten.

3. Klicken Sie auf **Weitere Optionen** > **Agent deinstallieren**.

   Ein neues Fenster wird angezeigt.

4. Klicken Sie auf **Ausgewählte Agents entfernen**.

5. Klicken Sie auf **Übernehmen**.

Agents über die Webkonsole deinstallieren

Wenn Sie den Messaging Security Agent deinstallieren, werden der IIS Admin-Dienst/Apache Server und alle zugehörigen Dienste automatisch beendet und neu gestartet.

Prozedur

1. Navigieren Sie zu **Geräte**.

2. Um Security Agents zu deinstallieren, wählen Sie eine Gruppe und anschließend die Agents aus. Um einen Messaging Security Agent zu deinstallieren, wählen Sie ihn aus.

   Tipp

   Um mehrere aufeinanderfolgende Security Agents auszuwählen, klicken Sie auf den ersten Agent des Bereichs. Halten Sie die Umschalttaste gedrückt und klicken Sie dann auf den letzten Agent des Bereichs. Um mehrere nicht unmittelbar aufeinanderfolgende Agents auszuwählen, klicken Sie auf den ersten Agent des Bereichs. Halten Sie die STRG-Taste gedrückt und klicken Sie dann auf die Agents, die Sie auswählen möchten.

3. Klicken Sie auf **Weitere Optionen** > **Agent deinstallieren**.

   Ein neues Fenster wird angezeigt.

4. Klicken Sie auf **Ausgewählte Agents deinstallieren**.

5. Klicken Sie auf **Übernehmen**.

Eine Meldung mit der Anzahl der vom Server gesendeten Deinstallationsbenachrichtigungen und der Anzahl der die Benachrichtigung empfangenden Agents wird angezeigt.

Hinweis

Geben Sie bei einem Messaging Security Agent den jeweiligen Kontonamen und das Kennwort für den Microsoft Exchange Server ein, wenn Sie dazu aufgefordert werden.

6. Klicken Sie auf **OK**.
7. Um zu überprüfen, ob der Agent deinstalliert wurde, aktualisieren Sie das Fenster Sicherheitseinstellungen. Der Agent sollte nicht mehr in der Sicherheitsgruppenansicht angezeigt werden.

Security Agent von Endpunkt deinstallieren

Abhängig von Ihrer Konfiguration kann zur Deinstallation eventuell ein Kennwort erforderlich sein. Stellen Sie sicher, falls ein Kennwort erforderlich ist, dass Sie dieses nur solchen Benutzern mitteilen, die das Deinstallationsprogramm ausführen, und ändern Sie das Kennwort sofort, nachdem es an andere Benutzer weitergegeben wurde.

Das Kennwort kann unter **Administration** > **Allgemeine Einstellungen** > **Registerkarte Desktop/Server** > **Security Agent Deinstallationskennwort** festgelegt oder deaktiviert werden.

Prozedur

1. Klicken Sie auf **Systemsteuerung** > **Software**.
2. Suchen Sie **Trend Micro Worry-Free Business Security Agent**, und klicken Sie auf **Ändern** oder **Deinstallieren** – je nach Verfügbarkeit.
3. Folgen Sie den Anweisungen.
4. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort für die Deinstallation ein.

Der Security Server informiert den Benutzer über den Fortschritt und Abschluss der Deinstallation. Der Client muss zum Abschluss der Deinstallation nicht neu gestartet werden.

Messaging Security Agent vom Microsoft Exchange Server deinstallieren (nur Advanced)

Wenn Sie den Messaging Security Agent deinstallieren, werden der IIS Admin-Dienst/Apache Server und alle zugehörigen Dienste automatisch beendet und neu gestartet.

Prozedur

1. Melden Sie sich mit Administratorberechtigungen am Microsoft Exchange Server an.
2. Klicken Sie auf **Systemsteuerung** > **Programm deinstallieren**.
3. Suchen Sie **Trend Micro Messaging Security Agent**, und klicken Sie auf **Ändern**.
4. Folgen Sie den Anweisungen.

Kapitel 4

Geräte verwalten

Worry-Free Business Security unterteilt das Fenster **Geräte** in zwei Hauptabschnitte.

- Gerätestruktur

  Die Gerätestruktur ist eine erweiterbare Liste logischer Gruppen. Sie können Gruppen basierend auf dem Endpunkttyp verwalten. Sie haben auch die Möglichkeit, Gruppen manuell einzurichten und Security Agents gemäß Ihren Anforderungen anzuordnen.

  Weitere Informationen hierzu finden Sie unter *Gerätestruktur verwenden auf Seite 4-2*.

- Tabelle Gruppeninformationen

  Wenn Sie in der Gerätestruktur eine Gruppe auswählen, wird eine Liste mit den Security Agents in der Gruppe im rechten Fensterbereich angezeigt.

  Weitere Informationen hierzu finden Sie unter *Gerätebefehle verwenden auf Seite 4-5*.

Gerätestruktur verwenden

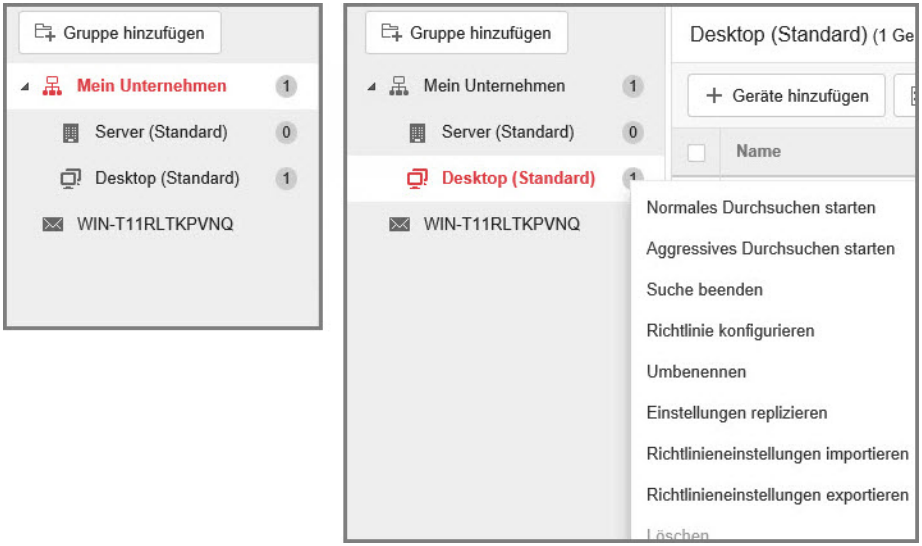


ABBILDUNG 4-1. Menü 'Gerätestrukturbefehle' verwenden

Gehen Sie folgendermaßen vor, um das Menü 'Gerätestruktur' zu öffnen:

- Wählen Sie eine Gruppe aus der Gerätestruktur aus und klicken Sie auf das Zahnradsymbol neben dem Gruppennamen.
- Wählen Sie einen Messaging Security Agent aus und klicken Sie auf das Zahnradsymbol neben dem Namen des Agent.

Je nachdem, welche Art von Gruppe Sie ausgewählt haben, sind einige Befehle nur in bestimmten Gruppentypen verfügbar oder möglicherweise deaktiviert.

TABELLE 4-1. Gerätestrukturbefehle

BEFEHL	BESCHREIBUNG
Gruppe hinzufügen	Fügt eine neue Gruppe zur Gerätestruktur hinzu Weitere Informationen hierzu finden Sie unter *Gruppen hinzufügen auf Seite 4-9*.
Normale Suche starten	• Startet das Durchsuchen aller Endpunkte in der ausgewählten Gruppe • Startet das Durchsuchen des Exchange Servers
Aggressive Suche starten	Startet eine erweiterte Suche auf allen Endpunkten in der ausgewählten Gruppe, um Bedrohungen, die bei der normalen Suche nicht entfernt werden können, zu analysieren und zu bereinigen. **Hinweis** Die Ausführung einer aggressiven Suche wirkt sich möglicherweise auf die Leistung des Endpunkts aus und kann eine höhere Anzahl an Fehlalarmen erzeugen.
Suche beenden	• Beendet das Durchsuchen aller Endpunkte in der ausgewählten Gruppe • Beendet das Durchsuchen des Exchange Servers
Allgemeine Einstellungen konfigurieren	Konfiguriert allgemeine Security Agent-Einstellungen für Sicherheitsüberprüfungen, die Liste mit zulässigen/gesperrten Elementen, Security Agent-Steuerung und Geräteverwaltung. Weitere Informationen hierzu finden Sie unter *Allgemeine Einstellungen auf Seite 11-2*.

Befehl	Beschreibung
Richtlinie konfigurieren	• Konfiguriert die Sicherheitseinstellungen für alle Security Agents in der ausgewählten Gruppe Weitere Informationen hierzu finden Sie unter *Zusammenfassung der grundlegenden Sicherheitseinstellungen für Security Agents auf Seite 5-2*. • Konfiguriert die Sicherheitseinstellungen für den ausgewählten Messaging Security Agent Weitere Informationen hierzu finden Sie unter *Die grundlegenden Sicherheitseinstellungen für Messaging Security Agents (nur Advanced) verwalten auf Seite 6-1*.
Umbenennen	Ändert den Namen der ausgewählten Gruppe
Einstellungen replizieren	Kopiert die Einstellungen von einer Gruppe in eine andere. Die Security Agents in der Zielgruppe übernehmen dann dieselben Einstellungen wie die Quellgruppe. Weitere Informationen hierzu finden Sie unter *Einstellungen replizieren auf Seite 4-18*.
Richtlinieneinstellungen importieren	Importiert die Einstellungen, die von einer anderen Gruppe bezogen wurden Weitere Informationen hierzu finden Sie unter *Einstellungen von Security Agent Gruppen importieren und exportieren auf Seite 4-19*.
Richtlinieneinstellungen exportieren	Exportiert die Einstellungen der ausgewählten Gruppe Weitere Informationen hierzu finden Sie unter *Einstellungen von Security Agent Gruppen importieren und exportieren auf Seite 4-19*.
Löschen	Löscht eine Gruppe aus der Gerätestruktur

Gerätebefehle verwenden

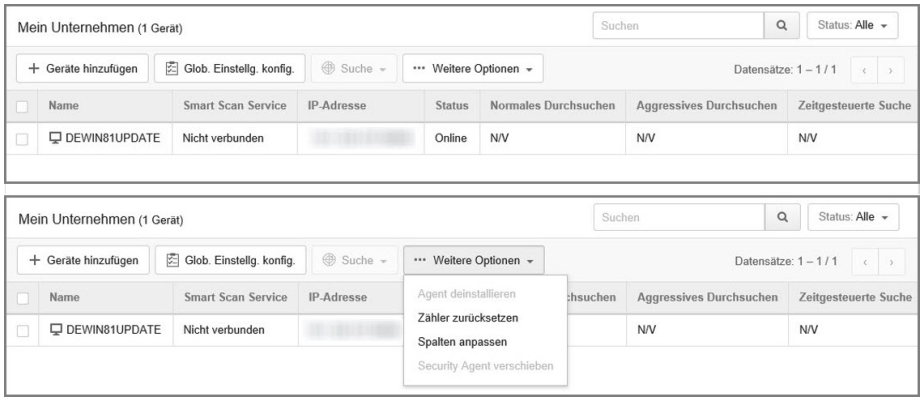


ABBILDUNG 4-2. Menü 'Gerätebefehle' verwenden

Nachdem Sie eine Gruppe aus der Gerätestruktur ausgewählt haben, wird rechts in einer Tabelle eine Liste der Security Agents in der Gruppe angezeigt. Die Menüleiste oben in der Tabelle enthält die Befehle, mit denen Sie die Security Agents verwalten können. Je nachdem, welche Art von Gruppe Sie ausgewählt haben, sind einige Befehle nur in bestimmten Gruppentypen verfügbar oder möglicherweise deaktiviert.

Verwenden Sie die Suchleiste im oberen Bereich des Fensters **Geräte** , um nach Endpunkten anhand von Namen, Kennzeichnungen oder IP-Adressen zu suchen.

Tipp

Um nach Endpunkten innerhalb eines Netzwerks zu suchen, können Sie Teile einer IP-Adresse eingeben. Zum Beispiel würde die Suche nach '192' alle IP-Adressen, in denen '192' enthalten ist, zurückgeben, und '192.' würde alle IP-Adressen zurückgeben, die mit '192' beginnen. Allerdings können Platzhalterzeichen und Sonderzeichen (*, +, (,), -, &) nicht für die Suche nach Endpunktnamen verwendet werden.

TABELLE 4-2. Gerätebefehle

BEFEHL	BESCHREIBUNG
Geräte hinzufügen	Nehmen Sie eine der folgenden Installationen vor: • **Security Agent** auf einem Endpunkt (Desktop oder Server) • **Messaging Security Agent** auf Microsoft Exchange Server (nur Advanced) Weitere Informationen hierzu finden Sie unter *Agents zu Gruppen hinzufügen auf Seite 4-7*.
Richtlinie konfigurieren	Konfiguriert die Sicherheitseinstellungen für alle Security Agents in der ausgewählten Gruppe Weitere Informationen hierzu finden Sie unter *Zusammenfassung der grundlegenden Sicherheitseinstellungen für Security Agents auf Seite 5-2*.
Normale Suche starten	Startet das Durchsuchen der ausgewählten Endpunkte
Aggressive Suche starten	Startet eine erweiterte Suche auf allen Endpunkten in der ausgewählten Gruppe, um Bedrohungen, die bei der normalen Suche nicht entfernt werden können, zu analysieren und zu bereinigen. **Hinweis** Die Ausführung einer aggressiven Suche wirkt sich möglicherweise auf die Leistung des Endpunkts aus und kann eine höhere Anzahl an Fehlalarmen erzeugen.
Suche beenden	Beendet das Durchsuchen der ausgewählten Endpunkte
Agent deinstallieren	Entfernt den Security Agent von den ausgewählten Endpunkten. Weitere Informationen hierzu finden Sie unter *Agents entfernen auf Seite 3-40*.
Zähler zurücksetzen	Für alle Security Agents im Netzwerk werden die Zähler für die Erkennung von Sicherheitsrisiken zurückgesetzt. Protokolle, die sich auf die Informationen beziehen, sind weiterhin über die Protokollabfrage verfügbar.

Befehl	Beschreibung
Spalten anpassen	Wählt die Spalten für die Anzeige in der Tabelle aus Weitere Informationen hierzu finden Sie unter *Spalten der Geräteliste anpassen auf Seite 4-9*.
Security Agent verschieben	Verschieben Sie die ausgewählten Security Agents in eine andere Gruppe oder auf einen anderen Security Server. Weitere Informationen hierzu finden Sie unter *Agents verschieben auf Seite 4-12*.

Agents zu Gruppen hinzufügen

Nachdem ein Agent installiert wurde und an den Security Server berichtet, fügt der Server ihn zu einer Gruppe hinzu.

- Auf Server-Plattformen installierte Security Agents werden der Gruppe **Server (Standard)** hinzugefügt.
- Auf Desktop-Plattformen installierte Security Agents werden der Gruppe **Desktops (Standard)** hinzugefügt.

Hinweis

Um Security Agents anderen Gruppen zuzuweisen, können Sie sie verschieben. Weitere Informationen finden Sie unter *Agents verschieben auf Seite 4-12*.

- Jeder Messaging Security Agent (nur Advanced) bildet seine eigene Gruppe. Mehrere Messaging Security Agents können nicht in einer Gruppe organisiert werden.

Falls die Anzahl der Agents in der Sicherheitsgruppenansicht falsch ist, wurden eventuell Agents entfernt, ohne dass der Server benachrichtigt wurde (wenn während der Entfernung des Agents beispielsweise die Kommunikation zwischen Server und Client unterbrochen wurde). Dadurch behält der Server die Agent-Informationen in seiner Datenbank und zeigt den Agent in der Webkonsole als offline an. Wenn Sie den Agent erneut

installieren, erstellt der Server einen neuen Datensatz in der Datenbank und behandelt den Agent als neuen Eintrag, sodass in der Sicherheitsgruppenansicht Duplikate angezeigt werden. Verwenden Sie die Funktion Agentenverbindungsüberprüfung in **Administration** > **Allgemeine Einstellungen** > **System**, um die Datenbank nach doppelt eingetragenen Agents zu durchsuchen.

Security Agents installieren

Siehe folgende Themen:

- *Voraussetzungen für die Installation des Security Agents auf Seite 3-2*
- *Überlegungen zur Installation des Security Agents auf Seite 3-2*
- *Installationsmethoden für den Security Agent auf Seite 3-7*
  - *Installation über die interne Webseite auf Seite 3-9*
  - *Mit dem Anmeldeskript-Setup installieren auf Seite 3-12*
  - *Mit Client Packager installieren auf Seite 3-14*
  - *Mit Remote-Installation installieren auf Seite 3-18*
  - *Mit dem Vulnerability Scanner installieren auf Seite 3-22*
  - *Per E-Mail-Benachrichtigung installieren auf Seite 3-33*
- *Aufgaben nach der Installation auf Security Agents durchführen auf Seite 3-35*

Messaging Security Agents installieren (nur Advanced)

Siehe folgende Themen:

- *Voraussetzungen für die Installation des Messaging Security Agents auf Seite 3-38*
- *Messaging Security Agent installieren (nur Advanced) auf Seite 3-38*

Gruppen hinzufügen

Fügen Sie eine Server-Gruppe oder eine Desktop-Gruppe hinzu, die einen oder mehrere Security Agents enthalten kann.

Das Hinzufügen einer Gruppe, die Messaging Security Agents enthält, ist nicht möglich. Wenn ein Messaging Security Agent installiert wurde und dem Security Server berichtet, wird er automatisch als eigene Gruppe in der **Sicherheitsgruppenansicht** angezeigt.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Klicken Sie auf **Gruppe hinzufügen**.

   Ein neues Fenster wird angezeigt.
3. Wählen Sie einen Gruppentyp aus.
   - **Desktops**
   - **Server**
4. Geben Sie den Namen für die Gruppe ein.
5. Klicken Sie auf **Einstellungen importieren von Gruppe** und wählen Sie anschließend die Gruppe aus, um die Einstellungen einer vorhandenen Gruppe auf die neue Gruppe anzuwenden. Es werden nur Gruppen für den ausgewählten Gruppentyp angezeigt.
6. Klicken Sie auf **Speichern**.

Spalten der Geräteliste anpassen

Sie können die anzuzeigenden Spalten auswählen, indem Sie oben in der Geräteliste auf **Weitere Optionen** > **Spalten anpassen** klicken.

Spalte	Angezeigte Informationen
Für Security Agents	
Client	
IP-Adresse	IP-Adresse des Clients, auf dem der Agent installiert ist
Status	• **Online**: Der Agent ist mit dem Security Server verbunden. • **Offline**: Der Agent ist vom Security Server getrennt.
Agent-Version	Agent-Version
Betriebssystem	Betriebssystem des Clients, auf dem der Agent installiert ist
Architektur	• **x64**: 64-Bit-Betriebssystem • **x86**: 32-Bit-Betriebssystem
Exchange-Version	Microsoft Exchange server version
Suche	
Smart Scan Service **Hinweis** Diese Spalte wird nur angezeigt, wenn als Suchmethode Smart Scan verwendet wird.	• **Verbunden**: Der Agent ist mit dem Smart Scan Service verbunden. • **Nicht verbunden**: Der Agent ist nicht mit dem Smart Scan Service verbunden. **Hinweis** Der Smart Scan Service wird auf dem Security Server gehostet. Falls die Verbindung mit einem Agent getrennt wird, kann sich dieser nicht mit dem Security Server verbinden oder der Smart Scan Service ist nicht funktionsfähig (z. B. wenn der Service angehalten wurde). • **Deaktiviert**: Der Agent verwendet die herkömmliche Suche
Agent-Pattern von Smart Scan/Viren-Pattern	Version der Agent-Pattern von Smart Scan/Viren-Pattern
Zeitgesteuerte Suche	Datum und Uhrzeit der letzten zeitgesteuerten Suche

Spalte	Angezeigte Informationen
Aggressives Durchsuchen	Datum und Uhrzeit der letzten aggressiven Suche
POP3 Mail Scan	• **Aktiviert** • **Deaktiviert**
Suchmethode	• **Smart**: Lokale und internetbasierte Suchen • **Herkömmlich**: Nur lokale Suchen Weitere Informationen finden Sie unter *Suchmethoden auf Seite 5-3*.
Normales Durchsuchen	Datum und Uhrzeit der letzten normalen Suche
Bedrohung	
Entdeckte Viren	Anzahl der entdeckten Viren/Malware
Entdeckte Spyware	Anzahl der gefundenen Spyware/Grayware
Entdeckter Spam	Anzahl der Spam-E-Mails
URLs, gegen die verstoßen wurde	Anzahl der verbotenen URLS, auf die zugegriffen wurde
Viren-Engine	Viren-Scan-Engine-Version
Für Messaging Security Agents (nur Advanced)	
Name	Host-Name des Clients, auf dem der Agent installiert ist
IP-Adresse	IP-Adresse des Clients, auf dem der Agent installiert ist
Online/Offline	• **Online**: Der Agent ist mit dem Security Server verbunden. • **Offline**: Der Agent ist vom Security Server getrennt.
Betriebssystem	Betriebssystem des Clients, auf dem der Agent installiert ist
Architektur	• **x64**: 64-Bit-Betriebssystem • **x86**: 32-Bit-Betriebssystem
Exchange-Version	Microsoft Exchange server version

Spalte	Angezeigte Informationen
Viren-Pattern	Version der Viren-Pattern-Datei
Viren-Engine	Viren-Scan-Engine-Version
Agent-Version	Agent-Version

Agents verschieben

Es gibt mehrere Möglichkeiten, um Agents zu verschieben.

Zu verschiebender Agent	Details	So verschieben Sie Agents
Security Agent	Verschieben Sie Security Agents zwischen Gruppen. Nach der Verschiebung übernimmt der Agent automatisch die Einstellungen der neuen Gruppe.	Verwenden Sie die Webkonsole, um einen oder mehrere Agents zu verschieben. Weitere Informationen finden Sie unter *Security Agents zwischen Gruppen verschieben auf Seite 4-14*.
	Falls Sie mindestens zwei Security Server besitzen, können Sie Security Agents zwischen Servern verschieben. Nach der Verschiebung wird der Agent unter der Gruppe **Desktops (Standard)** oder **Server (Standard)** auf dem anderen Security Server gruppiert, abhängig vom Betriebssystem des Clients. Der Agent übernimmt die Einstellungen der neuen Gruppe automatisch.	• Verwenden Sie die Webkonsole, um einen oder mehrere Agents zu verschieben. Weitere Informationen finden Sie unter *Agents mit der Webkonsole zwischen Security Servern verschieben auf Seite 4-14*. • Führen Sie das Tool Client Mover auf einem Client aus, um den Agent zu verschieben, der auf diesem Client installiert ist. Weitere Informationen finden Sie unter *Einen Security Agent mit Client Mover zwischen Security Servern verschieben auf Seite 4-16*.
Messaging Security Agent (nur Advanced)	Falls Sie mindestens zwei Security Server besitzen, können Sie Messaging Security Agents zwischen Servern verschieben. Nach der Verschiebung bildet der Agent eine eigene Gruppe auf dem anderen Security Server und behält seine Einstellungen bei.	Verwenden Sie die Webkonsole, um Agents nacheinander zu verschieben. Weitere Informationen finden Sie unter *Agents mit der Webkonsole zwischen Security Servern verschieben auf Seite 4-14*.

Security Agents zwischen Gruppen verschieben

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Wählen Sie die Agents, die Sie verschieben möchten.

   Tipp

   Um mehrere aufeinanderfolgende Security Agents auszuwählen, klicken Sie auf den ersten Agent des Bereichs. Halten Sie die Umschalttaste gedrückt und klicken Sie dann auf den letzten Agent des Bereichs. Um mehrere nicht unmittelbar aufeinanderfolgende Agents auszuwählen, klicken Sie auf den ersten Agent des Bereichs. Halten Sie die STRG-Taste gedrückt und klicken Sie dann auf die Agents, die Sie auswählen möchten.

4. Verschieben Sie die Agents mit Drag & Drop in die neue Gruppe.

Agents mit der Webkonsole zwischen Security Servern verschieben

Vorbereitungen

Wenn Sie einen Agent zwischen Security Servern verschieben, gilt Folgendes:

- Wenn ein Agent, der eine frühere Version ausführt, auf einen Security Server mit der aktuellsten Version verschoben wird, wird der Agent automatisch aktualisiert.
- Verschieben Sie Agents mit der aktuellen Version nicht auf Security Server, die eine frühere Version ausführen, da der Agent dadurch nicht verwaltet wird (der Agent wird sich bei seinem früheren Server abmelden, kann sich jedoch nicht beim neuen Server anmelden und wird daher in keiner Webkonsole angezeigt). Der Agent behält seine aktuelle Version bei und es erfolgt kein Downgrade.

- Die Security Server müssen dieselbe Spracheinstellung haben.
- Notieren Sie den Host-Namen und den Listening-Port des Security Servers, auf den der Agent verschoben wird. Den Host-Namen und Listening-Port finden Sie im Fenster Sicherheitseinstellungen des Security Servers über dem Bereich Aufgaben.

Prozedur

1. Gehen Sie auf der Webkonsole des Security Servers, der den Agent aktuell verwaltet, zu **Geräte**.
2. Wählen Sie eine Gruppe und anschließend die Agents aus, um Security Agents zu verschieben. Wählen Sie einen Messaging Security Agent aus, um ihn zu verschieben.
3. Klicken Sie auf **Weitere Optionen** > **Security Agent verschieben**.

   Ein neues Fenster wird angezeigt.
4. Geben Sie den Host-Namen und den Listening-Port des Security Servers ein, auf den der Agent verschoben wird.
5. Klicken Sie auf **Verschieben**.
6. Öffnen Sie die Webkonsole des neuen Servers und suchen Sie die Agents in der Sicherheitsgruppenansicht, um zu überprüfen, dass die Agents ab sofort dem neuen Security Server berichten.

   Hinweis

   Wenn der Security Agent nicht in der Sicherheitsgruppenansicht angezeigt wird, starten Sie den Trend Micro Security Server Master Service neu.

Einen Security Agent mit Client Mover zwischen Security Servern verschieben

Vorbereitungen

Wenn Sie einen Agent zwischen Security Servern verschieben, gilt Folgendes:

- Wenn ein Agent, der eine frühere Version ausführt, auf einen Security Server mit der aktuellsten Version verschoben wird, wird der Agent automatisch aktualisiert.
- Verschieben Sie Agents mit der aktuellen Version nicht auf Security Server, die eine frühere Version ausführen, da der Agent dadurch nicht verwaltet wird (der Agent wird sich bei seinem früheren Server abmelden, kann sich jedoch nicht beim neuen Server anmelden und wird daher in keiner Webkonsole angezeigt). Der Agent behält seine aktuelle Version bei und es erfolgt kein Downgrade.
- Die Security Server müssen dieselbe Spracheinstellung haben.
- Notieren Sie den Host-Namen und den Listening-Port des Security Servers, auf den der Agent verschoben wird. Den Host-Namen und Listening-Port finden Sie im Fenster Sicherheitseinstellungen des Security Servers über dem Bereich Aufgaben.
- Melden Sie sich über ein Administratorkonto beim Client an.

Prozedur

1. Öffnen Sie eine Befehlszeile auf dem Client.

   Hinweis

   Öffnen Sie als Administrator die Eingabeaufforderung.

2. Geben Sie `cd` und den Security Agent-Installationsordner ein. Beispiel: `cd C:\Programme\Trend Micro\Security Agent`
3. Führen Sie Client Mover aus, indem Sie folgende Syntax verwenden:

```
<Name der ausführbaren Datei> -s <Servername> -p <Server-Listening-Port> -c <Client-Listening-Port> -pwd <Kennwort für Agent-Berechtigung 'Entladen und Entsperren'>
```

TABELLE 4-3. Client Mover Parameter

PARAMETER	ERKLÄRUNG
`<Name der ausführbaren Datei>`	`IpXfer.exe` (32 Bit) `IpXfer_x64.exe` (64 Bit)
`<Server-Name>`	Der Name des Worry-Free Business Security Zielservers (der Server, auf den der Agent übertragen werden soll).
`<Server-Listening-Port>`	Der Listening-Port (oder der vertrauenswürdige Port) des Security Servers.
`<Client-Listening-Port>`	Die Portnummer, die vom Security Agent zur Kommunikation mit dem Server verwendet wird.
`<Kennwort für Agent-Berechtigung 'Entladen und Entsperren'>`	Das zum Entladen und Entsperren des Security Agents verwendete Kennwort

Beispiel:

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

4. Öffnen Sie die Webkonsole des neuen Servers und suchen Sie den Agent in der Sicherheitsgruppenansicht, um zu überprüfen, dass der Security Agent ab sofort dem neuen Security Server berichten.

Hinweis

Wenn der Security Agent nicht in der Sicherheitsgruppenansicht angezeigt wird, starten Sie den Trend Micro Security Server Master Service neu.

Einstellungen replizieren

Replizieren Sie Einstellungen zwischen Security Agent Gruppen oder zwischen Messaging Security Agents (nur Advanced).

Gruppeneinstellungen von Security Agents replizieren

Übertragen Sie mit dieser Funktion die Einstellungen einer bestimmten Desktop- oder Servergruppe auf eine andere Gruppe des gleichen Typs. Es ist nicht möglich, die Einstellungen einer Servergruppe auf eine Desktopgruppe und umgekehrt zu übertragen.

Wenn es für einen besonderen Gruppentyp nur eine Gruppe gibt, wird diese Funktion deaktiviert.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf das Zahnradsymbol neben dem Namen der Gruppe.
4. Klicken Sie auf **Einstellungen replizieren**.

   Ein neues Fenster wird angezeigt.
5. Wählen Sie die Zielgruppen aus, auf die Sie die Einstellungen übertragen möchten.
6. Klicken Sie auf **Übernehmen**.

Messaging Security Agent-Einstellungen replizieren (nur Advanced)

Sie können nur Einstellungen zwischen Messaging Security Agents replizieren, wenn diese sich in derselben Domäne befinden.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf das Zahnradsymbol neben dem Messaging Security Agent.
4. Klicken Sie auf **Einstellungen replizieren**.

   Ein neues Fenster wird angezeigt.
5. Wählen Sie den Messaging Security Agent aus, auf den Sie die Einstellungen übertragen möchten.
6. Klicken Sie auf **Übernehmen**.
7. Wenn die Replikation fehlschlägt:
   a. Starten Sie den Registrierungs-Editor (regedit).
   b. Gehen Sie zu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`.
   c. Klicken Sie mit der rechten Maustaste auf **winreg** > **Berechtigungen**.
   d. Fügen Sie die **Smex Administratorgruppe** der Zieldomäne hinzu, und aktivieren Sie **Lesezugriff**.

Einstellungen von Security Agent Gruppen importieren und exportieren

Exportieren Sie die Einstellungen einer Desktop- oder einer Server-Gruppe in eine `.DAT`-Datei, um sie zu sichern. Sie können die `.DAT`-Datei auch zum Importieren der Einstellungen in eine andere Gruppe verwenden.

Hinweis

Sie können Einstellungen in Desktop- und Servergruppen importieren oder exportieren. Einstellungen sind nicht abhängig vom Gruppentyp. Abhängig vom Gruppentyp können Sie auch die Funktion **Einstellungen replizieren** verwenden. Weitere Informationen über die Funktion **Einstellungen replizieren** finden Sie unter *Einstellungen replizieren auf Seite 4-18*.

TABELLE 4-4. Einstellungen, die importiert und exportiert werden können

AUSWAHL	FENSTER MIT DEN EINSTELLUNGEN	EINSTELLUNGEN, DIE EXPORTIERT/IMPORTIERT WERDEN KÖNNEN
Desktop-Gruppe ( ) oder Server-Gruppe ( )	Geräte (**Geräte** > **Richtlinie konfigurieren**)	• Virenschutz/Anti-Spyware (Echtzeitsuche) • Vorausschauendes Maschinenlernen • Verhaltensüberwachung • Vertrauenswürdiges Programm • Quarantäne • Web Reputation • URL-Filter • Firewall • Gerätesteuerung • Benutzer-Tools (nur für Desktop-Gruppen verfügbar) • Agent-Berechtigungen
	Manuelle Suche (**Suchen** > **Manuelle Suche**)	Alle Einstellungen
	Zeitgesteuerte Suche (**Suchen** > **Zeitgesteuerte Suche**)	Alle Einstellungen

Einstellungen exportieren

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Server-Gruppe.
3. Klicken Sie auf das Zahnradsymbol neben dem Namen der Gruppe.
4. Klicken Sie auf **Richtlinieneinstellungen exportieren**.

   Ein neues Fenster wird angezeigt.
5. Klicken Sie auf **Exportieren**.

   Ein Dialogfeld wird angezeigt.
6. Klicken Sie auf **Speichern**, navigieren Sie zu Ihrem bevorzugten Speicherort und klicken Sie erneut auf **Speichern**.

Einstellungen importieren

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Server-Gruppe.
3. Klicken Sie auf **Richtlinieneinstellungen importieren**.

   Ein neues Fenster wird angezeigt.
4. Klicken Sie auf **Durchsuchen**, um die Datei zu suchen, und anschließend auf **Importieren**.

Kapitel 5

Grundlegende Sicherheitseinstellungen für Security Agents verwalten

In diesem Kapitel wird die Konfiguration der grundlegenden Sicherheitseinstellungen für Security Agents beschrieben.

Zusammenfassung der grundlegenden Sicherheitseinstellungen für Security Agents

Tabelle 5-1. Zusammenfassung der grundlegenden Sicherheitseinstellungen für Security Agents

Optionen	Beschreibung	Standard
Suchmethode	Sie können konfigurieren, ob die Smart Scan aktiviert ist oder nicht.	Während der Installation wird "Aktiviert" oder "Deaktiviert" ausgewählt.
Virenschutz/Anti-Spyware	Optionen für die Echtzeitsuche, den Virenschutz und Anti-Spyware konfigurieren.	Aktiviert (Echtzeitsuche)
Vorausschauendes Maschinenlernen	Optionen für die Konfiguration von Vorausschauendes Maschinenlernen	Deaktiviert
Verhaltensüberwachung	Optionen für die Verhaltensüberwachung konfigurieren	Für Desktop-Gruppen aktiviert Für Servergruppen deaktiviert
Vertrauenswürdiges Programm	Legen Sie fest, welche Programme nicht auf verdächtiges Verhalten hin überwacht werden müssen.	n. v.
Quarantäne	Den Quarantäne-Ordner angeben	http://<Security Server-Name oder -IP-Adresse>
Web Reputation	Web Reputation Optionen "Im Büro" und "Nicht im Büro" konfigurieren	Im Büro: Aktiviert, Niedrig Nicht im Büro:Aktiviert, Mittel
URL-Filter	URL-Filter sperren Websites, die gegen festgelegte Richtlinien verstoßen.	Aktiviert, Niedrig

Optionen	Beschreibung	Standard
Zulässige/gesperrte URLs	Konfigurieren Sie die Liste der global zulässigen und gesperrten Absender.	Deaktiviert
Firewall	Firewall-Optionen konfigurieren	Deaktiviert
Gerätesteuerung	Konfiguriert automatische Ausführung, USB- und Netzwerkzugriff	Deaktiviert
Benutzer-Tools	Wi-Fi Advisor und Trend Micro Anti-Spam Symbolleiste konfigurieren	Deaktiviert: Wi-Fi Advisor Deaktiviert: Anti-Spam Symbolleiste in unterstützten E-Mail-Clients
Agent-Berechtigungen	Den Zugriff auf Einstellungen von der Agent-Konsole konfigurieren Upgrade des Security Agents und Hotfix-Installation deaktivieren	n. v.

Suchmethoden

Bei der Suche nach Sicherheitsrisiken können Security Agents eine von zwei Suchmethoden anwenden:

- **Smart Scan**: Security Agents, die die Smart Scan anwenden, werden in diesem Dokument als **Agents mit intelligenter Suche** bezeichnet. Smart Scan Agents nutzen die lokale Suche und webbasierte Abfragen, die von File-Reputation-Diensten bereitgestellt werden.
- **Herkömmliche Suche**: Security Agents, die Smart Scan nicht anwenden, werden in diesem Dokument als **Agents zur herkömmlichen Suche** bezeichnet. Agents zur herkömmlichen Suche speichern alle Komponenten auf dem Client und durchsuchen alle Dateien lokal.

Die folgende Tabelle beinhaltet einen Vergleich zwischen den beiden Suchmethoden.

TABELLE 5-2. Vergleich zwischen herkömmlicher Suche und intelligenter Suche

VERGLEICHSGRUNDLAGE	HERKÖMMLICHE SUCHE	SMART SCAN
Suchverhalten	Der Security Agent zur herkömmlichen Suche durchsucht den Client.	• Der Smart Scan-Agent durchsucht den Client. • Wenn der Security Agent das Risiko der Datei während der Suche nicht ermitteln kann, überprüft Security Agent dies, indem er eine Suchabfrage an den Suchserver sendet (bei Security Agents, die mit dem Smart Scan Server verbunden sind) oder das Trend Micro Smart Protection Network (bei Security Agents, die nicht mit dem Smart Scan Server verbunden sind). **Hinweis** Der Scan Server ist ein auf dem Smart Scan Server ausgeführter Dienst. • Der Security Agent legt die Ergebnisse der Suchabfrage zur Verbesserung der Suchleistung in einem Zwischenspeicher ab.
Verwendete und aktualisierte Komponenten	Alle unter der Update-Adressse verfügbaren Security Agent Komponenten, außer das Agent-Pattern von Smart Scan	Alle unter der Update-Adresse verfügbaren Komponenten, außer das Viren-Pattern
Typische Update-Adresse	ActiveUpdate Server	ActiveUpdate Server

Suchmethoden konfigurieren

Vorbereitungen

Wenn Sie den Security Server installiert haben, können Sie Smart Scan aktivieren. Ist Smart Scan aktiviert, wird er von allen Security Agents als Standardsuchmethode verwendet. Andernfalls wird die herkömmliche Suche als Standardsuchmethode verwendet. Sie können je nach den jeweiligen Anforderungen zwischen den Suchmethoden wechseln. Beispiel:

- Wenn die herkömmliche Suche verwendet wird und erst nach langer Zeit abgeschlossen ist, können Sie zu Smart Scan, einer schnelleren und effizienteren Suchmethode, wechseln. Sie sollten auch zu Smart Scan wechseln, wenn der Agent über wenig Speicherplatz auf der Festplatte verfügt. Smart Scan-Agents laden kleinere Pattern herunter, so dass weniger Speicherplatz belegt wird.

  Gehen Sie vor dem Wechsel zu Smart Scan zu **Administration** > **Allgemeine Einstellungen**, klicken Sie auf die Registerkarte **Desktop/Server** und gehen Sie zum Abschnitt **Allgemeine Sucheinstellungen**. Vergewissern Sie sich, dass die Option **Smart Scan Service deaktivieren** deaktiviert ist.

- Verwenden Sie die herkömmliche Suche, wenn Sie einen Leistungsabfall des Security Servers bemerken. Dieser könnte darauf hindeuten, dass der Server nicht alle Suchanfragen der Agents zeitnah bearbeiten kann.

Die folgende Tabelle enthält weitere Überlegungen zum Wechsel zwischen den Suchmethoden:

TABELLE 5-3. Überlegungen zum Wechsel zwischen den Suchmethoden

ÜBERLEGUNG	DETAILS
Security Server-Verbindung	Stellen Sie sicher, dass die Security Agents eine Verbindung zum Security Server aufbauen können. Nur Online-Agents erhalten die Benachrichtigung, zu einer anderen Suchmethode zu wechseln. Offline-Agents erhalten die Benachrichtigung erst dann, wenn sie wieder online gehen. Vergewissern Sie sich auch, dass der Security Server über die neuesten Komponenten verfügt, weil die Agents neue Komponenten vom Security Server herunterladen müssen. Agents, die auf Smart Scan umgeschaltet werden, benötigen das Agent-Pattern von Smart Scan und Agents, die auf die herkömmliche Suche umgeschaltet werden, das Viren-Pattern.
Anzahl der Security Agents, die umgeschaltet werden sollen	Wenn Sie eine relativ kleine Anzahl von Security Agents gleichzeitig umschalten, werden die Ressourcen des Security Servers effizient genutzt. Der Security Server kann andere kritische Aufgaben ausführen, während Agents zwischen den Suchmethoden wechseln.
Timing	Wenn Sie Security Agents zum ersten Mal umschalten, muss zunächst die **Vollversion** des Agent-Pattern von Smart Scan (für Agents, die auf Smart Scan umgeschaltet werden) bzw. des Viren-Pattern (für Agents, die auf die herkömmliche Suche umgeschaltet werden), heruntergeladen werden. Die Umschaltung sollte bei geringem Netzaufkommen durchgeführt werden, um sicherzustellen, dass der Download-Prozess in kurzer Zeit beendet wird. Deaktivieren Sie außerdem vorübergehend die Funktion 'Jetzt aktualisieren', und aktivieren Sie sie wieder, nachdem der Wechsel zwischen den Suchmethoden abgeschlossen ist. **Hinweis** Danach laden die Agents **kleinere, inkrementelle** Versionen des Agent-Pattern von Smart Scan bzw. des Viren-Pattern herunter, sofern sie regelmäßig aktualisiert werden.

Überlegung	Details
IPv6-Unterstützung	Ein reiner IPv6-Smart Scan Agent, der offline ist, kann Abfragen nicht direkt an das Trend Micro Smart Protection Network senden. Ein Dual-Stack-Proxy-Server, der IP-Adressen konvertieren kann wie DeleGate, muss so konfiguriert werden, dass der Smart Scan-Agent Abfragen senden kann.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.
4. Gehen Sie zu **Suchmethode**.
5. Wählen Sie die bevorzugte Suchmethode.
6. Klicken Sie auf **Speichern**.

Echtzeitsuche für Security Agents

Die Echtzeitsuche wird kontinuierlich und dauerhaft ausgeführt. Jedes Mal, wenn eine Datei geöffnet, heruntergeladen, kopiert oder geändert wird, wird sie von der Echtzeitsuche im **Security Agent** auf Bedrohungen durchsucht.

Echtzeitsuche für Security Agents konfigurieren

Prozedur

1. Navigieren Sie zu **Geräte**.

2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.
4. Klicken Sie auf **Virenschutz/Anti-Spyware**.

   Ein neues Fenster wird angezeigt.
5. Wählen Sie **Echtzeitsuche nach Virenschutz/Anti-Spyware aktivieren** aus.
6. Sucheinstellungen konfigurieren. Weitere Informationen finden Sie unter *Suchziele und Aktionen für Security Agents auf Seite 7-10*:

   Hinweis

   Wenn Sie Benutzern Rechte zur Konfiguration ihrer eigenen Sucheinstellungen erteilen, werden diese benutzerdefinierten Einstellungen bei der Suche verwendet.
7. Klicken Sie auf **Speichern**.

Vorausschauendes Maschinenlernen

Das Trend Micro Vorausschauendes Maschinenlernen setzt moderne Technologien ein, um Bedrohungsinformationen zu korrelieren und ausführliche Dateianalysen durchzuführen und so unbekannte neue Sicherheitsrisiken durch digitale DNS-Fingerabdrücke, API-Zuordnung und weitere Funktionen zu erkennen. Beim 'Vorausschauendes Maschinenlernen' wird außerdem eine Verhaltensanalyse für unbekannte Prozesse oder Prozesse mit geringer Prävalenz durchgeführt, um zu ermitteln, ob eine neue oder unbekannte Bedrohung versucht, das Netzwerk zu infizieren.

Beim 'Vorausschauendes Maschinenlernen' handelt es sich um ein leistungsstarkes Tool, mit dem Ihre Umgebung vor unbekannten und Zero-Day-Angriffen geschützt wird.

Fundtyp	Beschreibung
Datei	Nach der Erkennung einer unbekannten oder selten vorkommenden Datei durchsucht der Security Agent die Datei mit Hilfe der Funktion "Fortgeschrittene Bedrohungssuchmaschine", um Dateifunktionen zu extrahieren, und sendet den Bericht an das Modul "Vorausschauendes Maschinenlernen", das im Trend Micro Smart Protection Network gehostet wird. Durch die Verwendung von Malware-Modellen wird beim 'Vorausschauendes Maschinenlernen' das Beispiel mit dem Malware-Modell verglichen, ein Wahrscheinlichkeitswert zugewiesen und der mögliche Malware-Typ ermittelt, der in der Datei enthalten ist. Je nach Konfiguration der Funktion "Vorausschauendes Maschinenlernen" kann der Security Agent versuchen, die betroffene Datei unter „Quarantäne“ zu stellen, um zu verhindern, dass sich die Bedrohung im Netzwerk verbreitet.
Prozess	Nach der Erkennung eines unbekannten oder selten vorkommenden Prozesses überwacht der Security Agent diesen Prozess mit Hilfe der Funktion "Maschine für kontextbezogene Intelligenz" und sendet den Verhaltensbericht an das Modul "Vorausschauendes Maschinenlernen". Durch die Verwendung von verhaltensbezogenen Malware-Modellen wird beim 'Vorausschauendes Maschinenlernen' das Prozessverhalten mit dem Modell verglichen, ein Wahrscheinlichkeitswert zugewiesen und der mögliche Malware-Typ ermittelt, der vom Prozess ausgeführt wird. Je nach Konfiguration der Funktion "Vorausschauendes Maschinenlernen" kann Security Agent den betroffenen Prozess oder das Skript „beenden“ und die Datei bereinigen, die den Prozess oder das Skript ausgeführt hat.

Vorausschauendes Maschinenlernen konfigurieren

Hinweis

Für vorausschauendes Maschinenlernen ist Folgendes erforderlich:

- Aktivieren der Verhaltensüberwachung unter **Richtlinie konfigurieren** > **Verhaltensüberwachung**
- Eine funktionierende Internetverbindung, um eine Verbindung mit dem Smart Protection Network herzustellen

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.
4. Klicken Sie auf **Vorausschauendes Maschinenlernen**.
5. Wählen Sie **Vorausschauendes Maschinenlernen aktivieren** aus.
6. Wählen Sie den Typ der Erkennungen und die zugehörige Aktion aus, die Vorausschauendes Maschinenlernen durchführt.

Erkennungstyp	Aktionen
Datei	• **Quarantäne**: Wählen Sie diese Option aus, um Dateien automatisch unter Quarantäne zu stellen, die basierend auf der Analyse von "Vorausschauendes Maschinenlernen" mit Malware in Verbindung stehende Funktionen aufweisen. • **Nur protokollieren**: Wählen Sie diese Option aus, um unbekannte Dateien zu durchsuchen und die Analyse von "Vorausschauendes Maschinenlernen" zur weiteren internen Überprüfung der Bedrohung zu protokollieren.

Erkennungstyp	Aktionen
Prozess	• **Beenden**: Wählen Sie diese Option aus, um Prozesse oder Skripts automatisch zu beenden, die basierend auf der Analyse von "Vorausschauendes Maschinenlernen" mit Malware in Verbindung stehendes Verhalten aufweisen. **Wichtig** Mit Hilfe der Funktion "Vorausschauendes Maschinenlernen" wird versucht, die Dateien zu bereinigen, die böswillige Prozesse oder Skripts ausgeführt haben. Wenn die Bereinigungsaktion nicht erfolgreich ist, verschiebt "Vorausschauendes Maschinenlernen" die betroffenen Dateien in die Quarantäne. • **Nur protokollieren**: Wählen Sie diese Option aus, um nach unbekannten Prozessen oder Skripts zu suchen und die Analyse von "Vorausschauendes Maschinenlernen" zur weiteren internen Überprüfung der Bedrohung zu protokollieren.

7. Klicken Sie auf **Speichern**.

Verhaltensüberwachung

Security Agents überprüfen Clients ständig auf ungewöhnliche Änderungen im Betriebssystem oder in installierter Software. Administratoren (oder Benutzer) können Ausschlusslisten erstellen, um bestimmte Programme trotz Verstoß gegen eine überwachte Änderung auszuführen oder bestimmte Programme vollständig zu sperren. Außerdem dürfen Programme mit gültiger digitaler Signatur immer gestartet werden.

Eine weitere Funktion der Verhaltensüberwachung besteht darin, zu verhindern, dass .EXE- und .DLL-Dateien gelöscht oder verändert werden. Wenn die Verhaltensüberwachung aktiviert ist, erstellen Benutzer

Ausnahmen, um bestimmte Programme zuzulassen oder zu sperren. Außerdem können Benutzer auswählen, dass alle Intuit QuickBooks-Programme geschützt werden.

Verhaltensüberwachung konfigurieren

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.
4. Klicken Sie auf **Verhaltensüberwachung**.
5. Aktualisieren Sie auf Anforderung folgende Einstellungen:
   - **Verhaltensüberwachung aktivieren**

     Hinweis

     Wenn Benutzer ihre eigenen Einstellungen der Verhaltensüberwachung anpassen können sollen, navigieren Sie zu **Geräte** > **{Gruppe}** > **Richtlinie konfigurieren** > **Agent-Berechtigungen** > **Verhaltensüberwachung** und wählen Sie **Benutzern erlauben, die Einstellungen der Verhaltensüberwachung zu ändern**.
   - **Sperren des Malware-Verhaltens für bekannte oder potenzielle Bedrohungen aktivieren**: Das Sperren des Malware-Verhaltens wird mithilfe eines internen Regelsatzes erreicht, der in **Pattern-Dateien** definiert ist. Mithilfe dieser Regeln wird bekanntes und verdächtiges Bedrohungsverhalten identifiziert, das häufig bei Malware vorkommt. Zu den Beispielen für solches verdächtiges Verhalten gehören unter anderem das plötzliche und unerklärliche Ausführen neuer Dienste, Änderungen an der Firewall oder Änderungen von Systemdateien.

Die Überwachung des Malware-Verhaltens bietet die folgenden Suchoptionen für Bedrohungsstufen:

- **Bekannte Bedrohungen**: Blockiert mit bekannten Bedrohungen verbundene Verhaltensweisen.
- **Bekannte und potenzielle Bedrohungen**: Hiermit wird mit bekannten Bedrohungen verbundenes Verhalten blockiert, und es werden entsprechende Maßnahmen gegen potenziell bösartiges Verhalten ergriffen.

- **Benutzer fragen, bevor neu entdeckte Programme ausgeführt werden, die über HTTP (Server-Plattformen ausgenommen) heruntergeladen wurden**: Die Verhaltensüberwachung wird zusammen mit Web Reputation verwendet, um die Verbreitung von Dateien sicherzustellen, die über HTTP-Kanäle oder E-Mail-Anwendungen heruntergeladen wurden. Nach der Erkennung einer "neu entdeckten" Datei können Administratoren festlegen, dass Benutzer vor der Ausführung der Datei informiert werden. Trend Micro stuft ein Programm auf der Grundlage der Anzahl der Dateierkennungen oder des historischen Alters der Datei als neu gefunden ein, so wie dies durch das Smart Protection Network definiert ist.

Hinweis

Bei HTTP-Kanälen werden ausführbare Dateien (.exe) durchsucht. Bei E-Mail-Anwendungen (nur Outlook und Windows Live Mail) werden ausführbare Dateien (.exe) in nicht kennwortgeschützten archivierten Dateien (zip/rar) durchsucht.

- **Intuit QuickBooks-Schutz aktivieren**: Diese Funktion schützt alle Intuit QuickBooks-Dateien und -Ordner vor unbefugten Änderungen durch andere Programme. Die Aktivierung dieser Funktion beeinträchtigt die durch Intuit QuickBooks-Programme vorgenommenen Änderungen nicht, sondern verhindert nur, dass andere unbefugte Anwendungen Dateien ändern.

  Folgende Produkte werden unterstützt:

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

Hinweis

Da alle ausführbaren Intuit-Dateien über eine digitale Signatur verfügen, werden Updates dieser Dateien nicht gesperrt. Falls andere Programme versuchen, die binäre Intuit-Datei zu ändern, zeigt der Agent eine Nachricht mit dem Namen des Programms an, das versucht, die binären Dateien zu aktualisieren. Sie können andere Programme berechtigen, die Intuit-Dateien zu aktualisieren. Fügen Sie dazu das gewünschte Programm zur Ausnahmeliste der Verhaltensüberwachung auf dem Agent hinzu. Vergessen Sie nicht, das Programm nach dem Update aus der Ausnahmeliste zu entfernen.

- **Schutz vor Ransomware**: Verhindert die nicht autorisierte Änderung oder Verschlüsselung von Dateien auf Computern durch „Ransomware“-Bedrohungen. Ransomware ist eine Art von Malware, die den Zugriff auf Dateien beschränkt und verlangt, dass Sie für die Wiederherstellung der betroffenen Dateien bezahlen.
  - **Dokumentschutz vor nicht autorisierter Verschlüsselung oder Veränderung aktivieren**: Schützt Dokumente vor nicht autorisierten Änderungen.
    - **Dateien, die von verdächtigen Programmen geändert wurden, automatisch sichern**: Sichert automatisch Dateien, die von verdächtigen Programmen geändert wurden, sofern der Dokumentschutz aktiviert ist.
  - **Sperren von Vorgängen aktivieren, die häufig mit Ransomware verbunden sind**: Schützt Endpunkte vor Ransomware-Angriffen, indem Prozesse gesperrt werden, die häufig mit Hijacking-Versuchen in Verbindung stehen.

- (Nur Desktop-Gruppen) **Programmüberprüfung zum Erkennen und Sperren gefährdeter ausführbarer Dateien aktivieren**: Erhöht den Schutz durch Überwachung der Prozesse auf Ransomware-typisches Verhalten.
- **Programme beenden, die ein abnormales Verhalten im Zusammenhang mit Exploit-Angriffen aufweisen**: Der Anti-Exploit-Schutz funktioniert in Verbindung mit der Programmüberwachung, um das Verhalten von Programmen zu überwachen und abnormales Verhalten zu erkennen, das darauf hindeuten kann, dass ein Angreifer eine Programmschwachstelle ausgenutzt hat. Sobald ein Problem erkannt wurde, beendet die Verhaltensüberwachung die Programmprozesse.

Hinweis

Für den Schwachstellenschutz muss die Option **Programmüberprüfung zum Erkennen und Sperren gefährdeter ausführbarer Dateien aktivieren** ausgewählt werden.

Hinweis

Um die Wahrscheinlichkeit zu verringern, dass Worry-Free Business Security einen sicheren Prozess als bösartig erkennt, müssen Sie sicherstellen, dass der Computer auf das Internet zugreifen kann, um weitere Überprüfungsprozesse mit Hilfe von Trend Micro-Servern auszuführen.

- **Ausnahmen**: Ausnahmen beinhalten eine Liste der zulässigen Programme und eine Liste der gesperrten Programme. Programme in der Liste der zulässigen Programme können auch dann ausgeführt werden, wenn dies gegen eine überwachte Änderung verstößt, während Programme in der Liste der gesperrten Programme nie ausgeführt werden können.
  - **Vollständigen Programmpfad eingeben**: Geben Sie den vollständigen Windows- oder UNC-Pfad des Programms ein. Trennen Sie mehrere Einträge mit einem Strichpunkt. Klicken

Sie auf **Zur Liste der zulässigen Programme hinzufügen** oder **Zur Liste der gesperrten Programme hinzufügen**. Verwenden Sie bei Bedarf Umgebungsvariablen, um den Pfad anzugeben.

- **Liste der zulässigen Programme**: Programme in dieser Liste können gestartet werden. Klicken Sie auf das entsprechende Symbol, um einen Eintrag zu löschen.

  Die Liste der zulässigen Programme unterstützt Platzhalter und Umgebungsvariablen.

  Eine Liste der unterstützten Umgebungsvariablen finden Sie unter *Unterstützte Umgebungsvariablen auf Seite 5-16*.

- **Liste der gesperrten Programme**: Programme in dieser Liste können nie gestartet werden. Klicken Sie auf das entsprechende Symbol, um einen Eintrag zu löschen.

  Die Liste der gesperrten Programme unterstützt nur Platzhalter.

6. Klicken Sie auf **Speichern**.

Unterstützte Umgebungsvariablen

Die folgende Tabelle listet die Umgebungsvariablen auf, die Sie verwenden können, wenn Sie einen Datei- oder Ordnerpfad zur Liste hinzufügen.

Umgebungsvariable	Beispiel	Entsprechender Pfad
$allappdata$	$allappdata$\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:\Programme\test\sample.exe
$programdirx86$	$programdirx86$\test\sample.exe	C:\Programme (x86)\test\sample.exe

Umgebungsvariable	Beispiel	Entsprechender Pfad
$rootdir$	$rootdir$\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

Vertrauenswürdiges Programm

In der Liste vertrauenswürdiger Programme aufgeführte Programme werden nicht auf verdächtige Dateizugriffsaktivitäten überwacht.

Vertrauenswürdiges Programm konfigurieren

Hinweis

Die Liste der vertrauenswürdigen Programme unterstützt keine Platzhalter und Umgebungsvariablen.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.

4. Klicken Sie auf **Vertrauenswürdiges Programm**.

   Ein neues Fenster wird angezeigt.

5. Um ein Programm von der Überwachung auf verdächtige Dateizugriffsaktivitäten auszuschließen, geben Sie den vollständigen Dateipfad ein, und klicken Sie auf **Zur Liste der vertrauenswürdigen Programme hinzufügen**.

   `<Laufwerkname>:/<Pfad>/<Dateiname>`

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

   Beispiel 2: `D:\backup\tool.exe`

   Somit können Hacker keine Programmnamen verwenden, die in der Ausschlussliste enthalten sind, aber zur Ausführung unter einem anderen Dateipfad abgelegt wurden.

6. Klicken Sie auf **Speichern**.

Quarantäne-Ordner

Wenn die Aktion für eine infizierte Datei 'Quarantäne' ist, verschlüsselt der Security Agent die Datei und verschiebt diese **vorübergehend** in einen Quarantäneordner in:

- `<Security Agent Installationsordner>\quarantine` für Agents, die von Version 6.x oder einer früheren Version aktualisiert wurden
- `<Security Agent Installationsordner>\SUSPECT\Backup` für neu installierte Agents und Agents, die von Version 7.x oder einer höheren Version aktualisiert wurden

Der Security Agent sendet die infizierte Datei an einen zentralen Quarantäne-Ordner, den Sie unter **Geräte** > **{Gruppe}** > **Richtlinie konfigurieren** > **Quarantäne** in der Webkonsole konfigurieren können.

Zentraler Standardquarantäne-Ordner

Der zentrale Standardquarantäne-Ordner befindet sich auf dem Security Server. Das Verzeichnis ist im URL-Format und enthält den Host-Namen oder die IP-Adresse des Security Servers, z. B. `http://server`. Der entsprechende absolute Pfad ist `<Security Server Installationsordner>\PCCSRV\Virus`.

- Verwaltet der Server sowohl IPv4- als auch IPv6-Agents, verwenden Sie den Host-Namen, damit alle Agents Quarantänedateien an den Server senden können.
- Hat der Server nur eine IPv4-Adresse oder wird über sie identifiziert, können nur reine IPv4- und Dual-Stack-Agents Quarantänedateien an den Server senden.
- Hat der Server nur eine IPv6-Adresse oder wird über sie identifiziert, können nur reine IPv6- und Dual-Stack-Agents Quarantänedateien an den Server senden.

Alternativer Standardquarantäne-Ordner

Sie können auch einen alternativen Quarantäne-Ordner festlegen, indem Sie den Speicherort als URL, UNC-Pfad oder absoluten Dateipfad eingeben. Security Agents sollten eine Verbindung zu diesem alternativen Verzeichnis aufbauen können. Das alternative Verzeichnis sollte beispielsweise eine IPv6-Adresse haben, wenn es Quarantänedateien von den Dual-Stack-Clients und den reinen IPv6-Agents empfangen soll. Trend Micro empfiehlt die Benennung eines Dual-Stack-Verzeichnisses, die Identifizierung des Verzeichnisses nach seinem Host-Namen und die Verwendung eines UNC-Pfads bei Eingabe des Verzeichnisses.

Richtlinien zur Nutzung des zentralen Quarantäne-Ordners

In der folgenden Tabelle finden Sie eine Anleitung zur Verwendung von URLs, UNC-Pfaden oder absoluten Dateipfaden:

Tabelle 5-4. Quarantäne-Ordner

Quarantäne-Ordner	Kompatibles Format	Beispiel	Hinweise
Standardverzeichnis des Security Servers	URL	`http:// <Server-Host-Name oder IP>`	Wenn Sie das Standardverzeichnis beibehalten, konfigurieren Sie die Wartungseinstellungen für das Verzeichnis, wie z. B. die Größe des Quarantäne-Ordners, im Bereich **Administration** > **Allgemeine Einstellungen** > **Registerkarte System** > **Quarantäne-Wartung** .
	UNC-Pfad	`\\<Server-Host-Name oder IP>\ofcscan\Virus`	
Ein anderes Verzeichnis auf dem Security Server	UNC-Pfad	`\\<Server-Host-Name oder IP>\ D $\Dateien in Quarantäne`	Wenn Sie das Standardverzeichnis nicht verwenden möchten (z. B. aufgrund von unzureichendem Speicherplatz), geben Sie den UNC-Pfad in ein anderes Verzeichnis ein. Geben Sie in diesem Fall den entsprechenden absoluten Pfad im Bereich **Administration** > **Allgemeine Einstellungen** > **Registerkarte System** > **Quarantäne-Wartung** ein, damit die Wartungseinstellungen wirksam werden.

Quarantäne-Ordner	Kompatibles Format	Beispiel	Hinweise
Ein Verzeichnis auf einem anderen Security Server-Computer (falls sich andere Security Server in Ihrem Netzwerk befinden)	URL	`http://<Server2-Host-Name oder IP>`	Vergewissern Sie sich, dass Agents eine Verbindung zu diesem Verzeichnis aufbauen können. Bei Angabe eines ungültigen Verzeichnisses behält der Agent die unter Quarantäne gestellten Dateien, bis ein gültiger Quarantäne-Ordner angegeben wird. Im Viren-/Malware-Protokoll des Servers lautet das Suchergebnis "Die Datei konnte nicht in den festgelegten Quarantäne-Ordner verschoben werden". Wenn Sie einen UNC-Pfad verwenden, stellen Sie sicher, dass der Quarantäne-Ordner für die Gruppe "Alle" freigegeben ist und dass Sie dieser Gruppe Lese- und Schreibberechtigungen zugewiesen haben.
	UNC-Pfad	`\\<Server2-Host-Name oder IP>\ofcscan\Virus`	
Anderer Computer im Netzwerk	UNC-Pfad	`\\<computer_name>\temp`	
Ein anderes Verzeichnis auf dem Client	Absoluter Pfad	`C:\temp`	Geben Sie einen absoluten Pfad an, wenn: • Sie möchten, dass sich Dateien in Quarantäne nur auf dem Client befinden. • Sie nicht möchten, dass die Agents die Dateien im Standardverzeichnis des Clients speichern. Wenn der Pfad nicht vorhanden ist, erstellt der Security Agent ihn automatisch.

Den Quarantäne-Ordner konfigurieren

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.
4. Klicken Sie auf **Quarantäne**.

   Ein neues Fenster wird angezeigt.
5. Konfigurieren Sie den Quarantäne-Ordner. Weitere Informationen finden Sie unter *Quarantäne-Ordner auf Seite 5-18*.
6. Klicken Sie auf **Speichern**.

Web Reputation

Web Reputation kann den Zugriff auf URLs im Web oder auf in E-Mails eigebettete URLs verhindern, die potenzielle Sicherheitsrisiken darstellen. Web Reputation überprüft die Reputation der URL anhand von Trend Micro Web Reputation-Servern und gleicht anschließend die Zuverlässigkeit einer Website mit der entsprechenden Web Reputation-Richtlinie ab, die auf dem Client angewendet wird. Je nach geltender Richtlinie:

- Der Security Agent sperrt den Zugriff auf eine Website oder lässt ihn zu.
- Der Messaging Security Agent (nur Advanced) kann E-Mail-Nachrichten mit bösartigen URLs in den Quarantäneordner schieben, löschen oder kennzeichnen oder das Senden der Nachricht zulassen, wenn die URL sicher ist

Bei Treffern in der Datenbank benachrichtigt Web Reputation den Administrator per E-Mail und den Benutzer über eine Online-Mitteilung.

Konfigurieren Sie für Security Agents unterschiedliche Sicherheitsstufen je nach Standort des Clients (Im Büro/Nicht im Büro).

Wenn Web Reputation einen Link sperrt, den Sie als sicher erachten, fügen Sie den Link zur Liste der zulässigen Links hinzu.

Tipp

Um Netzwerkbandbreite zu sparen, empfiehlt Trend Micro, die unternehmensinternen Websites in die Liste der von Web Reputation zugelassenen URLs einzutragen.

Vertrauenswürdigkeitsrate

Der 'Reputationswert' eines URLs bestimmt, ob es sich um eine Internet-Bedrohung handelt. Trend Micro berechnet diese Rate mit eigenen Bewertungssystemen.

Trend Micro stuft einen URL als Internet-Bedrohung ein, wenn die Rate innerhalb eines festgelegten Schwellenwerts liegt und als sicher, wenn dieser Wert überschritten wird.

Ein Security Agent verfügt über drei Sicherheitsstufen, durch die festgelegt wird, ob er einen URL zulässt oder sperrt.

- **Hoch**: Seiten mit folgender Bewertung blockieren:
  - **Gefährlich**: bekanntermaßen betrügerisch oder Bedrohungsquellen sind
  - **Äußerst verdächtig**: im Verdacht stehen, betrügerisch oder möglicherweise Bedrohungsquellen zu sein
  - **Verdächtig**: Mit Spam in Verbindung oder möglicherweise infiziert.
  - **Nicht geprüft**: Obwohl Trend Micro Websites aktiv auf deren Sicherheit testet, ist es möglich, dass Benutzer auf ungetestete Websites treffen, wenn diese neu sind oder seltener besucht werden. Das Sperren ungetesteter Sites kann die Sicherheit erhöhen, doch es kann auch dazu führen, dass der Zugriff auf sichere Sites gesperrt wird.

- **Mittel**: Seiten mit folgender Bewertung blockieren:
  - **Gefährlich**: bekanntermaßen betrügerisch oder Bedrohungsquellen sind
  - **Äußerst verdächtig**: im Verdacht stehen, betrügerisch oder möglicherweise Bedrohungsquellen zu sein
- **Niedrig**: Seiten mit folgender Bewertung blockieren:
  - **Gefährlich**: bekanntermaßen betrügerisch oder Bedrohungsquellen sind

Web Reputation für Security Agents konfigurieren

Web Reputation bewertet das potenzielle Sicherheitsrisiko aller angeforderten Links, indem bei jeder HTTP-/HTTPS-Anfrage die Trend Micro-Security-Datenbank abgefragt wird.

Hinweis

(Nur Standard) Einstellungen für Web Reputation "Im Büro" und "Nicht im Büro" konfigurieren. Wenn Location Awareness deaktiviert ist, werden die Einstellungen von Im Büro für die Verbindungen von Nicht im Büro verwendet. Weitere Informationen zu Location Awareness finden Sie unter *Desktop-/Server-Einstellungen konfigurieren auf Seite 11-5*.

Wenn sowohl Web Reputation als auch die Prävention von Angriffen auf Browser aktiviert sind, werden URLs, die nicht durch Web Reputation gesperrt wurden, anschließend durch die Funktion zur Prävention von Angriffen auf Browser durchsucht. Die Funktion zur Prävention von Angriffen auf Browser durchsucht die eingebetteten Objekte (z. B.: jar, class, pdf, swf, html, js) auf den Webseiten des URL.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.

3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.

4. Klicken Sie auf **Web Reputation** > **Im Büro** oder **Web Reputation** > **Nicht im Büro**.

   Ein neues Fenster wird angezeigt.

5. Aktualisieren Sie auf Anforderung folgende Einstellungen:

   - **Web Reputation aktivieren**
   - Sicherheitsstufe: **Hoch**, **Mittel** oder **Niedrig**
   - Prävention von Angriffen auf Browser: **Seiten mit schädlichem Skript sperren**

6. Klicken Sie auf **Speichern**.

URL-Filter

URL-Filter unterstützen Sie bei der Vergabe von Zugriffsberechtigungen für Websites, um unproduktive Arbeitszeiten zu reduzieren, Internet-Bandbreite zu schonen und eine sichere Internet-Umgebung zu schaffen. Sie können den gewünschten Grad an URL-Filterschutz auswählen oder selbst definieren, welche Arten von Websites Sie anzeigen möchten.

Hinweis

Um Kunden zu schützten, blockiert Trend Micro automatisch alle URLs mit Inhalten, die in den meisten Teilen der Erde verboten sind.

URL-Filter konfigurieren

Über **Benutzerdefiniert** können Sie bestimmte Arten von Websites festlegen, die zu bestimmten Tageszeiten gesperrt werden.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.
4. Klicken Sie auf **URL-Filter**.

   Ein neues Fenster wird angezeigt.
5. Aktualisieren Sie auf Anforderung folgende Einstellungen:
   - **URL-Filter aktivieren**
   - **Filterstärke**
     - **Hoch**: Sperrt bekannte oder potenzielle Sicherheitsbedrohungen, unangemessenen oder möglicherweise anstößigen Inhalt, der die Produktivität oder Netzwerkbandbreite beeinträchtigen kann, sowie nicht bewertete Seiten
     - **Mittel**: Sperrt bekannte Sicherheitsbedrohungen und unangemessenen Inhalt
     - **Niedrig**: Sperrt bekannte Sicherheitsbedrohungen
     - **Benutzerdefiniert**: Wählen Sie eigene Kategorien aus, und legen Sie fest, ob diese Kategorien während der Geschäftszeiten oder der Freizeit gesperrt werden sollen.
   - **Filterregeln**: Wählen Sie die zu sperrenden Kategorien oder Subkategorien aus.
   - **Geschäftszeiten**: Tage und Stunden, die nicht als Geschäftszeiten definiert sind, werden als Freizeit betrachtet.
6. Klicken Sie auf **Speichern**.

Zulässige/gesperrte URLs

Die automatische Genehmigung oder Sperrung von URLs unterstützt die Vergabe von Zugriffsberechtigungen für Websites und trägt zu einer sichereren Internet-Umgebung bei. In den allgemeinen Einstellungen können Sie die genehmigten oder gesperrten URLs ermitteln.

Darüber hinaus können Sie für bestimmte Gruppen benutzerdefinierte Listen mit genehmigten oder gesperrten URLs erstellen. Bei Auswahl der Option **Zulässige/gesperrte URLs für diese Gruppe anpassen** verwendet der Security Agent die benutzerdefinierte Liste der jeweiligen Gruppe mit genehmigten oder gesperrten URLs, um den Zugriff auf Websites zu steuern.

Zulässige/gesperrte URLs konfigurieren

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.
4. Klicken Sie auf **Zulässige/gesperrte URLs**.

   Ein neues Fenster wird angezeigt.
5. Aktualisieren Sie folgende Einstellungen bei Bedarf.
   - **Zulässige/gesperrte URLs für diese Gruppe anpassen**: Die in dieser Liste angegebenen URLs überschreiben alle anderen Einstellungen.
   - Geben Sie im Textfeld **Genehmigte URLs** die URLs von Websites ein, die Sie von den Überprüfungen durch Web Reputation und URL-Filter ausschließen möchten. Trennen Sie mehrere URLs mit einem Strichpunkt (;). Klicken Sie auf **Hinzufügen**.

Tipp

Klicken Sie auf **Aus allgemeinen Einstellungen importieren**, um alle Einträge einzufügen. Anschließend können Sie die URLs für diese Gruppe anpassen.

- Geben Sie im Textfeld **Gesperrte URLs** die URLs von Websites ein, die vom URL-Filter gesperrt werden sollen. Trennen Sie mehrere URLs mit einem Strichpunkt (;). Klicken Sie auf **Hinzufügen**.

Tipp

Klicken Sie auf **Aus allgemeinen Einstellungen importieren**, um alle Einträge einzufügen. Anschließend können Sie die URLs für diese Gruppe anpassen.

6. Klicken Sie auf **Speichern**.

Firewall

Die Firewall errichtet eine Barriere zwischen dem Client und dem Netzwerk, über die bestimmte Arten des Netzwerkverkehrs gesperrt oder zugelassen werden. Darüber hinaus erkennt die Firewall bestimmte Muster in Netzwerkpaketen, die auf einen Angriff auf die Clients hindeuten können.

Zur Konfiguration der Firewall stehen in Worry-Free Business Security zwei Optionen zur Verfügung: der einfache Modus und der erweiterte Modus. Im einfachen Modus ist die Firewall mit den von Trend Micro empfohlenen Standardeinstellungen aktiviert. Verwenden Sie den erweiterten Modus, um die Firewall-Einstellungen anzupassen.

Tipp

Trend Micro empfiehlt, andere softwarebasierte Firewalls vor der Installation und Aktivierung der Trend Micro Firewall zu deinstallieren.

Firewall-Standardeinstellungen – Einfacher Modus

Die Standardeinstellungen der Firewall dienen als Grundlage für die Erstellung einer eigenen Client-Firewall-Schutzstrategie. Die Standardeinstellungen umfassen allgemeine Bedingungen auf Ihren Clients, wie z. B. die Notwendigkeit, auf das Internet zuzugreifen oder Dateien über den FTP-Server auszutauschen.

Hinweis

Standardmäßig deaktiviert Worry-Free Business Security die Firewall auf allen neuen Gruppen und Security Agents.

TABELLE 5-5. Standardeinstellungen der Firewall

EINSTELLUNGEN	STATUS
Sicherheitsebene	Niedrig Ein- und ausgehender Datenverkehr werden zugelassen, nur Netzwerkviren werden gesperrt
Intrusion Detection System	Deaktiviert
Warnmeldung (senden)	Deaktiviert

TABELLE 5-6. Standardausnahmen für die Firewall

NAME DER AUSNAHME	AKTION	RICHTUNG	PROTOKOLL	PORT
DNS	Zulassen	Eingehend und ausgehend	TCP/UDP	53
NetBIOS	Zulassen	Eingehend und ausgehend	TCP/UDP	137, 138, 139, 445
HTTPS	Zulassen	Eingehend und ausgehend	TCP	443
HTTP	Zulassen	Eingehend und ausgehend	TCP	80

Name der Ausnahme	Aktion	Richtung	Protokoll	Port
Telnet	Zulassen	Eingehend und ausgehend	TCP	23
SMTP	Zulassen	Eingehend und ausgehend	TCP	25
FTP	Zulassen	Eingehend und ausgehend	TCP	21
POP3	Zulassen	Eingehend und ausgehend	TCP	110
MSA	Zulassen	Eingehend und ausgehend	TCP	16372, 16373
LDAP	Zulassen	Eingehend und ausgehend	TCP/UDP	389

Tabelle 5-7. Standardmäßige Firewall-Einstellungen nach Standort

Speicherort	Firewall-Einstellungen
Im Büro	Deaktiviert
Nicht im Büro	Deaktiviert

Den Datenverkehr filtern

Die Firewall filtert den gesamten ein- und ausgehenden Datenverkehr und sperrt bestimmte Arten von Datenverkehr gemäß den folgenden Kriterien:

- Richtung (eingehend/ausgehend)
- Protokoll (TCP/UDP/ICMP/ICMPv6)
- Zielports
- Zielcomputer

Suche nach Netzwerkviren

Die Firewall untersucht außerdem jedes Paket auf Netzwerkviren.

Stateful Inspection

Die Firewall ist eine Firewall mit Stateful Inspection: Alle Verbindungen zum Client werden überwacht und sämtliche Verbindungszustände registriert. Sie kann bestimme Zustände in den Verbindungen ermitteln, zu ergreifende Aktionen vorschlagen und Störungen des Normalzustands feststellen. Aus diesem Grund umfasst die effektive Nutzung der Firewall nicht nur das Erstellen von Profilen und Richtlinien, sondern auch die Analyse von Verbindungen und das Filtern von Paketen, die die Firewall passieren.

Allgemeiner Firewall-Treiber

Bei einem Virenausbruch sperrt der allgemeine Firewall-Treiber bestimmte Ports gemäß den benutzerdefinierten Einstellungen der Firewall. Außerdem verwendet dieser Treiber das Netzwerkviren-Pattern, um Netzwerkviren zu entdecken.

Die Firewall konfigurieren

Konfigurieren Sie die Firewall für die Profile 'Im Büro' und 'Nicht im Büro'. Wenn Location Awareness deaktiviert ist, werden die Einstellungen von Im Büro für die Verbindungen von Nicht im Büro verwendet.

Weitere Informationen zu Location Awareness finden Sie unter *Desktop-/Server-Einstellungen konfigurieren auf Seite 11-5*.

Trend Micro deaktiviert die Firewall standardmäßig.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.
4. Klicken Sie auf **Firewall** > **Im Büro** oder auf **Nicht im Büro**.

5. Wählen Sie **Firewall aktivieren**.

6. Wählen Sie unter folgenden Einstellungen:

   - **Einfacher Modus**: Aktiviert die Firewall mit den Standardeinstellungen.

     Weitere Informationen finden Sie unter *Firewall auf Seite 5-28*.

   - **Erweiterter Modus**: Aktiviert die Firewall mit benutzerdefinierten Einstellungen.

7. Falls Sie **Erweiterter Modus** aktiviert haben, aktualisieren Sie die folgenden Optionen bei Bedarf:

   - **Sicherheitsstufe**: Die Sicherheitsstufe bestimmt die Verkehrsregeln für Ports, die nicht in der Ausnahmeliste enthalten sind.

     - **Hoch**: In der Sicherheitsstufe Hoch wird der gesamte ein- und ausgehende Datenverkehr gesperrt, sofern dieser nicht durch die Ausnahmeliste zugelassen wurde.

     - **Mittel**: In der Sicherheitsstufe Mittel wird der gesamte eingehende Datenverkehr gesperrt sowie der gesamte ausgehende Datenverkehr zugelassen, sofern dieser nicht durch die Ausnahmeliste zugelassen oder gesperrt wurde.

     - **Niedrig**: In der Sicherheitsstufe Niedrig wird der gesamte ein- und ausgehende Datenverkehr zugelassen, sofern dieser nicht durch die Ausnahmeliste gesperrt wurde. Dies ist die Standardeinstellung für den einfachen Modus.

   - **Einstellungen**

     - **Intrusion Detection System aktivieren**: Intrusion Detection System erkennt Pattern in Netzwerkpaketen, die möglicherweise auf einen Angriff hindeuten.

       Weitere Informationen finden Sie unter *Intrusion Detection System auf Seite D-3*.

- **Warnmeldungen aktivieren**: Wenn Worry-Free Business Security eine Regelverletzung entdeckt, wird eine Benachrichtigung an den Client gesendet.

- **Ausnahmen**: Die in der Ausnahmeliste enthaltenen Ports werden nicht gesperrt.

  Weitere Informationen finden Sie unter *Mit Firewall-Ausnahmen arbeiten auf Seite 5-33*.

8. Klicken Sie auf **Speichern**.

Mit Firewall-Ausnahmen arbeiten

Die Ausnahmeliste der Firewall enthält Einträge, die von Ihnen konfiguriert werden können, um verschiedene Arten von Netzwerkverkehr, ausgehend von den Portnummern und IP-Adressen des Clients, zu sperren oder zuzulassen. Während eines Virenausbruchs wendet der Security Server die Ausnahmen auf die Trend Micro Richtlinien an, die zum Schutz Ihres Netzwerks automatisch verteilt werden.

Beispielsweise können Sie während eines Virenausbruchs den gesamten Client-Verkehr sperren, einschließlich des Datenverkehrs über den HTTP-Port (Port 80). Wenn die gesperrten Clients dennoch einen Internet-Zugang haben sollen, können Sie den Proxy-Server für das Internet zur Ausnahmeliste hinzufügen.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.
4. Klicken Sie auf **Firewall** > **Im Büro** oder auf **Firewall** > **Nicht im Büro**.

   Ein neues Fenster wird angezeigt.

5. Wählen Sie **Firewall aktivieren**.
6. Wählen Sie **Erweiterter Modus**.
7. Eine Ausnahme hinzufügen:
   a. Klicken Sie auf **Hinzufügen**.

      Ein neues Fenster wird angezeigt.
   b. Geben Sie den Namen für die Ausnahme ein.
   c. Klicken Sie neben dem Feld **Aktion** auf eine der folgenden Optionen:
      - **Netzwerkverkehr zulassen**
      - **Netzwerkverkehr ablehnen**
   d. Wählen Sie neben **Richtung** entweder **Eingehend** oder **Ausgehend**, um zu bestimmen, für welche Art von Datenverkehr die Ausnahmen gelten sollen.
   e. Wählen Sie aus der Liste Protokoll das Netzwerkprotokoll aus:
      - **Alle**
      - **TCP/UDP** (Standard)
      - **TCP**
      - **UDP**
      - **ICMP**
      - **ICMPv6**
   f. Klicken Sie zur Angabe der Client-Ports auf eine der folgenden Optionen:
      - **Alle Ports** Standard)
      - **Bereich**: Geben Sie einen Portbereich ein.
      - **Ausgewählte Ports**: Geben Sie einzelne Ports an. Trennen Sie die Einträge durch Komma voneinander.

g. Wählen Sie unter **Computer** die IP-Adressen der Clients aus, die in diese Ausnahme einbezogen werden sollen. Wenn Sie beispielsweise **Netzwerkverkehr ablehnen (eingehend und ausgehend)** wählen und die IP-Adresse für einen einzigen Client im Netzwerk eingeben, kann kein Client, dessen Richtlinie diese Ausnahme enthält, Daten an diese IP-Adresse senden oder Daten von dort empfangen. Klicken Sie auf eine der folgenden Optionen:

- **Alle IP-Adressen** (Standard)
- **Einzelne IP**: Geben Sie eine IPv4- bzw. eine IPv6-Adresse oder einen Host-Namen ein. Klicken Sie auf **Auflösen**, um den Host-Namen des Clients in eine IP-Adresse aufzulösen.
- **IP-Bereich (für IPv4 oder IPv6)**: Geben Sie in die Felder **Von** und **Bis** entweder zwei IPv4- oder zwei IPv6-Adressen ein. Es ist nicht möglich, in ein Feld eine IPv6-Adresse und in das andere eine IPv4-Adresse einzugeben.
- **IP-Bereich (für IPv6)**: Geben Sie ein IPv6-Adresspräfix und eine Länge ein.

h. Klicken Sie auf **Speichern**.

8. Klicken Sie auf **Bearbeiten**, um eine Ausnahme zu bearbeiten, und ändern Sie anschließend die Einstellungen im angezeigten Fenster.

9. Wählen Sie die Ausnahme aus und klicken Sie auf **Nach oben** oder **Nach unten**, um eine Ausnahme in der Liste nach oben oder nach unten zu verschieben, bis sie sich auf der gewünschten Position befindet.

10. Um eine Ausnahme zu entfernen, wählen Sie sie aus, und klicken Sie auf **Löschen**.

Firewall in einer Agents-Gruppe deaktivieren

Prozedur

1. Navigieren Sie zu **Geräte**.

2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.
4. Klicken Sie auf **Firewall** > **Im Büro** oder auf **Firewall** > **Nicht im Büro**.

   Ein neues Fenster wird angezeigt.
5. Wählen Sie **Firewall deaktivieren**.
6. Klicken Sie auf **Speichern**.

Firewall für alle Agents deaktivieren

Prozedur

1. Gehen Sie zu **Administration** > **Allgemeine Einstellungen**.
2. Klicken Sie auf **Desktop/Server**.
3. Wählen Sie unter **Firewall-Einstellungen Firewall deaktivieren und Treiber deinstallieren**.
4. Klicken Sie auf **Speichern**.

Gerätesteuerung

Die Gerätesteuerung reguliert den Zugriff auf externe Speichergeräte, die mit Endpunkten verbunden sind. Insbesondere beschränkt die Gerätesteuerung den Zugriff auf alle Arten von Speichergeräten, die über eine USB-Schnittstelle verbunden sind, mit Ausnahme von mobilen Geräten und Digitalkameras.

Gerätesteuerung konfigurieren

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.
4. Klicken Sie auf **Gerätesteuerung**.
5. Aktualisieren Sie auf Anforderung folgende Einstellungen:
   - **Gerätesteuerung aktivieren**
   - **Schutz vor automatisch ausgeführten Dateien auf USB-Laufwerken aktivieren**
   - **Berechtigungen**:Legen Sie die Berechtigungen für USB-Geräte und Netzwerkressourcen fest.

     Tabelle 5-8. Berechtigungen für die Gerätesteuerung

Berechtigungen	Dateien auf dem Gerät	Eingehende Dateien
Vollständiger Zugriff	Zulässige Aktionen: Kopieren, Verschieben, Öffnen, Speichern, Löschen, Ausführen	Zulässige Aktionen: Speichern, Verschieben, Kopieren Das bedeutet, dass eine Datei kann auf dem Gerät gespeichert, verschoben und kopiert werden kann.

Berechtigungen	Dateien auf dem Gerät	Eingehende Dateien
Kein Zugriff	Unzulässige Aktionen: Alle Aktionen Die enthaltenen Geräte und Dateien werden dem Benutzer angezeigt (beispielsweise in Windows Explorer).	Unzulässige Aktionen: Speichern, Verschieben, Kopieren
Lesen	Zulässige Aktionen: Kopieren, Öffnen Unzulässige Aktionen: Speichern, Verschieben, Löschen, Ausführen	Unzulässige Aktionen: Speichern, Verschieben, Kopieren
Ändern	Zulässige Aktionen: Kopieren, Verschieben, Öffnen, Speichern, Löschen Unzulässige Aktionen: Ausführen	Zulässige Aktionen: Speichern, Verschieben, Kopieren
Lesen und Ausführen	Zulässige Aktionen: Kopieren, Öffnen, Ausführen Unzulässige Aktionen: Speichern, Verschieben, Löschen	Unzulässige Aktionen: Speichern, Verschieben, Kopieren

- **Ausnahmen**: Falls einem Benutzer kein Lesezugriff auf ein bestimmtes Gerät gewährt wird, kann er trotzdem alle Dateien und Programme in der Liste der zulässigen Programme öffnen oder ausführen.

  Ist jedoch der Schutz vor automatisch ausgeführten Dateien aktiviert, kann eine Datei auch dann nicht ausgeführt werden, wenn sie in der Liste der zulässigen Programme aufgeführt ist.

  Um der Liste der zulässigen Programme eine Ausnahme hinzuzufügen, geben Sie den Dateinamen einschließlich des Pfades

oder der digitalen Signatur ein, und klicken Sie auf **Zur Liste der zulässigen Programme hinzufügen**.

6. Klicken Sie auf **Speichern**.

Benutzer-Tools

- **Anti-Spam Symbolleiste**: Ein Spam-Filter für Microsoft Outlook mit statistischen Auswertungen und der Möglichkeit, bestimmte Einstellungen zu ändern.
- **HouseCall**: Bestimmt die Sicherheit einer Wireless-Verbindung durch Überprüfung der Seriosität von Zugangspunkten anhand der Gültigkeit ihrer SSIDs, Authentifizierungsmethoden und Verschlüsselungsanforderungen. Eine Warnung in Form eines Popups wird angezeigt, wenn eine Verbindung unsicher ist.
- **Case Diagnostic Tool**: Bei Problemen können mit dem Trend Micro Case Diagnostic Tool (CDT) die notwendigen Debugging-Informationen zum Produkt des Kunden zusammengestellt werden. Das Tool aktiviert und deaktiviert automatisch den Debug-Status und sammelt je nach Problemkategorie die erforderlichen Dateien. Diese Informationen helfen Trend Micro bei der Lösung produktbezogener Probleme.

  Dieses Tool ist nur in der Security Agent-Konsole verfügbar.
- **Client Mover**: Mit diesem Tool können Clients von einem Server auf einen anderen verschoben werden. Die Server müssen dieselbe Spracheinstellung und denselben Typ haben.
- **Client/Server-Kommunikations-Tool**: Verwenden Sie dieses Tool zur Fehlerbehebung bei der Client/Server-Kommunikation.

Benutzer-Tools konfigurieren

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.
4. Klicken Sie auf **Benutzer-Tools**.

   Ein neues Fenster wird angezeigt.
5. Aktualisieren Sie auf Anforderung folgende Einstellungen:
   - **Wi-Fi Advisor**: Überprüft die Sicherheit von Wireless-Netzwerken, die auf der Gültigkeit ihrer SSIDs, Authentifizierungsmethoden und Verschlüsselungsvoraussetzungen basieren.
   - **Anti-Spam Symbolleiste**: Filtert Spam in Microsoft Outlook.
6. Klicken Sie auf **Speichern**.

Agent-Berechtigungen

Erteilen Sie Agent-Berechtigungen, damit Benutzer die Einstellungen des Security Agents auf dem Client ändern können.

Tipp

Damit die Einhaltung geregelter Sicherheitsrichtlinien im gesamten Unternehmen gewährleistet bleibt, sollten Sie nur eingeschränkte Benutzerberechtigungen erteilen. Dadurch stellen Sie sicher, dass Benutzer die Sucheinstellungen nicht verändern oder den Security Agent entfernen.

Agent-Berechtigungen konfigurieren

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie eine Desktop- oder Servergruppe aus.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Das Fenster **Richtlinie konfigurieren: <Gruppenname>** wird angezeigt.
4. Klicken Sie auf **Agent-Berechtigungen**.
5. Aktualisieren Sie auf Anforderung folgende Einstellungen:

Abschnitt	Berechtigungen
Virenschutz/Anti-Spyware	• Einstellungen für die Echtzeitsuche • Einstellungen für die manuelle Suche • Einstellungen für die zeitgesteuerte Suche • Zeitgesteuerte Suche überspringen:
Firewall	Firewall-Einstellungen
Web Reputation – Weiterhin anzeigen	Ein Link erscheint, der Benutzern die Anzeige einer bestimmten bösartigen URL bis zum Neustart des Computers weiterhin ermöglicht. Die Warnungen für andere bösartige URLs werden weiterhin angezeigt.
URL-Filter – Weiterhin anzeigen	Ein Link erscheint, der Benutzern die Anzeige einer bestimmten eingeschränkten URL bis zum Neustart des Computers weiterhin ermöglicht. Die Warnungen für andere unzulässige URLs werden weiterhin angezeigt.
Verhaltensüberwachung	Ermöglicht Benutzern, die Einstellungen der Verhaltensüberwachung zu ändern.
Vertrauenswürdiges Programm	Ermöglicht Benutzern, die Liste vertrauenswürdiger Programme zu ändern.

Abschnitt	Berechtigungen
Proxy-Einstellungen	Ermöglicht Benutzern, Proxy-Einstellungen zu konfigurieren. **Hinweis** Das Deaktivieren dieser Funktion setzt die Proxy-Einstellungen auf ihre Standardwerte zurück.
Update-Berechtigungen	• Ermöglicht Benutzern, manuelle Updates durchzuführen. • Verwenden Sie Trend Micro ActiveUpdate als untergeordnete Update-Quelle. • Hotfix-Installationen deaktivieren **Hinweis** Die Verteilung von Hotfixes, Patches, sicheren/kritischen Patches und Service Packs an viele Agents gleichzeitig kann den Netzwerkverkehr erheblich steigern. Wenn Sie diese Option für verschiedene Gruppen aktivieren, können Sie die Verteilung staffeln. Durch das Aktivieren dieser Option werden außerdem automatische **Versions-Upgrades** für Agents deaktiviert (zum Beispiel von der Beta-Version auf die Release-Version der aktuellen Produktversion), aber NICHT automatische **Versions-Upgrades** (zum Beispiel von Version 7.x auf die aktuelle Version). Um automatische Versions-Upgrades zu deaktivieren, müssen Sie das Installationspaket für den Security Server ausführen und die Option für das Verzögern von Upgrades wählen.
Client-Sicherheit	Verhindern Sie, dass Benutzer oder andere Prozesse Trend Micro-Programmdateien, Registrierungen und Prozesse ändern.

6. Klicken Sie auf **Speichern**.

Kapitel 6

Die grundlegenden Sicherheitseinstellungen für Messaging Security Agents (nur Advanced) verwalten

In diesem Kapitel wird der Messaging Security Agent beschrieben und die Einstellungen der Echtzeitsuche sowie die Konfiguration der Optionen für Anti-Spam, Content-Filter, Sperren von Anhängen und Quarantäne-Wartung für den Agent werden erläutert.

Messaging Security Agents

Messaging Security Agents schützen Microsoft Exchange Server. Der Agent kann Bedrohungen in E-Mails abwehren, indem er die E-Mails, die den Postfachspeicher von Microsoft Exchange passieren oder zwischen dem Exchange Server und externen Zieladressen ausgetauscht werden, durchsucht. Außerdem kann der Messaging Security Agent:

- Spam reduzieren
- E-Mails anhand ihres Inhalts sperren
- Das Empfangen/Versenden von E-Mails mit Anhängen sperren oder einschränken
- Bösartige URLs in E-Mails entdecken
- Das Übertragen vertraulicher Daten verhindern

Wichtige Informationen über Messaging Security Agents

- Messaging Security Agents können nur auf Microsoft Exchange Servern installiert werden.
- Der Messaging Security Agent unterstützt einige Funktionen von Microsoft Exchange Server Enterprise nicht, wie beispielsweise die Datenverfügbarkeitsgruppe (Data Availability Group, DAG).
- Die Sicherheitsgruppenansicht in der Webkonsole zeigt alle Messaging Security Agents an. Mehrere Messaging Security Agents können nicht in einer Gruppe zusammengefasst werden. Jeder Messaging Security Agent muss einzeln verwaltet werden.
- Worry-Free Business Security sammelt mit Hilfe des Messaging Security Agents Sicherheitsinformationen von den Microsoft Exchange Servern. Der Messaging Security Agent berichtet beispielsweise Spam-Funde oder abgeschlossene Komponenten-Updates an den Security Server. Diese Informationen werden dann auf der Webkonsole angezeigt. Der Security Server erstellt anhand dieser Daten auch Protokolle und Berichte über den Sicherheitsstatus Ihrer Microsoft Exchange Server.

Jeder Bedrohungsfund erstellt einen Protokolleintrag und eine Benachrichtigung. Entdeckt der Messaging Security Agent mehrere Bedrohungen in einer E-Mail, werden dementsprechend mehrere Protokolleinträge und Benachrichtigungen erstellt. Dieselbe Bedrohung kann besonders dann mehrmals entdeckt werden, wenn Sie den Cache-Modus in Outlook 2003 verwenden. Bei aktiviertem Cache-Modus wird eine Bedrohung möglicherweise sowohl im Warteschlangenverzeichnis als auch im Ordner der gesendeten Objekte oder im Postausgang entdeckt.

- Auf Computern mit Microsoft Exchange Server 2007 verwendet der Messaging Security Agent eine SQL-Serverdatenbank. Um Probleme zu vermeiden, sind die Messaging Security Agent Dienste von der SQL-Server-Dienstinstanz `MSSQL$SCANMAIL` abhängig. Sobald diese Instanz beendet oder neu gestartet wird, werden auch die folgenden Messaging Security Agent Dienste beendet:

  - `ScanMail_Master`
  - `ScanMail_RemoteConfig`

  Starten Sie diese Dienste manuell neu, falls `MSSQL$SCANMAIL` beendet oder neu gestartet wird. `MSSQL$SCANMAIL` wird beendet oder neu gestartet, wenn beispielsweise der SQL-Server aktualisiert wird.

So durchsucht der Messaging Security Agent E-Mails

Der Messaging Security Agent durchsucht E-Mails nach folgendem Muster:

1. Suche nach Spam (Anti-Spam)

   a. Vergleich der E-Mail mit den vom Administrator erstellten Listen der zulässigen oder gesperrten Absender

   b. Suche nach Phishing-Vorfällen

   c. Vergleich der E-Mail mit der Ausnahmeliste von Trend Micro

   d. Vergleich der E-Mail mit der Spam-Signaturdatenbank

   e. Anwendung heuristischer Suchregeln

2. Suche nach Content-Filter-Verstößen
3. Suche nach Anhängen, die gegen benutzerdefinierte Parameter verstoßen
4. Suche nach Viren und Malware (Virenschutz)
5. Suche nach bösartigen URLs

Standardeinstellungen des Messaging Security Agents

Stellen Sie fest, wie Sie Ihre Konfiguration des Messaging Security Agents anhand der Optionen in der Tabelle optimieren können.

Tabelle 6-1. Trend Micro Standardaktionen für den Messaging Security Agent

Suchoption	Echtzeitsuche	Manuelle und zeitgesteuerte Suche
Anti-spam		
Spam	Nachricht in den Spam-Ordner des Benutzers verschieben (Standard bei installiertem Junk-Ordner von Outlook oder dem End User Quarantine Tool)	Nicht zutreffend
Phishing	Gesamte Nachricht löschen	Nicht zutreffend
Content-Filter		
Nachrichten filtern, die eine der definierten Bedingungen erfüllen	Gesamte Nachricht in Quarantäne	Ersetzen
Nachrichten filtern, die jede der definierten Bedingungen erfüllen	Gesamte Nachricht in Quarantäne	Nicht zutreffend

Suchoption	Echtzeitsuche	Manuelle und zeitgesteuerte Suche
Den Inhalt von Nachrichten bestimmter E-Mail-Konten überprüfen	Gesamte Nachricht in Quarantäne	Ersetzen
Eine Ausnahme für bestimmte E-Mail-Konten erstellen	Bestanden	Bestanden
Sperren von Anhängen		
Aktion	Anhang mit Text/Datei ersetzen	Anhang mit Text/Datei ersetzen
Sonstiger		
Verschlüsselte und kennwortgeschützte Dateien	Übergehen (Bei Auswahl der Aktion Übergehen werden verschlüsselte und kennwortgeschützte Dateien übergangen, und es wird kein Protokolleintrag erstellt.)	Übergehen (Bei Auswahl der Aktion Übergehen werden verschlüsselte und kennwortgeschützte Dateien übergangen, und es wird kein Protokolleintrag erstellt.)
Ausgeschlossene Dateien (Dateien über spezielle Sucheinschränkungen)	Übergehen (Bei Auswahl der Aktion Übergehen werden Dateien oder Nachrichtentexte über die vorgegebenen Sucheinschränkungen übergangen, und es wird kein Protokolleintrag erstellt.)	Übergehen (Bei Auswahl der Aktion Übergehen werden Dateien oder Nachrichtentexte über die vorgegebenen Sucheinschränkungen übergangen, und es wird kein Protokolleintrag erstellt.)

Echtzeitsuche für Messaging Security Agents

Die Echtzeitsuche wird kontinuierlich und dauerhaft ausgeführt. Die Echtzeitsuche für den **Messaging Security Agent** (nur Advanced) überwacht alle bekannten Vireneintrittspunkte und durchsucht den gesamten eingehenden Nachrichtenverkehr, SMTP-Nachrichten, Dokumente in

Freigabeordnern sowie von anderen Microsoft Exchange Servern replizierte Dateien in Echtzeit.

Die Echtzeitsuche für Messaging Security Agents konfigurieren

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.
4. Klicken Sie auf **Virenschutz**.

   Ein neues Fenster wird angezeigt.
5. Wählen Sie **Echtzeit-Virenschutz aktivieren**.
6. Sucheinstellungen konfigurieren. Weitere Informationen finden Sie unter *Suchziele und Aktionen für Messaging Security Agents auf Seite 7-18*.
7. Klicken Sie auf **Speichern**.

   Konfigurieren Sie, welche Benutzer bei Ereignissen benachrichtigt werden sollen. Weitere Informationen finden Sie unter *Ereignisse für Benachrichtigungen konfigurieren auf Seite 10-4*.

Anti-Spam

Worry-Free Business Security bietet zwei Möglichkeiten zur Spam-Abwehr: **Email Reputation** und **Content-Suche**.

Um Spam- und Phishing-Mails auszufiltern, verwendet der Messaging Security Agent die folgenden Komponenten:

- Trend Micro Anti-Spam Engine
- Trend Micro Spam-Pattern-Dateien

Sowohl die Engine als auch die Pattern-Datei werden von Trend Micro regelmäßig aktualisiert und als Download zur Verfügung gestellt. Mit Hilfe eines manuellen oder zeitgesteuerten Updates kann der Security Server diese Komponenten herunterladen.

Die Anti-Spam Engine filtert E-Mails anhand von Spam-Signaturen und heuristischen Regeln. Sie durchsucht E-Mails und weist jeder Nachricht gemäß ihrer Übereinstimmung mit den Regeln und Pattern aus der Pattern-Datei einen bestimmten Spam-Wert zu. Der Messaging Security Agent vergleicht den Spam-Wert mit der benutzerdefinierten Stufe der Spam-Erkennung. Liegt der Spam-Wert über dieser Stufe, ergreift der Agent die entsprechenden Aktionen gegen die Spam-Mail.

Beispiel: Spammer verwenden in ihren E-Mails oft Ausrufezeichen oder setzen sogar mehrere Ausrufezeichen hintereinander. Entdeckt der Messaging Security Agent eine solche Nachricht, erhöht er automatisch den Spam-Wert für diese E-Mail.

Tipp

Zusätzlich zur Anti-Spam-Funktion können Sie den Content-Filter für die Überprüfung der Nachrichtenkopfzeile, des Betreffs sowie des Nachrichtentextes und der Informationen über den Dateianhang konfigurieren, um damit Spam und andere unerwünschte Inhalte auszufiltern.

Der Benutzer kann die Art und Weise, wie die Anti-Spam Engine Spam-Werte zuweist, nicht ändern, aber er kann die Stufe der Spam-Erkennung anpassen, mit der der Messaging Security Agent zwischen Spam und rechtmäßigen E-Mails unterscheidet.

Hinweis

Microsoft Outlook kann Nachrichten, die der Messaging Security Agent als Spam identifiziert hat, automatisch filtern und an den Junk-Mail-Ordner senden.

Email Reputation

Die Email Reputation Technologie stuft Spam gemäß der Vertrauenswürdigkeit des sendenden MTAs (Mail Transport Agent) ein und entbindet dadurch den Security Server von dieser Aufgabe. Bei aktivierter Email Reputation wird der gesamte eingehende SMTP-Datenverkehr von den IP-Datenbanken geprüft, um zu ermitteln, ob die sendende IP-Adresse zulässig ist oder als bekannter Spam-Überträger gelistet ist.

Für Email Reputation gibt es zwei Service-Level. Diese sind:

- **Standard**: Der Service-Level Standard verwendet eine Datenbank, die die Vertrauenswürdigkeit von mehr als zwei Milliarden IP-Adressen nachverfolgt. IP-Adressen, die immer wieder mit Spam-Nachrichten in Verbindung gebracht werden, werden in die Datenbank aufgenommen und nur in seltenen Fällen entfernt.
- **Advanced**: Dieser Service-Level basiert auf DNS und Abfragen, ähnlich dem Service-Level Standard. Das wichtigste Element dieses Service ist die Standard-Reputationsdatenbank, die gemeinsam mit der dynamischen Echtzeit-Reputationsdatenbank Nachrichten bekannter und verdächtiger Spam-Quellen sperrt.

Wird eine E-Mail-Nachricht einer gesperrten oder verdächtigen IP-Adresse gefunden, sperrt Email Reputation die Nachricht, bevor diese das Gateway erreicht.

Email Reputation konfigurieren

Konfigurieren Sie Email Reputation, um Nachrichten von bekannten oder verdächtigen Spam-Quellen zu sperren. Erstellen Sie außerdem Ausschlüsse zum Zulassen oder Sperren von Nachrichten anderer Absender.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.

3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.

4. Klicken Sie auf **Anti-Spam** > **Email Reputation**.

   Ein neues Fenster wird angezeigt.

5. Aktualisieren Sie auf der Registerkarte **Ziel** folgende Optionen bei Bedarf:

   - **Echtzeit-Anti-Spam aktivieren (Email Reputation)**
   - **Service-Level**:
     - **Standard**
     - **Advanced**
   - **Zulässige IP-Adressen**: E-Mail-Nachrichten von diesen IP-Adressen werden nie gesperrt. Geben Sie die IP-Adresse ein, die Sie zulassen möchten, und klicken Sie auf **Hinzufügen**. Bei Bedarf können Sie eine Liste mit IP-Adressen aus einer Textdatei importieren. Um eine IP-Adresse zu entfernen, wählen Sie die Adresse aus, und klicken Sie auf **Entfernen**.
   - **Gesperrte IP-Adressen**: E-Mail-Nachrichten von diesen IP-Adressen werden immer gesperrt. Geben Sie die zu sperrende IP-Adresse ein, und klicken Sie auf **Hinzufügen**. Bei Bedarf können Sie eine Liste mit IP-Adressen aus einer Textdatei importieren. Um eine IP-Adresse zu entfernen, wählen Sie die Adresse aus, und klicken Sie auf **Entfernen**.

6. Klicken Sie auf **Speichern**.

7. Gehen Sie auf: https://ers.trendmicro.com/?lang=de_de, um Berichte anzuzeigen.

Hinweis

Email Reputation ist ein webbasierter Service. Administratoren können den Service-Level nur über die Webkonsole konfigurieren.

Content-Suche

Die Content-Suche ermittelt Spam auf Grundlage des Inhalts der Nachricht und nicht anhand der IP-Adresse des Senders. Der Messaging Security Agent verwendet bei der Spam-Suche in E-Mails die Trend Micro Anti-Spam Engine und Spam-Pattern-Dateien, bevor er die betreffenden Dateien an den Informationsspeicher sendet. Der Microsoft Exchange Server verarbeitet abgewiesene Spam-Nachrichten nicht weiter, so dass diese Nachrichten nicht in die Postfächer der Benutzer gelangen.

Hinweis

Verwechseln Sie die Content-Suche (auf Signaturen und heuristischen Techniken basierende Anti-Spam-Funktionalität) nicht mit dem Content-Filter (auf kategorisierten Schlüsselwörtern basierendes Durchsuchen und Sperren von E-Mails). Weitere Informationen finden Sie unter *Content-Filter auf Seite 6-16*.

Content-Suche konfigurieren

Der Messaging Security Agent entdeckt Spam-Nachrichten in **Echtzeit** und ergreift die entsprechende Aktion zum Schutz der Microsoft Exchange Server.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.

4. Klicken Sie auf **Anti-Spam** > **Content-Suche**.

   Ein neues Fenster wird angezeigt.

5. Wählen Sie **Echtzeit-Anti-Spam aktivieren**.

6. Wählen Sie die Registerkarte **Ziel**, um die Methode und die Spam-Erkennungsrate festzulegen, mit der der Messaging Security Agent Spam-Mails ausfiltert:

   a. Wählen Sie in der Liste "Spam-Erkennungsrate" eine der Einstellungen **Niedrig**, **Mittel** oder **Hoch**. Mit dieser Einstellung filtert Messaging Security Agent alle Nachrichten.

      - **Hoch**: Dies ist die strengste Stufe der Spam-Erkennung. Der Messaging Security Agent durchsucht alle E-Mail-Nachrichten nach verdächtigen Dateien oder verdächtigem Text, aber die Wahrscheinlichkeit von Fehlalarmen ist hoch. Fehlalarme sind E-Mail-Nachrichten, die der Messaging Security Agent als Spam ausfiltert, obwohl es sich dabei um zulässige E-Mails handelt.

      - **Mittel**: Dies ist die empfohlene Standardeinstellung. Der Messaging Security Agent überwacht mit einer hohen Spam-Erkennungsstufe und einer relativ geringen Wahrscheinlichkeit von Fehlalarmen.

      - **Niedrig**: Dies ist die niedrigste Stufe der Spam-Erkennung. Hier filtert der Messaging Security Agent nur die am häufigsten verwendeten, offensichtlichen Spam-Nachrichten aus, aber die Wahrscheinlichkeit von Fehlalarmen ist sehr gering. Nach Spam-Rate ausfiltern.

   b. Klicken Sie auf **Phishing-Vorfälle erkennen**, damit der Messaging Security Agent Phishing-Vorfälle ausfiltert. Weitere Informationen finden Sie unter *Phishing-Vorfälle auf Seite 1-13*.

   c. Fügen Sie Adressen zur Liste der "Zulässigen Absender" oder der "Gesperrten Absender" hinzu. Weitere Informationen finden Sie unter *Listen der zulässigen und der gesperrten Absender auf Seite 6-13*.

      - **Zulässige Absender**: E-Mail-Nachrichten von diesen Adressen oder Domain-Namen werden nie gesperrt. Geben Sie die

Adressen oder Domain-Namen ein, die zugelassen werden sollen, und klicken Sie auf **Hinzufügen**. Bei Bedarf können Sie eine Liste mit Adressen oder Domain-Namen aus einer Textdatei importieren. Um Adressen oder Domain-Namen zu entfernen, wählen Sie die entsprechende Adresse aus, und klicken Sie auf **Entfernen**.

- **Gesperrte Absender**: E-Mail-Nachrichten von diesen Adressen oder Domain-Namen werden immer gesperrt. Geben Sie die Adressen oder Domain-Namen ein, die gesperrt werden sollen, und klicken Sie auf **Hinzufügen**. Bei Bedarf können Sie eine Liste mit Adressen oder Domain-Namen aus einer Textdatei importieren. Um Adressen oder Domain-Namen zu entfernen, wählen Sie die entsprechende Adresse aus, und klicken Sie auf **Entfernen**.

Hinweis

Der Microsoft Exchange Administrator verwaltet für den Exchange Server eine separate Liste der zulässigen und gesperrten Absender. Definiert ein Endbenutzer einen Absender als zulässig, der in der Administrator-Liste der gesperrten Absender enthalten ist, kennzeichnet Messaging Security Agent Nachrichten von diesem gesperrten Absender als Spam und ergreift die entsprechende Aktion.

7. Wählen Sie die Registerkarte **Aktion**, um festzulegen, welche Aktionen der Messaging Security Agent beim Fund einer Spam-Nachricht oder eines Phishing-Vorfalls ausführt.

Hinweis

Weitere Informationen über Aktionen finden Sie unter *Suchziele und Aktionen für Messaging Security Agents auf Seite 7-18*.

Der Messaging Security Agent führt je nach Konfiguration eine der folgenden Aktionen durch:

- **Quarantäne-Nachrichten in den Spam-Ordner auf dem Server verschieben**

- **Nachricht in den Spam-Ordner des Benutzers verschieben**

  Hinweis

  Konfigurieren Sie das End User Quarantine Tool, wenn Sie diese Aktion auswählen Weitere Informationen finden Sie unter *Spam-Wartung konfigurieren auf Seite 6-77*.

- **Gesamte Nachricht löschen**
- **Markieren und senden**

8. Klicken Sie auf **Speichern**.

Listen der zulässigen und der gesperrten Absender

Die Liste der zulässigen Absender enthält vertrauenswürdige E-Mail-Adressen. Der Messaging Security Agent filtert Nachrichten von diesen Adressen nur dann nach Spam aus, wenn die Option **Phishing-Vorfälle erkennen** aktiviert ist. Wenn **Phishing-Vorfälle erkennen** aktiviert ist und der Agent in einer E-Mail einen Phishing-Vorfall erkennt, wird die E-Mail nicht zugestellt, auch wenn der Absender in der Liste der zulässigen Absender enthalten ist. Die Liste der gesperrten Absender enthält nicht vertrauenswürdige E-Mail-Adressen. Der Agent kennzeichnet E-Mails von Absendern aus dieser Liste immer als Spam und führt die entsprechende Aktion aus.

Es gibt zwei Listen der zulässigen Absender: eine für den Microsoft Exchange Administrator und eine für die Endbenutzer.

- Die Listen der zulässigen oder gesperrten Absender des Microsoft Exchange Administrators (im Fenster **Anti-Spam**) legen fest, wie der Messaging Security Agent mit E-Mail-Nachrichten für den Microsoft Exchange Server verfährt.
- Der Endbenutzer verwaltet den Spam-Ordner, der während der Installation erstellt wird. Die Listen der Endbenutzer beeinflussen nur die Weiterleitung der Nachrichten, die auf dem Server für den jeweiligen Endbenutzer gespeichert werden.

Allgemeine Richtlinien

- Die Listen der zulässigen und gesperrten Absender auf einem Microsoft Exchange Server heben die Listen der zulässigen und gesperrten Absender auf einem Client auf. Befindet sich beispielsweise die E-Mail-Adresse 'benutzer@beispiel.de' in der Liste der vom Administrator gesperrten Absender, und der Endbenutzer hat sie zu seiner Liste der zulässigen Absender hinzugefügt, gelangen die E-Mails von dieser Adresse in die Microsoft Exchange Speicherdatenbank und werden vom Messaging Security Agent als Spam gekennzeichnet. Die entsprechenden Aktionen werden durchgeführt. Wenn der Agent die Aktion Quarantäne-Nachrichten in den Spam-Ordner des Benutzers verschieben ausführt, versucht er, die Nachricht in den Spam-Ordner des Endbenutzers zu verschieben. Die Nachricht wird jedoch in den Posteingang des Endbenutzers umgeleitet, da der Endbenutzer die Adresse als zulässig deklariert hat.

- In Outlook sind Anzahl und Größe der Adressen in der Liste beschränkt. Um Systemfehler zu vermeiden, begrenzt der Messaging Security Agent die Anzahl der Adressen, die vom Endbenutzer in die Liste der zulässigen Absender eingetragen werden kann. Die Begrenzung ergibt sich aus Länge und Anzahl der E-Mail-Adressen.

Platzhalter verwenden

In der Liste der zulässigen oder gesperrten Absender können Platzhalter verwendet werden. Der Messaging Security Agent verwendet ein Sternchen (*) als Platzhalter.

Im Benutzernamen dürfen keine Platzhalter enthalten sein. Wenn Sie jedoch ein Muster wie z. B. '*@trend.de' eingeben, verfährt der Agent damit wie mit '@trend.de'.

Platzhalter können nur dann verwendet werden, wenn dieser:

- neben nur einem Punkt steht und der erste oder letzte Buchstabe einer Zeichenkette ist.

- links von einem @-Zeichen steht und der erste Buchstabe in der Zeichenkette ist.

- ein fehlender Bereich am Anfang oder Ende einer Zeichenkette ist und dieselbe Funktion wie ein Platzhalter hat.

Tabelle 6-2. Platzhalter in E-Mail-Adressen

Pattern	Übereinstimmung (Beispiele)	Keine Übereinstimmung (Beispiele)
paul@beispiel.com	paul@beispiel.com	Adressen, die vom Muster abweichen
@beispiel.com *@beispiel.com	paul@beispiel.com tina@beispiel.com	paul@ms1.beispiel.com paul@beispiel.com.de tina@beispiel.com.de
beispiel.com	paul@beispiel.com paul@ms1.beispiel.com tina@ms1.rd.beispiel.com tina@beispiel.com	paul@beispiel.com.de tina@meinbeispiel.com.de tim@beispiel.comon
*.beispiel.com	paul@ms1.beispiel.com tina@ms1.rd.beispiel.com tim@ms1.beispiel.com	paul@beispiel.com paul@meinbeispiel.com.de tina@ms1.beispiel.comon
beispiel.com.*	paul@beispiel.com.de paul@ms1.beispiel.com.de paul@ms1.rd.beispiel.com.de tina@beispiel.com.de	paul@beispiel.com tina@ms1.beispiel.com paul@meinbeispiel.com.de
.beispiel.com.	paul@ms1.beispiel.com.de paul@ms1.rd.beispiel.com.de tina@ms1.beispiel.com.de	paul@beispiel.com paul@ms1.beispiel.com paul@trend.beispiel.de
..*.beispiel.com *****.beispiel.com	Wie '*.beispiel.com'	

Pattern	Übereinstimmung (Beispiele)	Keine Übereinstimmung (Beispiele)
beispiel.com beispiel.com beispiel.*.com @*.beispiel.com	Ungültige Muster	

Content-Filter

Der Content-Filter überprüft eingehende und ausgehende E-Mail-Nachrichten anhand benutzerdefinierter Regeln. Jede Regel enthält eine Liste mit Schlüsselwörtern und Ausdrücken. Der Content-Filter überprüft Header und/oder Inhalt von Nachrichten durch Vergleich der Nachrichten mit einer Schlüsselwörterliste. Wenn der Content-Filter ein Wort findet, das mit einem Schlüsselwort übereinstimmt, kann eine Aktion durchgeführt werden. Damit wird verhindert, dass der unerwünschte Inhalt an die Microsoft Exchange Clients gesendet wird. Der Messaging Security Agent kann bei jeder Aktion gegen unerwünschte Inhalte eine Benachrichtigung versenden.

Hinweis

Verwechseln Sie die Content-Suche (auf Signaturen und heuristischen Techniken basierende Anti-Spam-Funktionalität) nicht mit dem Content-Filter (auf kategorisierten Schlüsselwörtern basierendes Durchsuchen und Sperren von E-Mails). Weitere Informationen finden Sie unter *Content-Suche auf Seite 6-10*.

Mit Hilfe des Content-Filters kann der Administrator den E-Mail-Versand anhand des Nachrichtentextes überprüfen und kontrollieren. So lassen sich eingehende und ausgehende Nachrichten überwachen und auf belästigende, anstößige oder in sonstiger Weise unerwünschte Inhalte prüfen. Der Content-Filter enthält auch eine Funktion zur Synonymprüfung, mit der Sie den Gültigkeitsbereich Ihrer Richtlinien erweitern können. Sie können

beispielsweise Regeln erstellen, um Inhalte nach folgenden Kriterien zu überprüfen:

- Sexuell belästigender Sprachgebrauch
- Rassistischer Sprachgebrauch
- In den Text einer E-Mail-Nachricht eingebetteter Spam

Hinweis

Der Content-Filter ist standardmäßig deaktiviert.

Content-Filter-Regeln verwalten

Der Messaging Security Agent zeigt alle Content-Filter-Regeln im Fenster **Content-Filter** an. So rufen Sie dieses Fenster auf:

- Für die Echtzeitsuche:

  Geräte > **{Messaging Security Agent}** > **Richtlinie konfigurieren** > **Content-Filter**

- Für die manuelle Suche:

  Suchen > **Manuell** > **{Messaging Security Agent erweitern}** > **Content-Filter**

- Für die zeitgesteuerte Suche:

  Suchen > **Zeitgesteuert** > **{Messaging Security Agent erweitern}** > **Content-Filter**

Prozedur

1. Zeigen Sie zusammenfassende Informationen über diese Regeln an, einschließlich:
   - **Regel**: Zum Umfang von Worry-Free Business Security gehören Standardregeln, die Inhalte gemäß folgenden Kategorien filtern: **Vulgärer Sprachgebrauch**, **Rassendiskriminierung**, **Sexuelle**

Diskriminierung, **Falschmeldungen** und **Kettenmail**. Diese Regeln sind standardmäßig deaktiviert. Sie können sie an Ihren Bedarf anpassen oder löschen. Fügen Sie Ihre eigenen Regeln hinzu, falls keine der Standardregeln Ihrem Bedarf entspricht.

- **Aktion**: Der Messaging Security Agent führt diese Aktion aus, wenn unerwünschte Inhalte gefunden werden.
- **Priorität**: Der Messaging Security Agent wendet nacheinander alle Filter in der Reihenfolge an, in der sie auf dieser Seite angezeigt werden.
- **Aktiviert**: Ein grünes Symbol steht für eine aktivierte Regel, ein rotes Symbol weist auf eine deaktivierte Regeln hin.

2. Führen Sie folgende Aufgaben durch:

Task	Schritte
Content-Filter aktivieren/ deaktivieren	Aktivieren oder deaktivieren Sie **Echtzeit-Content-Filter aktivieren** oben im Fenster.
Eine Regel hinzufügen	Klicken Sie auf **Hinzufügen**. Ein neues Fenster wird geöffnet, in dem Sie den Typ der Regel wählen können, die Sie hinzufügen möchten. Weitere Informationen hierzu finden Sie unter *Arten von Content-Filter-Regeln auf Seite 6-21*.

Task	Schritte
Eine Regel ändern	a. Klicken Sie auf den Namen der Regel. Es öffnet sich ein neues Fenster. b. Die Optionen, die im Fenster verfügbar sind, hängen vom Typ der Regel ab. Prüfe Sie die kurze Pfadangabe oben im Fenster und beachten Sie den zweiten Eintrag in der kurzen Pfadangabe, um den Typ der Regel zu bestimmen. Beispiel: Content-Filtering > **Beliebige Bedingung erfüllen** > Regel bearbeiten Weitere Informationen zu Einstellungen von Regeln, die Sie ändern können, finden Sie unter folgenden Themen: • *Content-Filter-Regel für ein beliebiges Übereinstimmungskriterium hinzufügen auf Seite 6-25* • *Content-Filter-Regel für alle Übereinstimmungskriterien hinzufügen auf Seite 6-22* **Hinweis** Dieser Regeltyp steht für manuelle und zeitgesteuerte Content-Filter-Suchen nicht zur Verfügung. • *Content-Filter-Überwachungsregel hinzufügen auf Seite 6-28* • *Ausnahmen für Content-Filter-Regeln erstellen auf Seite 6-32*

Task	Schritte
Regeln neu ordnen	Die Content-Filter-Regeln werden vom Messaging Security Agent in der im Fenster **Content-Filter** angezeigten Reihenfolge auf E-Mails angewendet. Legen Sie die Reihenfolge fest, nach der die Regeln angewendet werden. Der Agent filtert alle E-Mails gemäß jeder Regel, bis ein Content-Verstoß eine Aktion auslöst (z. B. Löschen oder Quarantäne), und die Suche angehalten wird. Ändern Sie die Reihenfolge dieser Regeln, um den Filtervorgang zu optimieren. a. Aktivieren Sie das Kontrollkästchen für die Regel, deren Reihenfolge Sie ändern möchten. b. Klicken Sie auf **Neu ordnen**. Die Reihenfolgenummer für die Regel wird umrahmt. c. Löschen Sie im Feld der Spalte **Priorität** die bestehende Reihenfolgennummer, und geben Sie eine neue ein. **Hinweis** Vergewissern Sie sich, dass die eingegebene Nummer nicht größer ist als die Gesamtzahl der Regeln in der Liste. Wenn Sie eine größere Nummer als die Gesamtzahl der Regeln eingeben, wird der Wert von Worry-Free Business Security verworfen, und die Reihenfolge der Regel wird nicht geändert. d. Klicken Sie auf **Neue Anordnung speichern**. Die Regel wird an die eingegebene Prioritätsebene verschoben, und alle anderen Reihenfolgennummern der Regeln werden entsprechend geändert. Wenn Sie beispielsweise die Regel mit der Nummer 5 wählen und in 3 ändern, bleiben die Nummern 1 und 2 unverändert. Ab der Regel mit der Nummer 3 werden alle Nummern um 1 erhöht.
Regeln aktivieren/ deaktivieren	Klicken Sie auf das Symbol unter der Spalte Aktiviert.

Task	Schritte
Regeln entfernen	Wenn Sie eine Regel löschen, aktualisiert der Messaging Security Agent die Reihenfolge der anderen Regeln. **Hinweis** Eine gelöschte Regel kann nicht wiederhergestellt werden. Deaktivieren Sie eine Regel, anstatt sie zu löschen. a. Wählen Sie eine Regel aus. b. Klicken Sie auf **Entfernen**.

3. Klicken Sie auf **Speichern**.

Arten von Content-Filter-Regeln

Sie können Regeln erstellen, mit denen E-Mails entsprechend der von Ihnen festgelegten Bedingungen oder nach Absender- oder Empfängeradresse gefiltert werden. Als Bedingung können Sie in der Regel angeben, welche Header-Felder durchsucht werden sollen, ob der Nachrichtentext der E-Mail durchsucht werden soll oder nicht, und nach welchen Schlüsselwörtern gesucht werden soll.

Regeln können für folgende Aktionen erstellt werden:

- **Nachrichten filtern, die eine der definierten Bedingungen erfüllen**: Mit dieser Regel können Sie Inhalte aus allen Nachrichten im Rahmen einer Suche filtern. Weitere Informationen finden Sie unter *Content-Filter-Regel für ein beliebiges Übereinstimmungskriterium hinzufügen auf Seite 6-25*.

- **Nachrichten filtern, die jede der definierten Bedingungen erfüllen**: Mit dieser Regel können Sie Inhalte aus allen Nachrichten im Rahmen einer Suche filtern. Weitere Informationen finden Sie unter *Content-Filter-Regel für alle Übereinstimmungskriterien hinzufügen auf Seite 6-22*.

Hinweis

Dieser Regeltyp steht für manuelle und zeitgesteuerte Content-Filter-Suchen nicht zur Verfügung.

- **Den Inhalt von Nachrichten bestimmter E-Mail-Konten überprüfen**: Mit dieser Regel können Sie den Inhalt von Nachrichten bestimmter E-Mail-Konten überprüfen. Regeln zur Überwachung sind vergleichbar mit allgemeinen Content-Filter-Regeln, mit der Ausnahme, dass sie nur Inhalte bestimmter E-Mail-Konten filtern. Weitere Informationen finden Sie unter *Content-Filter-Überwachungsregel hinzufügen auf Seite 6-28*.
- **Ausnahmen für bestimmte E-Mail-Konten erstellen**: Mit dieser Regel wird eine Ausnahme für bestimmte E-Mail-Konten erstellt. Wenn Sie ein bestimmtes E-Mail-Konto ausschließen, wird dieses Konto nicht mehr auf Verstöße gegen Content-Regeln überprüft. Weitere Informationen finden Sie unter *Ausnahmen für Content-Filter-Regeln erstellen auf Seite 6-32*.

Nach dem Erstellen der Regel filtert der Messaging Security Agent alle ein- und ausgehenden E-Mails anhand Ihrer Regel. Verstößt eine E-Mail gegen eine Content-Regel, führt der Messaging Security Agent die entsprechende Aktion durch. Diese Aktion hängt auch von den Aktionen ab, die Sie in Ihrer Regel festgelegt haben.

Content-Filter-Regel für alle Übereinstimmungskriterien hinzufügen

Dieser Regeltyp steht für manuelle und zeitgesteuerte Content-Filter-Suchen nicht zur Verfügung.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

Ein neues Fenster wird angezeigt.

4. Klicken Sie auf **Content-Filtering**.

   Ein neues Fenster wird angezeigt.

5. Klicken Sie auf **Hinzufügen**.

   Ein neues Fenster wird angezeigt.

6. Wählen Sie die Option **Nachricht filtern, die alle festgelegten Bedingungen erfüllt**.

7. Klicken Sie auf **Weiter**.

8. Geben Sie den Namen Ihrer Regel in das Feld **Regel** ein.

9. Wählen Sie den Teil der Nachricht aus, der nach unerwünschtem Inhalt gefiltert werden soll. Der Messaging Security Agent kann E-Mails nach folgenden Elementen filtern:

   - Header (Von, An und Cc)
   - Betreff
   - Größe des Nachrichtentexts oder des Anhangs
   - Name der angehängten Datei

   Hinweis

   Der Messaging Security Agent kann den Inhalt des Headers oder des Betreffs nur während der Echtzeitsuche filtern.

10. Klicken Sie auf **Weiter**.

11. Wählen Sie die Aktion aus, die der Messaging Security Agent beim Fund von unerwünschten Inhalten durchführen soll. Der Messaging Security Agent kann die folgenden Aktionen ausführen (Beschreibungen finden Sie unter *Suchziele und Aktionen für Messaging Security Agents auf Seite 7-18*):

    - Durch Text/Datei ersetzen

Hinweis

Text in den Feldern "Von", "An", "CC" oder "Betreff" kann nicht ersetzt werden.

- Gesamte Nachricht in Quarantäne
- Nachrichtenteil in Quarantäne
- Gesamte Nachricht löschen
- Archivieren
- Gesamte Nachricht übergehen

12. Wählen Sie die Option **Empfänger benachrichtigen**, damit der Messaging Security Agent die beabsichtigten Empfänger von E-Mails mit gefiltertem Inhalt benachrichtigt.

Wählen Sie die Option **Externe Empfänger nicht benachrichtigen**, damit nur interne Nachrichten-Empfänger benachrichtigt werden. Legen Sie interne Adressen unter **Aktionen** > **Einstellungen für die Benachrichtigung** > **Interne Nachrichtendefinition** fest.

13. Wählen Sie die Option **Absender benachrichtigen**, damit der Messaging Security Agent die Absender von E-Mails mit gefiltertem Inhalt benachrichtigt.

Wählen Sie die Option **Externe Absender nicht benachrichtigen**, damit nur interne Nachrichten-Absender benachrichtigt werden. Legen Sie interne Adressen unter **Aktionen** > **Einstellungen für die Benachrichtigung** > **Interne Nachrichtendefinition** fest.

14. Klicken Sie im Abschnitt **Erweiterte Optionen** auf das Plussymbol (+), um den Unterabschnitt **Archivierungseinstellungen** zu öffnen.

a. Geben Sie in das Feld **Quarantäne-Ordner** den Pfad zum Ordner für die Funktion Content-Filter ein, in den die E-Mail in Quarantäne verschoben wird, oder akzeptieren Sie den Standardwert: `<Messaging Security Agent-Installationsordner>\storage\quarantine`

b. Geben Sie in das Feld **Archivverzeichnis** den Pfad zum Ordner für die Funktion Content-Filter ein, in den die E-Mail in Quarantäne verschoben wird, oder akzeptieren Sie den Standardwert: `<Messaging Security Agent-Installationsordner>\storage\Sicherung für Content-Filter`

15. Klicken Sie auf das Plussymbol (+), um den Unterabschnitt **Einstellungen für das Ersetzen** zu erweitern.

a. Geben Sie in das Feld **Name der Ersetzungsdatei** den Namen der Datei ein, mit der die Funktion Content-Filter eine E-Mail ersetzt, wenn eine Regel mit der Aktion 'Durch Text/Datei ersetzen' ausgelöst wurde, oder akzeptieren Sie den Standardwert.

b. Geben oder fügen Sie in das Feld **Neuer Text** den Inhalt des Ersetzungstextes ein, den die Funktion Content-Filter verwenden soll, wenn eine E-Mail eine Regel mit der Aktion 'Durch Text/Datei ersetzen' auslöst, oder akzeptieren Sie den Standardtext.

16. Klicken Sie auf **Fertig stellen**.

Der Assistent wird beendet, und Sie kehren zum Fenster "Content-Filter" zurück.

Content-Filter-Regel für ein beliebiges Übereinstimmungskriterium hinzufügen

- Für die Echtzeitsuche:

  Geräte > **{Messaging Security Agent}** > **Richtlinie konfigurieren** > **Content-Filter**

- Für die manuelle Suche:

  Suchen > **Manuell** > **{Messaging Security Agent erweitern}** > **Content-Filter**

- Für die zeitgesteuerte Suche:

Suchen > **Zeitgesteuert** > **{Messaging Security Agent erweitern}** > **Content-Filter**

Prozedur

1. Klicken Sie auf **Hinzufügen**.

   Ein neues Fenster wird angezeigt.

2. Wählen Sie die Option **Nachrichten filtern, die eine der definierten Bedingungen erfüllen**.

3. Klicken Sie auf **Weiter**.

4. Geben Sie den Namen Ihrer Regel in das Feld **Regel** ein.

5. Wählen Sie den Teil der Nachricht aus, der nach unerwünschtem Inhalt gefiltert werden soll. Der Messaging Security Agent kann E-Mails nach folgenden Elementen filtern:

   - Header (Von, An und Cc)
   - Betreff
   - Text
   - Anhang

   Hinweis

   Der Messaging Security Agent kann den Inhalt des Headers oder des Betreffs nur während der Echtzeitsuche filtern.

6. Klicken Sie auf **Weiter**.

7. Ändern Sie die Schlüsselwörter für den Teil, den Sie auf unerwünschte Inhalte durchsuchen möchten. Informationen zum Arbeiten mit Schlüsselwörtern finden Sie unter *Schlüsselwörter auf Seite D-5*.

   a. Aktivieren Sie ggf. die Groß- und Kleinschreibung für den Content-Filter.

b. Importieren Sie neue Schlüsselwort-Dateien nach Bedarf aus einer `.TXT`-Datei.

c. Legen Sie eine Liste mit Synonymen fest.

8. Klicken Sie auf **Weiter**.

9. Wählen Sie die Aktion aus, die der Messaging Security Agent beim Fund von unerwünschten Inhalten durchführen soll. Der Messaging Security Agent kann die folgenden Aktionen ausführen (Beschreibungen finden Sie unter *Suchziele und Aktionen für Messaging Security Agents auf Seite 7-18*):

- Durch Text/Datei ersetzen

  Hinweis

  Text in den Feldern "Von", "An", "CC" oder "Betreff" kann nicht ersetzt werden.

- Gesamte Nachricht in Quarantäne
- Nachrichtenteil in Quarantäne
- Gesamte Nachricht löschen
- Archivieren

10. Wählen Sie die Option **Empfänger benachrichtigen**, damit der Messaging Security Agent die beabsichtigten Empfänger von E-Mails mit gefiltertem Inhalt benachrichtigt.

Wählen Sie die Option **Externe Empfänger nicht benachrichtigen**, damit nur interne Nachrichten-Empfänger benachrichtigt werden. Legen Sie interne Adressen unter **Aktionen** > **Einstellungen für die Benachrichtigung** > **Interne Nachrichtendefinition** fest.

11. Wählen Sie die Option **Absender benachrichtigen**, damit der Messaging Security Agent die Absender von E-Mails mit gefiltertem Inhalt benachrichtigt.

Wählen Sie die Option **Externe Absender nicht benachrichtigen**, damit nur interne Nachrichten-Absender benachrichtigt werden. Legen Sie

interne Adressen unter **Aktionen** > **Einstellungen für die Benachrichtigung** > **Interne Nachrichtendefinition** fest.

12. Klicken Sie im Abschnitt **Erweiterte Optionen** auf das Plussymbol (+), um den Unterabschnitt **Archivierungseinstellungen** zu öffnen.

    a. Geben Sie in das Feld **Quarantäne-Ordner** den Pfad zum Ordner für die Funktion Content-Filter ein, in den die E-Mail in Quarantäne verschoben wird, oder akzeptieren Sie den Standardwert: `<Messaging Security Agent-Installationsordner>\storage\quarantine`

    b. Geben Sie in das Feld **Archivverzeichnis** den Pfad zum Ordner für die Funktion Content-Filter ein, in den die E-Mail in Quarantäne verschoben wird, oder akzeptieren Sie den Standardwert: `<Messaging Security Agent-Installationsordner>\storage\Sicherung für Content-Filter`

13. Klicken Sie auf das Plussymbol (+), um den Unterabschnitt **Einstellungen für das Ersetzen** zu erweitern.

    a. Geben Sie in das Feld **Name der Ersetzungsdatei** den Namen der Datei ein, mit der die Funktion Content-Filter eine E-Mail ersetzt, wenn eine Regel mit der Aktion ‘Durch Text/Datei ersetzen’ ausgelöst wurde, oder akzeptieren Sie den Standardwert.

    b. Geben oder fügen Sie in das Feld **Neuer Text** den Inhalt des Ersetzungstextes ein, den die Funktion Content-Filter verwenden soll, wenn eine E-Mail eine Regel mit der Aktion ‘Durch Text/Datei ersetzen’ auslöst, oder akzeptieren Sie den Standardtext.

14. Klicken Sie auf **Fertig stellen**.

    Der Assistent wird beendet, und Sie kehren zum Fenster "Content-Filter" zurück.

Content-Filter-Überwachungsregel hinzufügen

- Für die Echtzeitsuche:

Geräte > **{Messaging Security Agent}** > **Richtlinie konfigurieren** > **Content-Filter**

- Für die manuelle Suche:

  Suchen > **Manuell** > **{Messaging Security Agent erweitern}** > **Content-Filter**

- Für die zeitgesteuerte Suche:

  Suchen > **Zeitgesteuert** > **{Messaging Security Agent erweitern}** > **Content-Filter**

Prozedur

1. Klicken Sie auf **Hinzufügen**.

   Ein neues Fenster wird angezeigt.

2. Wählen Sie **Den Inhalt von Nachrichten bestimmter E-Mail-Konten überprüfen**.

3. Klicken Sie auf **Weiter**.

4. Geben Sie den Namen Ihrer Regel in das Feld **Regel** ein.

5. Legen Sie die zu überwachenden Konten fest.

6. Klicken Sie auf **Weiter**.

7. Wählen Sie den Teil der Nachricht aus, der nach unerwünschtem Inhalt gefiltert werden soll. Der Messaging Security Agent kann E-Mails nach folgenden Elementen filtern:

   - Betreff
   - Text
   - Anhang

Hinweis

Der Messaging Security Agent kann diese Teile einer E-Mail-Nachricht nur während der Echtzeitsuche filtern. Das Filtern von Header- und Betreff-Inhalten wird bei der manuellen und zeitgesteuerten Suche nicht unterstützt.

8. Ändern Sie die Schlüsselwörter für den Teil, den Sie auf unerwünschte Inhalte durchsuchen möchten. Informationen zum Arbeiten mit Schlüsselwörtern finden Sie unter *Schlüsselwörter auf Seite D-5*.

   a. Aktivieren Sie ggf. die Groß- und Kleinschreibung für den Content-Filter.

   b. Importieren Sie neue Schlüsselwort-Dateien nach Bedarf aus einer `.TXT`-Datei.

   c. Legen Sie eine Liste mit Synonymen fest.

9. Klicken Sie auf **Weiter**.

10. Wählen Sie die Aktion aus, die der Messaging Security Agent beim Fund von unerwünschten Inhalten durchführen soll. Der Messaging Security Agent kann die folgenden Aktionen ausführen (Beschreibungen finden Sie unter *Suchziele und Aktionen für Messaging Security Agents auf Seite 7-18*):

    - Durch Text/Datei ersetzen

      Hinweis

      Text in den Feldern "Von", "An", "CC" oder "Betreff" kann nicht ersetzt werden.

    - Gesamte Nachricht in Quarantäne
    - Nachrichtenteil in Quarantäne
    - Gesamte Nachricht löschen
    - Archivieren

11. Wählen Sie die Option **Empfänger benachrichtigen**, damit der Messaging Security Agent die beabsichtigten Empfänger von E-Mails mit gefiltertem Inhalt benachrichtigt.

    Wählen Sie die Option **Externe Empfänger nicht benachrichtigen**, damit nur interne Nachrichten-Empfänger benachrichtigt werden. Legen Sie interne Adressen unter **Aktionen** > **Einstellungen für die Benachrichtigung** > **Interne Nachrichtendefinition** fest.

12. Wählen Sie die Option **Absender benachrichtigen**, damit der Messaging Security Agent die Absender von E-Mails mit gefiltertem Inhalt benachrichtigt.

    Wählen Sie die Option **Externe Absender nicht benachrichtigen**, damit nur interne Nachrichten-Absender benachrichtigt werden. Legen Sie interne Adressen unter **Aktionen** > **Einstellungen für die Benachrichtigung** > **Interne Nachrichtendefinition** fest.

13. Klicken Sie im Abschnitt **Erweiterte Optionen** auf das Plussymbol (+), um den Unterabschnitt **Archivierungseinstellungen** zu öffnen.

    a. Geben Sie in das Feld **Quarantäne-Ordner** den Pfad zum Ordner für die Funktion Content-Filter ein, in den die E-Mail in Quarantäne verschoben wird, oder akzeptieren Sie den Standardwert:
    `<Messaging Security Agent-Installationsordner>\storage\quarantine`

    b. Geben Sie in das Feld **Archivverzeichnis** den Pfad zum Ordner für die Funktion Content-Filter ein, in den die E-Mail in Quarantäne verschoben wird, oder akzeptieren Sie den Standardwert:
    `<Messaging Security Agent-Installationsordner>\storage\Sicherung für Content-Filter`

14. Klicken Sie auf das Plussymbol (+), um den Unterabschnitt **Einstellungen für das Ersetzen** zu erweitern.

    a. Geben Sie in das Feld **Name der Ersetzungsdatei** den Namen der Datei ein, mit der die Funktion Content-Filter eine E-Mail ersetzt, wenn eine Regel mit der Aktion ‘Durch Text/Datei ersetzen’ ausgelöst wurde, oder akzeptieren Sie den Standardwert.

b. Geben oder fügen Sie in das Feld **Neuer Text** den Inhalt des Ersetzungstextes ein, den die Funktion Content-Filter verwenden soll, wenn eine E-Mail eine Regel mit der Aktion ‘Durch Text/Datei ersetzen’ auslöst, oder akzeptieren Sie den Standardtext.

15. Klicken Sie auf **Fertig stellen**.

Der Assistent wird beendet, und Sie kehren zum Fenster "Content-Filter" zurück.

Ausnahmen für Content-Filter-Regeln erstellen

- Für die Echtzeitsuche:

  Geräte > **{Messaging Security Agent}** > **Richtlinie konfigurieren** > **Content-Filter**

- Für die manuelle Suche:

  Suchen > **Manuell** > **{Messaging Security Agent erweitern}** > **Content-Filter**

- Für die zeitgesteuerte Suche:

  Suchen > **Zeitgesteuert** > **{Messaging Security Agent erweitern}** > **Content-Filter**

Prozedur

1. Klicken Sie auf **Hinzufügen**.

Ein neues Fenster wird angezeigt.

2. Wählen Sie **Ausnahmen für bestimmte E-Mail-Konten erstellen**.

3. Klicken Sie auf **Weiter**.

4. Geben Sie einen Regelnamen ein.

5. Geben Sie in das dafür vorgesehene Feld die E-Mail-Konten ein, die vom Content-Filtering ausgeschlossen werden sollen, und klicken Sie auf **Hinzufügen**.

   Die eingegebene Adresse wird zu Ihrer Liste der ausgenommenen E-Mail-Konten hinzugefügt. Der Messaging Security Agent wendet auf E-Mail-Konten in dieser Liste keine Content-Regeln an, deren Priorität geringer ist als die dieser Regel.

6. Wenn Sie mit der Bearbeitung der Liste fertig sind, klicken Sie auf **Fertig stellen**.

   Der Assistent wird beendet, und Sie kehren zum Fenster **Content-Filter** zurück.

Prävention vor Datenverlust

Sie können sich mit der Funktion Prävention vor Datenverlust vor Datenverlusten durch ausgehende E-Mails schützen. Mit dieser Funktion können Daten, wie beispielsweise Sozialversicherungsnummern, Telefonnummern, Kontonummern und andere vertrauliche Geschäftsdaten, die mit einem bestimmten Muster übereinstimmen, geschützt werden.

Folgende Microsoft Exchange Versionen werden in dieser Version unterstützt:

TABELLE 6-3. Unterstützte Microsoft Exchange Versionen

UNTERSTÜTZT	NICHT UNTERSTÜTZT
2007 x64	2003 x86/x64
2010 x64	2007 x86
	2010 x86

Vorbereitung

Bevor Sie vertrauliche Daten auf potenzielle Verluste hin überwachen, beantworten Sie die folgenden Fragen:

- Welche Daten müssen vor unbefugten Benutzern geschützt werden?
- Wo befinden sich diese Daten?
- Wo und wie werden diese Daten übertragen?
- Welche Benutzer sind befugt, auf diese Daten zuzugreifen oder sie zu übertragen?

Diese wichtige Prüfung erfordert normalerweise Informationen von mehreren Abteilungen und Mitarbeitern, die mit den vertraulichen Daten in Ihrem Unternehmen vertraut sind. Bei den nachfolgenden Verfahren wird vorausgesetzt, dass Sie die vertraulichen Daten identifiziert und Sicherheitsrichtlinien in Bezug auf die Handhabung vertraulicher Geschäftsdaten aufgestellt haben.

Die Funktion zur Prävention vor Datenverlust besteht aus drei grundlegenden Teilen:

- **Regeln** (Pattern, nach denen gesucht wird)
- **Domänen, die vom** Filtern ausgeschlossen werden
- **Zulässige Absender** (E-Mail-Konten, die vom Filtern ausgeschlossen werden)

Weitere Informationen finden Sie unter *Regeln zur Prävention vor Datenverlust verwalten auf Seite 6-34*.

Regeln zur Prävention vor Datenverlust verwalten

Der Messaging Security Agent zeigt alle Regeln zur Prävention vor Datenverlust im Fenster **Prävention vor Datenverlust** an (**Geräte** > **{Messaging Security Agent}** > **Richtlinie konfigurieren** > **Prävention vor Datenverlust**).

Prozedur

1. Zeigen Sie zusammenfassende Informationen über diese Regeln an, einschließlich:

   - **Regel**: Im Umfang von Worry-Free Business Security sind Standardregeln enthalten (weitere Informationen finden Sie unter *Standardregeln der Funktion Prävention vor Datenverlust auf Seite 6-42*). Diese Regeln sind standardmäßig deaktiviert. Sie können sie an Ihren Bedarf anpassen oder löschen. Fügen Sie Ihre eigenen Regeln hinzu, falls keine der Standardregeln Ihrem Bedarf entspricht.

     Tipp

     Bewegen Sie den Mauszeiger über die Regelbezeichnung, um die Regel anzuzeigen. Regeln, die einen regulären Ausdruck verwenden, werden durch ein Symbol in Form eines Vergrößerungsglases ( ) gekennzeichnet.

   - **Aktion**: Der Messaging Security Agent führt diese Aktion aus, wenn eine Regel ausgelöst wird.

   - **Priorität**: Der Messaging Security Agent wendet nacheinander alle Regeln in der Reihenfolge an, in der sie auf dieser Seite angezeigt werden.

   - **Aktiviert**: Ein grünes Symbol steht für eine aktivierte Regel, ein rotes Symbol weist auf eine deaktivierte Regeln hin.

2. Führen Sie folgende Aufgaben durch:

Task	Schritte
Prävention vor Datenverlust aktivieren/ deaktivieren	Aktivieren oder deaktivieren Sie die **Echtzeit-Prävention vor Datenverlust aktivierens** oben im Fenster.

Task	Schritte
Eine Regel hinzufügen	Klicken Sie auf **Hinzufügen**. Ein neues Fenster wird geöffnet, in dem Sie den Typ der Regel wählen können, die Sie hinzufügen möchten. Weitere Informationen hierzu finden Sie unter *Regeln zur Prävention vor Datenverlust hinzufügen auf Seite 6-43*.
Eine Regel ändern	Klicken Sie auf den Namen der Regel. Es öffnet sich ein neues Fenster. Weitere Informationen über Einstellungen von Regeln, die Sie ändern können, finden Sie unter *Regeln zur Prävention vor Datenverlust hinzufügen auf Seite 6-43*.

Regeln importieren und exportieren	Importieren Sie eine oder mehrere Regeln in eine Textdatei (oder exportieren Sie sie), wie nachstehend beschrieben. Wenn Sie wollen, können Sie die Regeln anschließend direkt in dieser Datei bearbeiten.
	
	`[SMEX_SUB_CFG_CF_RULE43ca5aea-6e75-44c5-94c9-d0b35d2be599]`
	
	`RuleName=Bubbly`
	
	`UserExample=`
	
	`Value=Bubbly`
	
	`[SMEX_SUB_CFG_CF_RULE8b752cf2-aca9-4730-a4dd-8e174f9147b6]`
	
	`RuleName=Kontonummer Master Card`
	
	`UserExample=Value=.REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b`

Task	Schritte
	Wählen Sie für den Export in eine Textdatei eine oder mehrere Regeln in der Liste aus und klicken Sie dann auf **Exportieren**. **Tipp** Sie können nur Regeln auswählen, die in einem einzigen Fenster angezeigt werden. Um Regeln auszuwählen, die momentan in verschiedenen Fenstern angezeigt werden, erhöhen Sie den Wert von 'Zeilen pro Seite', der sich oben in der Tabelle der Regelliste befindet, um ausreichend Zeilen für alle zu exportierenden Regeln anzuzeigen.
	So importieren Sie Regeln: a. Erstellen Sie eine Textdatei im oben dargestellten Format. Sie können auch auf **Weitere Standardregeln herunterladen** unter der Tabelle klicken und die Regeln dann speichern. b. Klicken Sie auf **Importieren**. Ein neues Fenster wird geöffnet. c. Klicken Sie auf **Durchsuchen**, um die zu importierende Datei auszuwählen, und klicken Sie anschließend auf **Importieren**. Die Funktion Prävention vor Datenverlust importiert die in der Datei enthaltenen Regeln und hängt diese an das Ende der aktuellen Regelliste an. **Tipp** Wenn Sie bereits mehr als 10 Regeln definiert haben, werden die importierten Regeln nicht auf der ersten Seite angezeigt. Zeigen Sie mit Hilfe der Symbole für die Seitennavigation, die sich oberhalb oder unterhalb der Regelliste befinden, die letzte Seite der Liste an. Die neu importierten Regeln sollten dort angezeigt werden.

Task	Schritte
Regeln neu ordnen	Die Regeln der Funktion Prävention vor Datenverlust werden vom Messaging Security Agent in der im Fenster **Prävention vor Datenverlust** angezeigten Reihenfolge auf E-Mails angewendet. Legen Sie die Reihenfolge fest, nach der die Regeln angewendet werden. Der Agent filtert alle E-Mails gemäß jeder Regel, bis ein Content-Verstoß eine Aktion auslöst (z. B. Löschen oder Quarantäne), und die Suche angehalten wird. Ändern Sie die Reihenfolge dieser Regeln, um die Prävention vor Datenverlust zu optimieren. a. Aktivieren Sie das Kontrollkästchen für die Regel, deren Reihenfolge Sie ändern möchten. b. Klicken Sie auf **Neu ordnen**. Die Reihenfolgenummer für die Regel wird umrahmt. c. Löschen Sie im Feld der Spalte **Priorität** die bestehende Reihenfolgennummer, und geben Sie eine neue ein. **Hinweis** Vergewissern Sie sich, dass die eingegebene Nummer nicht größer ist als die Gesamtzahl der Regeln in der Liste. Wenn Sie eine größere Nummer als die Gesamtzahl der Regeln eingeben, wird der Wert von Worry-Free Business Security verworfen, und die Reihenfolge der Regel wird nicht geändert. d. Klicken Sie auf **Neue Anordnung speichern**. Die Regel wird an die eingegebene Prioritätsebene verschoben, und alle anderen Reihenfolgennummern der Regeln werden entsprechend geändert. Wenn Sie beispielsweise die Regel mit der Nummer 5 wählen und in 3 ändern, bleiben die Nummern 1 und 2 unverändert. Ab der Regel mit der Nummer 3 werden alle Nummern um 1 erhöht.
Regeln aktivieren/ deaktivieren	Klicken Sie auf das Symbol unter der Spalte Aktiviert.

Task	Schritte
Regeln entfernen	Wenn Sie eine Regel löschen, aktualisiert der Messaging Security Agent die Reihenfolge der anderen Regeln. **Hinweis** Eine gelöschte Regel kann nicht wiederhergestellt werden. Deaktivieren Sie eine Regel, anstatt sie zu löschen. a. Wählen Sie eine Regel aus. b. Klicken Sie auf **Entfernen**.

Task	Schritte
Bestimmte Domänenkonten ausschließen	Innerhalb der Gebäude eines Unternehmens ist der Austausch vertraulicher Geschäftsdaten eine Notwendigkeit, die täglich vorkommt. Außerdem wäre die Verarbeitungslast auf Security Servern extrem hoch, wenn alle internen Nachrichten von der Funktion Prävention vor Datenverlust gefiltert werden müssten. Aus diesen Gründen müssen Sie eine oder mehrere Standarddomänen festlegen, die den firmeninternen E-Mail-Verkehr repräsentieren, damit die Funktion "Prävention vor Datenverlust" keine Nachrichten filtert, die von einem E-Mail-Konto zu einem anderen innerhalb der Unternehmensdomäne gesendet werden. Diese Liste ermöglicht, dass alle internen E-Mail-Nachrichten (innerhalb der Firmendomäne) die Regeln für die Prävention vor Datenverlust umgehen. Mindestens eine solche Domäne ist erforderlich. Sie können die Liste erweitern, wenn Sie mehr als eine Domäne verwenden. Beispiel: `*@beispiel.com` a. Klicken Sie auf das Plussymbol (+), um den Abschnitt **Bestimmte Domänenkonten, die von der Prävention vor Datenverlust ausgenommen sind** zu erweitern. b. Platzieren Sie den Cursor im Feld **Hinzufügen**, und geben Sie die Domäne mit Hilfe des folgenden Patterns ein: `*@beispiel.com` c. Klicken Sie auf **Hinzufügen**. Die Domäne wird in der Liste unterhalb des Felds **Hinzufügen** angezeigt. d. Klicken Sie auf **Speichern**, um den Prozess abzuschließen. **Warnung!** Die Funktion Prävention vor Datenverlust fügt die Domäne erst hinzu, wenn Sie auf **Speichern** klicken. Wenn Sie auf **Hinzufügen**, aber nicht auf **Speichern** klicken, wird die Domäne nicht hinzugefügt.

Task	Schritte
E-Mail-Konten zur Liste der zulässigen Absender hinzufügen	E-Mail von zulässigen Absendern wird außerhalb des Netzwerks ohne Filtern durch die Funktion "Prävention vor Datenverlust" übertragen. Die Funktion "Prävention vor Datenverlust" ignoriert den Inhalt aller E-Mails, die von E-Mail-Konten gesendet werden, die sich auf der Liste der zulässigen Konten befinden. a. Klicken Sie auf das Plussymbol (+), um den Abschnitt **Zulässige Absender** zu erweitern. b. Platzieren Sie den Cursor im Feld **Hinzufügen**, und geben Sie die vollständige E-Mail-Adresse mit Hilfe des folgenden Patterns ein: `beispiel@beispiel.com` c. Klicken Sie auf **Hinzufügen**. Die Adresse wird in der Liste unterhalb des Felds **Hinzufügen** angezeigt. d. Klicken Sie auf **Speichern**, um den Prozess abzuschließen. **Hinweis** Die Funktion Prävention vor Datenverlust fügt die Adresse erst hinzu, wenn Sie auf **Speichern** klicken. Wenn Sie auf **Hinzufügen**, aber nicht auf **Speichern** klicken, wird die Adresse nicht hinzugefügt.

Task	Schritte

E-Mail-Konten in die Liste der zulässigen Absender importieren	Sie können eine Liste von E-Mail-Adressen aus einer Textdatei importieren, die ein E-Mail-Konto pro Zeile enthält. Beispiel:
	`admin@example.com`
	`ceo@example.com`
	`president@example.com`
	a. Klicken Sie auf das Plussymbol (+), um den Abschnitt **Zulässige Absender** zu erweitern.
	b. Klicken Sie auf **Importieren**.
	Ein neues Fenster wird geöffnet.
	c. Klicken Sie auf **Durchsuchen**, um die zu importierende Textdatei auszuwählen, und klicken Sie anschließend auf **Importieren**.
	Die Funktion Prävention vor Datenverlust importiert die Regeln in der Datei und hängt diese an das Ende der aktuellen Liste an.

3. Klicken Sie auf **Speichern**.

Standardregeln der Funktion Prävention vor Datenverlust

Zum Umfang der Funktion Prävention vor Datenverlust gehören einige wenige Standardregeln, wie in nachfolgender Tabelle beschrieben.

Tabelle 6-4. Standardregeln der Funktion Prävention vor Datenverlust

Regelname	Beispiel	Regulärer Ausdruck
Kontonummer Visa Card	4111-1111-1111-1111	.REG. \b4\d{3}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
Kontonummer MasterCard	5111-1111-1111-1111	.REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b

Regelname	Beispiel	Regulärer Ausdruck
Kontonummer American Express	3111-111111-11111	.REG. \b3[4,7]\d{2}\-?\x20?\d{6}\-?\x20?\d{5}\b
Kontonummer 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-]
ISO-Datum	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\/-]

Hinweis

Über die Webkonsole kann eine ZIP-Datei mit weiteren DLP-Regeln heruntergeladen werden. Navigieren Sie zu **Sicherheitseinstellungen** > **{Messaging Security Agent}** > **Einstellungen konfigurieren** > **Prävention vor Datenverlust** , und klicken Sie auf **Weitere Standardregeln herunterladen**.

Regeln zur Prävention vor Datenverlust hinzufügen

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.
4. Klicken Sie auf **Prävention vor Datenverlust**.

Ein neues Fenster wird angezeigt.

5. Klicken Sie auf **Hinzufügen**.

   Ein neues Fenster wird angezeigt.

6. Wählen Sie den Teil der Nachricht, den Sie überprüfen möchten. Der Messaging Security Agent kann E-Mails nach folgenden Elementen filtern:

   - Header (Von, An und Cc)
   - Betreff
   - Text
   - Anhang

7. Eine Regel hinzufügen

   So fügen Sie eine schlüsselwortbasierte Regel hinzu:

   a. Wählen Sie **Schlüsselwort** aus.

   b. Geben Sie das Schlüsselwort in das angezeigte Feld ein. Das Schlüsselwort muss zwischen 1 und 64 alphanumerischen Zeichen lang sein.

   c. Klicken Sie auf **Weiter**.

   So fügen Sie eine Regel basierend auf automatisch erstellten Ausdrücken hinzu:

   a. Weitere Informationen zu Richtlinien für die Definition von regulären Ausdrücken finden Sie unter *Reguläre Ausdrücke auf Seite D-10*.

   b. Wählen Sie **Regulärer Ausdruck (automatisch erstellt)**.

   c. Geben Sie in das bereitgestellte Feld einen **Regelnamen** ein. Dabei handelt es sich um ein Pflichtfeld.

   d. Geben oder fügen Sie in das Feld **Beispiel** ein Beispiel für die Art der Zeichenfolge ein (mit einer Länge von bis zu 40 Zeichen), mit

der der reguläre Ausdruck übereinstimmen soll. Die alphanumerischen Zeichen werden als Großbuchstaben im schattierten Bereich mit Felderzeilen unterhalb des Felds **Beispiel** angezeigt.

e. Wenn der Ausdruck Konstanten enthält, wählen Sie diese aus, indem Sie auf die Felder klicken, in denen die Zeichen angezeigt werden.

   Wenn Sie auf ein Feld klicken, wird der jeweilige Rahmen rot angezeigt, um anzuzeigen, dass es sich um eine Konstante handelt. Das Tool für die automatische Generierung modifiziert den regulären Ausdruck, der unter dem schattierten Bereich angezeigt wird.

Hinweis

Nicht alphanumerische Zeichen (wie Leerzeichen, Strichpunkte und andere Satzzeichen) werden automatisch als Konstanten angesehen und können nicht in Variablen umgewandelt werden.

f. Um zu überprüfen, ob der erzeugte reguläre Ausdruck dem gewünschten Pattern entspricht, wählen Sie **Geben Sie ein weiteres Beispiel an, um die Regel zu verifizieren (optional)**.

   Ein Testfeld wird unter dieser Option angezeigt.

g. Geben Sie ein anderes Beispiel des gerade eingegebenen Patterns ein.

   Wenn dieser Ausdruck z. B. mit einer Reihe von Kontonummern mit dem Pattern '01-EX????? 20??' übereinstimmen soll, geben Sie ein anderes übereinstimmende Beispiel ein, z. B. '01-Extreme 2010', und klicken Sie anschließend auf **Test**.

   Das Tool validiert das neue Beispiel gegen den vorhandenen regulären Ausdruck. Wenn das neue Beispiel übereinstimmt, wird ein Symbol in Form eines grünen Häkchens neben das Feld platziert. Wenn der reguläre Ausdruck nicht mit dem neuen Beispiel übereinstimmt, wird ein Symbol in Form eines roten X neben das Feld gesetzt.

Warnung!

Bei regulären Ausdrücken, die von diesem Tool generiert wurden, wird die Groß-/Kleinschreibung berücksichtigt. Diese Ausdrücke können nur mit Pattern mit genau derselben Anzahl von Zeichen übereinstimmen. Sie können keine Pattern mit 'einem oder mehreren' Exemplaren eines bestimmten Zeichens auswählen.

h. Klicken Sie auf **Weiter**.

So fügen Sie eine Regel basierend auf benutzerdefinierten Ausdrücken hinzu:

Warnung!

Reguläre Ausdrücke sind ein leistungsfähiges Tool, um Übereinstimmungen mit Zeichenfolgen zu ermitteln. Vergewissern Sie sich, dass Sie mit der Syntax regulärer Ausdrücke vertraut sind, bevor Sie damit beginnen, diese Ausdrücke zu verwenden. Schlecht geschriebene reguläre Ausdrücke können die Leistung dramatisch beeinträchtigen. Trend Micro empfiehlt, zu Beginn einfache reguläre Ausdrücke zu verwenden. Beim Erstellen neuer Regeln sollten Sie die 'Archivieren'-Aktion verwenden und beobachten, wie die Funktion Prävention vor Datenverlust Nachrichten mit Hilfe dieser Regel verwaltet. Wird die Regel ohne unerwünschte Nebeneffekte ausgeführt, kann die Aktion entsprechend geändert werden.

a. Weitere Informationen zu Richtlinien für die Definition von regulären Ausdrücken finden Sie unter *Reguläre Ausdrücke auf Seite D-10*.

b. Wählen Sie **Regulärer Ausdruck (benutzerdefiniert)**.

   Die Felder **Regel** und **Regulärer Ausdruck** werden angezeigt.

c. Geben Sie in das bereitgestellte Feld einen **Regelnamen** ein. Dabei handelt es sich um ein Pflichtfeld.

d. Geben Sie in das Feld **Regulärer Ausdruck** einen regulären Ausdruck ein, der mit dem Präfix '`REG.`' beginnt und bis zu 255 Zeichen (inkl. Präfix) lang ist.

Warnung!

Beim Einfügen in dieses Feld ist besondere Vorsicht angebracht. Wenn überflüssige Zeichen wie beispielsweise ein Betriebssystem-spezifischer Zeilenumbruch oder ein HTML-Tag im Inhalt der Zwischenablage enthalten sind, wird der eingefügte Ausdruck ungenau. Aus diesem Grund empfiehlt Trend Micro, den Ausdruck von Hand einzugeben.

e. Um zu überprüfen, ob der reguläre Ausdruck dem gewünschten Pattern entspricht, wählen Sie **Geben Sie ein weiteres Beispiel an, um die Regel zu verifizieren (optional)**.

   Ein Testfeld wird unter dieser Option angezeigt.

f. Geben Sie ein anderes Beispiel des gerade eingegebenen Patterns ein (40 Zeichen oder weniger).

   Wenn dieser Ausdruck z. B. mit einer Reihe von Kontonummern mit dem Pattern 'ACC-????? 20??' übereinstimmen soll, geben Sie ein anderes übereinstimmendes Beispiel ein, z. B. 'Acc-65432 2012', und klicken Sie anschließend auf **Test**.

   Das Tool validiert das neue Beispiel gegen den vorhandenen regulären Ausdruck. Wenn das neue Beispiel übereinstimmt, wird ein Symbol in Form eines grünen Häkchens neben das Feld platziert. Wenn der reguläre Ausdruck nicht mit dem neuen Beispiel übereinstimmt, wird ein Symbol in Form eines roten X neben das Feld gesetzt.

g. Klicken Sie auf **Weiter**.

8. Wählen Sie eine Aktion für den Messaging Security Agent, die ausgeführt werden soll, wenn eine Regel ausgelöst wird (Beschreibungen finden Sie unter *Suchziele und Aktionen für Messaging Security Agents auf Seite 7-18*):

- Durch Text/Datei ersetzen

Hinweis

Text in den Feldern "Von", "An", "CC" oder "Betreff" kann nicht ersetzt werden.

- Gesamte Nachricht in Quarantäne
- Nachrichtenteil in Quarantäne
- Gesamte Nachricht löschen
- Archivieren
- Gesamte Nachricht übergehen

9. Wählen Sie **Empfänger benachrichtigen**, damit der Messaging Security Agent die beabsichtigen Empfänger benachrichtigt, wenn die Funktion Prävention vor Datenverlust Aktionen gegen eine spezifische E-Mail ausführt.

   Aus verschiedenen Gründen ist es nicht ratsam, externe E-Mail-Empfänger zu benachrichtigen, dass eine Nachricht gesperrt wurde, die vertrauliche Informationen enthielt. Wählen Sie die Option **Externe Empfänger nicht benachrichtigen**, damit nur interne Nachrichten-Empfänger benachrichtigt werden. Legen Sie interne Adressen unter **Aktionen** > **Einstellungen für die Benachrichtigung** > **Interne Nachrichtendefinition** fest.

10. Wählen Sie **Absender benachrichtigen** aus, damit der Messaging Security Agent die gewünschten Absender benachrichtigt, wenn Prävention vor Datenverlust Maßnahmen gegen eine bestimmte E-Mail-Nachricht ergreift.

    Aus verschiedenen Gründen ist es nicht ratsam, externe E-Mail-Absender zu benachrichtigen, dass eine Nachricht gesperrt wurde, die vertrauliche Informationen enthielt. Wählen Sie die Option **Externe Absender nicht benachrichtigen**, damit nur interne Nachrichten-Absender benachrichtigt werden. Legen Sie interne Adressen unter **Aktionen** > **Einstellungen für die Benachrichtigung** > **Interne Nachrichtendefinition** fest.

11. Klicken Sie im Abschnitt **Erweiterte Optionen** auf das Plussymbol (+), um den Unterabschnitt **Archivierungseinstellungen** zu öffnen.

    a. Geben Sie in das Feld **Quarantäne-Ordner** den Pfad zum Ordner für die Funktion Prävention vor Datenverlust ein, in den die E-Mail in Quarantäne verschoben wird, oder akzeptieren Sie den Standardwert: `<Messaging Security Agent-Installationsordner>\storage\quarantine`

    b. Geben Sie in das Feld **Archivverzeichnis** den Pfad zum Ordner für die Funktion Prävention vor Datenverlust ein, in den die E-Mail in Quarantäne verschoben wird, oder akzeptieren Sie den Standardwert: `<Messaging Security Agent-Installationsordner>\storage\Sicherung für Content-Filter`

12. Klicken Sie auf das Plussymbol (+), um den Unterabschnitt **Einstellungen für das Ersetzen** zu erweitern.

    a. Geben Sie in das Feld **Name der Ersetzungsdatei** den Namen der Datei ein, mit der die Funktion Prävention vor Datenverlust eine E-Mail ersetzt, wenn eine Regel mit der Aktion 'Durch Text/Datei ersetzen' ausgelöst wurde, oder akzeptieren Sie den Standardwert:

    b. Geben oder fügen Sie in das Feld **Neuer Text** den Inhalt des Ersetzungstextes ein, den die Funktion Prävention vor Datenverlust verwenden soll, wenn eine E-Mail eine Regel mit der Aktion 'Durch Text/Datei ersetzen' auslöst, oder akzeptieren Sie den Standardtext:

13. Klicken Sie auf **Fertig stellen**.

    Der Assistent wird beendet, und Sie kehren zum Fenster Prävention vor Datenverlust zurück.

Sperren von Anhängen

Das Sperren von Anhängen verhindert, dass E-Mail-Anhänge an den Microsoft Exchange Informationsspeicher gesendet werden. Sie können den

Messaging Security Agent so konfigurieren, dass er Anhänge nach Typ und Namen sperrt und anschließend alle Nachrichten, die Ihrer Konfiguration entsprechen, ersetzt, in Quarantäne verschiebt oder löscht.

Das Sperren kann während der manuellen, der zeitgesteuerten oder der Echtzeitsuche erfolgen. Die Aktionen Löschen und Quarantäne stehen für die manuelle und zeitgesteuerte Suche jedoch nicht zur Verfügung.

Die Erweiterung eines Anhangs kennzeichnet den Dateityp, z. B. `.txt`, `.exe` oder `.dll`. Der Messaging Security Agent überprüft jedoch nicht den Dateinamen, sondern den Datei-Header, um den tatsächlichen Dateityp zu ermitteln. Viren und Malware sind häufig eng mit bestimmten Dateitypen verknüpft. Sie können das von diesen Dateitypen ausgehende Sicherheitsrisiko für Ihre Microsoft Exchange Server verringern, wenn Sie den Messaging Security Agent so konfigurieren, dass Anhänge entsprechend dem Dateityp gesperrt werden. In gleicher Weise sind bestimmte Angriffe oft mit einem bestimmten Dateinamen verknüpft.

Tipp

Virenausbrüche lassen sich über die Sperrfunktion wirksam kontrollieren. Sie können Dateitypen mit einem hohen Risiko oder bestimmte Dateinamen, die einem bekannten Virus oder einer bekannten Malware zugeordnet sind, vorübergehend in Quarantäne verschieben. Später können Sie den Quarantäne-Ordner in Ruhe überprüfen und geeignete Aktionen für infizierte Dateien durchführen.

Das Sperren von Anhängen konfigurieren

Um Optionen zum Sperren von Anhängen für Microsoft Exchange Server zu konfigurieren, werden Regeln zum Sperren von Nachrichten mit bestimmten Anhängen festgelegt.

- Für die Echtzeitsuche:

  Geräte > **{Messaging Security Agent}** > **Richtlinie konfigurieren** > **Sperren von Anhängen**

- Für die manuelle Suche:

Suchen > **Manuell** > **{Messaging Security Agent erweitern}** > **Sperren von Anhängen**

- Für die zeitgesteuerte Suche:

  Suchen > **Zeitgesteuert** > **{Messaging Security Agent erweitern}** > **Sperren von Anhängen**

Prozedur

1. Aktualisieren Sie auf der Registerkarte **Ziel** folgende Optionen bei Bedarf:

   - **Alle Dateianhänge**: Der Agent kann alle E-Mails sperren, die Anhänge enthalten. Dieses Vorgehen ist jedoch sehr aufwändig. Sie können diese Suchmethode verfeinern, indem Sie die Anhangstypen oder -namen auswählen, die nicht gesperrt werden sollen.

     - **Dateitypen von Anhängen, die von der Suche ausgeschlossen werden**

     - **Dateinamen von Anhängen, die von der Suche ausgeschlossen werden**

   - **Bestimmte Anhänge**: Wenn Sie diese Suchart wählen, sucht der Agent nur nach E-Mails, die von Ihnen festgelegte Anhänge enthalten. Diese Suchmethode ist exklusiv und eignet sich in besonderem Maße für die Erkennung von E-Mails mit Anhängen, die Sie für verdächtig halten. Die Suche ist sehr schnell, wenn Sie lediglich eine geringe Anzahl von Anhangsnamen oder -typen festlegen.

     - **Dateitypen von Anhängen**: Der Agent überprüft nicht den Dateinamen, sondern den Datei-Header, um den tatsächlichen Dateityp zu identifizieren.

     - **Dateinamen von Anhängen**: Zur Identifizierung des tatsächlichen Dateityps überprüft der Agent standardmäßig nicht den Dateinamen, sondern den Datei-Header. Wenn Sie das Sperren von Anhängen für die Suche nach ausgewählten

Namen konfigurieren, erkennt der Agent Anhänge anhand ihres Namens.

- **Dateitypen oder -namen von Anhängen in Zip-Dateien sperren**

2. Wählen Sie die Registerkarte **Aktion**, um festzulegen, welche Aktionen der Messaging Security Agent beim Fund eines Anhangs ausführen soll. Der Messaging Security Agent kann die folgenden Aktionen ausführen (Beschreibungen finden Sie unter *Suchziele und Aktionen für Messaging Security Agents auf Seite 7-18*):

   - Durch Text/Datei ersetzen
   - Gesamte Nachricht in Quarantäne
   - Nachrichtenteil in Quarantäne
   - Gesamte Nachricht löschen

3. Wählen Sie die Option **Empfänger benachrichtigen**, damit der Messaging Security Agent die beabsichtigten Empfänger von E-Mails mit Anhängen benachrichtigt.

   Wählen Sie die Option **Externe Empfänger nicht benachrichtigen**, damit nur interne Nachrichten-Empfänger benachrichtigt werden. Legen Sie interne Adressen unter **Aktionen** > **Einstellungen für die Benachrichtigung** > **Interne Nachrichtendefinition** fest.

4. Wählen Sie die Option **Absender benachrichtigen**, damit der Messaging Security Agent die Absender von E-Mails mit Anhängen benachrichtigt.

   Wählen Sie die Option **Externe Absender nicht benachrichtigen**, damit nur interne Nachrichten-Absender benachrichtigt werden. Legen Sie interne Adressen unter **Aktionen** > **Einstellungen für die Benachrichtigung** > **Interne Nachrichtendefinition** fest.

5. Klicken Sie auf das Plussymbol (+), um den Unterabschnitt **Einstellungen für das Ersetzen** zu erweitern.

   a. Geben Sie in das Feld **Name der Ersetzungsdatei** den Namen der Datei ein, mit der die Funktion Sperren von Anhängen eine E-Mail ersetzt, wenn eine Regel mit der Aktion ‘Durch Text/Datei ersetzen’ ausgelöst wurde, oder akzeptieren Sie den Standardwert.

b. Geben oder fügen Sie in das Feld **Neuer Text** den Inhalt des Ersetzungstextes ein, den die Funktion Sperren von Anhängen verwenden soll, wenn eine E-Mail eine Regel mit der Aktion 'Durch Text/Datei ersetzen' auslöst, oder akzeptieren Sie den Standardtext.

6. Klicken Sie auf **Speichern**.

Web Reputation

Web Reputation kann den Zugriff auf URLs im Web oder auf in E-Mails eigebettete URLs verhindern, die potenzielle Sicherheitsrisiken darstellen. Web Reputation überprüft die Reputation der URL anhand von Trend Micro Web Reputation-Servern und gleicht anschließend die Zuverlässigkeit einer Website mit der entsprechenden Web Reputation-Richtlinie ab, die auf dem Client angewendet wird. Je nach geltender Richtlinie:

- Der Security Agent sperrt den Zugriff auf eine Website oder lässt ihn zu.
- Der Messaging Security Agent (nur Advanced) kann E-Mail-Nachrichten mit bösartigen URLs in den Quarantäneordner schieben, löschen oder kennzeichnen oder das Senden der Nachricht zulassen, wenn die URL sicher ist

Bei Treffern in der Datenbank benachrichtigt Web Reputation den Administrator per E-Mail und den Benutzer über eine Online-Mitteilung.

Konfigurieren Sie für Security Agents unterschiedliche Sicherheitsstufen je nach Standort des Clients (Im Büro/Nicht im Büro).

Wenn Web Reputation einen Link sperrt, den Sie als sicher erachten, fügen Sie den Link zur Liste der zulässigen Links hinzu.

Tipp

Um Netzwerkbandbreite zu sparen, empfiehlt Trend Micro, die unternehmensinternen Websites in die Liste der von Web Reputation zugelassenen URLs einzutragen.

Vertrauenswürdigkeitsrate

Der 'Reputationswert' eines URLs bestimmt, ob es sich um eine Internet-Bedrohung handelt. Trend Micro berechnet diese Rate mit eigenen Bewertungssystemen.

Trend Micro stuft einen URL als Internet-Bedrohung ein, wenn die Rate innerhalb eines festgelegten Schwellenwerts liegt und als sicher, wenn dieser Wert überschritten wird.

Ein Security Agent verfügt über drei Sicherheitsstufen, durch die festgelegt wird, ob er einen URL zulässt oder sperrt.

- **Hoch**: Seiten mit folgender Bewertung blockieren:
  - **Gefährlich**: bekanntermaßen betrügerisch oder Bedrohungsquellen sind
  - **Äußerst verdächtig**: im Verdacht stehen, betrügerisch oder möglicherweise Bedrohungsquellen zu sein
  - **Verdächtig**: Mit Spam in Verbindung oder möglicherweise infiziert.
  - **Nicht geprüft**: Obwohl Trend Micro Websites aktiv auf deren Sicherheit testet, ist es möglich, dass Benutzer auf ungetestete Websites treffen, wenn diese neu sind oder seltener besucht werden. Das Sperren ungetesteter Sites kann die Sicherheit erhöhen, doch es kann auch dazu führen, dass der Zugriff auf sichere Sites gesperrt wird.
- **Mittel**: Seiten mit folgender Bewertung blockieren:
  - **Gefährlich**: bekanntermaßen betrügerisch oder Bedrohungsquellen sind
  - **Äußerst verdächtig**: im Verdacht stehen, betrügerisch oder möglicherweise Bedrohungsquellen zu sein
- **Niedrig**: Seiten mit folgender Bewertung blockieren:
  - **Gefährlich**: bekanntermaßen betrügerisch oder Bedrohungsquellen sind

Web Reputation für Messaging Security Agents konfigurieren

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.
4. Klicken Sie auf **Web Reputation**.

   Ein neues Fenster wird angezeigt.
5. Aktualisieren Sie auf Anforderung folgende Einstellungen:
   - **Web Reputation aktivieren**
   - Sicherheitsstufe: **Hoch**, **Mittel** oder **Niedrig**
   - Zugelassene URL(s)
     - **Zulässige URLs**: Trennen Sie mehrere URLs mit einem Strichpunkt (;). Klicken Sie auf **Hinzufügen**.

       Hinweis

       Wird ein Link zugelassen, werden auch alle untergeordneten Domains zugelassen.

       Verwenden Sie Platzhalter mit Vorsicht, da mit ihnen möglicherweise große Gruppen von URLs zugelassen werden.
     - **Liste der zulässigen URLs**: Die in dieser Liste enthaltenen Links werden nicht gesperrt.
6. Klicken Sie auf die Registerkarte **Aktion** und wählen Sie eine Aktion aus, die der Messaging Security Agent durchführen soll, wenn eine Web Reputation Richtlinie ausgelöst wird (Beschreibungen finden Sie unter *Suchziele und Aktionen für Messaging Security Agents auf Seite 7-18*):

- Durch Text/Datei ersetzen

> **Hinweis**
>
> Text in den Feldern "Von", "An", "CC" oder "Betreff" kann nicht ersetzt werden.

- Nachricht in den Spam-Ordner des Benutzers verschieben
- Gesamte Nachricht löschen
- Markieren und senden

7. Wählen Sie **Diese Aktion für URLs durchführen, die nicht von Trend Micro bewertet wurden**, um nicht klassifizierte URLs wie verdächtige URLs zu behandeln. Die im vorherigen Schritt festgelegte Aktion wird für alle E-Mails mit nicht klassifizierten URLs durchgeführt.

8. Wählen Sie **Empfänger benachrichtigen**, damit der Messaging Security Agent die beabsichtigen Empfänger benachrichtigt, wenn die Funktion Web Reputation Aktionen gegen eine spezifische E-Mail ausführt.

   Aus verschiedenen Gründen ist es nicht ratsam, externe E-Mail-Empfänger zu benachrichtigen, dass eine Nachricht gesperrt wurde, die bösartige URLs enthielt. Wählen Sie die Option **Externe Empfänger nicht benachrichtigen**, damit nur interne Nachrichten-Empfänger benachrichtigt werden. Legen Sie interne Adressen unter **Aktionen** > **Einstellungen für die Benachrichtigung** > **Interne Nachrichtendefinition** fest.

9. Wählen Sie **Absender benachrichtigen** aus, damit der Messaging Security Agent die gewünschten Absender benachrichtigt, wenn Web Reputation Maßnahmen gegen eine bestimmte E-Mail-Nachricht ergreift.

   Aus verschiedenen Gründen ist es nicht ratsam, externe E-Mail-Absender zu benachrichtigen, dass eine Nachricht gesperrt wurde, die bösartige URLs enthielt. Wählen Sie die Option **Externe Absender nicht benachrichtigen**, damit nur interne Nachrichten-Absender benachrichtigt werden. Definieren Sie interne Adressen über **Aktionen**

> **Einstellungen für die Benachrichtigung** > **Interne Nachrichtendefinition**.

10. Klicken Sie auf **Speichern**.

Mobile Security

Mithilfe der Mobile Security-Einstellungen wird verhindert, dass unbefugte Geräte auf Informationen in Microsoft Exchange Server zugreifen und diese herunterladen. Administratoren legen fest, welche Geräte auf Microsoft Exchange Server zugreifen können, und zusätzlich wird angegeben, ob die Benutzer dieser Geräte ihre E-Mails, Kalendernotizen, Kontakte oder Aufgaben herunterladen oder aktualisieren können.

Die Administratoren können auch Sicherheitsrichtlinien für Geräte übernehmen. Mithilfe dieser Richtlinien werden die Kennwortlänge und die Komplexität von Kennwörtern gesteuert, sowie ob Geräte nach einer bestimmten Zeit der Inaktivität gesperrt werden sollen oder Verschlüsselung nutzen müssen, und ob Gerätedaten nach einer bestimmten Anzahl fehlgeschlagener Anmeldeversuche zurückgesetzt werden sollen.

Mobile Security-Unterstützung

Tabelle 6-5. Mobilgeräteunterstützung

Betriebssystem	IIS-Version	Datenschutzrichtlinien für Gerät		Zugriffskontrolle		
		Exchange 2007 (oder höher) (64 Bit)	Exchange 2003 (32-Bit)	Exchange 2010 (und höher) (64 Bit)	Exchange 2007 (64-Bit)	Exchange 2003 (32-Bit)
• Windows 2008 (64-bit) • SBS 2008 (64 Bit)	7 +	Ja	Inkompatibel	Ja	Nein	Inkompatibel
Windows 2003 (64-bit)	6.0	Ja	Inkompatibel	Nein	Nein	Inkompatibel
• Windows 2003 (32-bit) • SBS 2003 (32 Bit)	6.0	Inkompatibel	Nein	Inkompatibel	Inkompatibel	Nein

Tabelle 6-6. Unterstützung des Betriebssystems des mobilen Geräts

Mobilgerätebetriebssystem	Betriebssystemversion
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

Gerätezugriffssteuerung konfigurieren

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.
4. Klicken Sie auf **Mobile Security** > **Gerätezugriffssteuerung**.

   Ein neues Fenster wird angezeigt.
5. Wählen Sie **Gerätezugriffskontrolle aktivieren**.
6. Klicken Sie auf **Hinzufügen**.
7. Geben Sie einen Richtliniennamen und eine aussagekräftige Beschreibung ein.
8. Wählen Sie aus, welche Geräte für den Zugriff auf Microsoft Exchange Server zugelassen/gesperrt werden sollen, indem Sie den bzw. die Gerätebesitzer angeben:
   - **Alle**
   - **Gerätebesitzer angeben**
9. Wenn **Gerätebesitzer angeben** ausgewählt ist:
   a. Geben Sie den Namen eines Gerätebesitzers ein, und klicken Sie auf **Suchen**, um den Gerätebesitzer in der globalen Adressenliste von Microsoft Exchange Server zu finden.

   b. Wählen Sie den Gerätebesitzer aus, und klicken Sie dann auf **Hinzufügen**.
10. Wählen Sie, sofern bekannt, das Betriebssystem des Geräts in der Dropdownliste **Typ** aus.

11. Wählen Sie, sofern bekannt, die Option **Versionsnummernbereich angeben** aus, und geben Sie an, welche Versionen dieses Betriebssystems zulässig sind.
12. Geben Sie an, ob der Zugriff auf E-Mails, Kalendernotizen, Kontakte oder Aufgaben des Gerätebesitzers vom Messaging Security Agent zugelassen oder blockiert werden soll.
13. Klicken Sie auf **Speichern**.

Eine ausstehende Gerätezurücksetzung abbrechen

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.
4. Klicken Sie auf **Mobile Security** > **Gerät zurücksetzen**.

   Ein neues Fenster wird angezeigt.
5. Wählen Sie das Gerät in der Tabelle der Geräte zum Zurücksetzen aus, und klicken Sie auf **Zurücksetzen abbrechen**.
6. Klicken Sie auf **OK**.

Geräte manuell zurücksetzen

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.

3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.

4. Klicken Sie auf **Mobile Security** > **Gerät zurücksetzen**.

   Ein neues Fenster wird angezeigt.

5. Klicken Sie auf **Geräte auswählen**.

   Ein neues Fenster wird angezeigt.

6. Geben Sie den Namen eines Gerätebesitzers ein, und klicken Sie auf **Suchen**, um das Gerät dieser Person zu finden.

7. Wenn das Gerät zum Zurücksetzen verfügbar ist, wählen Sie das Gerät aus, und klicken Sie auf **Zurücksetzen**.

   Hinweis

   Es ist nicht möglich, ein Gerät auszuwählen, wenn der Gerätestatus nach einer Suche **Zurücksetzen erfolgreich** oder **Zurücksetzen ausstehend** lautet.

Sicherheitsrichtlinien konfigurieren

Worry-Free Business Security verwendet als Standardrichtlinie die Microsoft Exchange-Standardrichtlinie. Die Standardrichtlinie wird in der Liste der Sicherheitsrichtlinien angezeigt.

In Worry-Free Business Security werden Nicht-Standardrichtlinien, die über die Management-Konsole von Microsoft Exchange oder Exchange Cmdlet hinzugefügt wurden, nicht beibehalten.

Trend Micro empfiehlt Administratoren, die Sicherheitsrichtlinien über die Worry-Free Business Security-Management-Konsole oder über Microsoft Exchange zu verwalten.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.
4. Klicken Sie auf **Mobile Security** > **Sicherheitsrichtlinien**.

   Ein neues Fenster wird angezeigt.
5. Klicken Sie auf **Hinzufügen**.
6. Geben Sie einen Richtliniennamen und eine aussagekräftige Beschreibung ein.
7. Geben Sie den Namen eines Gerätebesitzers ein, und klicken Sie auf **Suchen**, um den Gerätebesitzer in der globalen Adressenliste von Microsoft Exchange Server zu finden.
8. Wählen Sie den Gerätebesitzer aus, und klicken Sie dann auf **Hinzufügen**.
9. Wählen Sie die Sicherheitskriterien aus, die auf das Gerät angewendet werden sollen:
   - **Minimale Kennwortlänge**: Richtlinien zu Kennwörtern für Mobilgeräte finden Sie unter *Kennwortkomplexitätsanforderungen auf Seite 6-63*.
   - **Mindestanzahl an erforderlichen Zeichensätzen**: Richtlinien zu Kennwörtern für Mobilgeräte finden Sie unter *Kennwortkomplexitätsanforderungen auf Seite 6-63*.
   - **Gerät nach Inaktivität sperren**
   - **Geräteverschlüsselung anfordern**: Das Mobilgerät muss die Verschlüsselung unterstützen.
   - **Gerät nach fehlgeschlagenen Anmeldeversuchen zurücksetzen**

10. Klicken Sie auf **Speichern**.

Kennwortkomplexitätsanforderungen

Die Anforderungen bezüglich der Kennwortkomplexität variieren je nach Gerätetyp und Betriebssystem.

In der folgenden Tabelle wird das Verhalten der „Komplexitätsoption“ der einzelnen aufgeführt, die bis zum Zeitpunkt der Veröffentlichung von Worry-Free Business Security 9.0 SP3 getestet wurden.

Hinweis

Die Funktionsweise der Kennwortkomplexität ist vom Gerätetyp und der Betriebssystemversion abhängig. Wenn das angegebene Kennwort den Komplexitätsanforderungen nicht entspricht, erhalten die Benutzer der meisten Geräte eine Nachricht, in der die speziellen Anforderungen für das Gerät angegeben werden.

TABELLE 6-7. Android-Geräte

KOMPLEXITÄTSSTUFE	KOMPLEXITÄTSANFORDERUNGEN	
	ANDROID 4	ANDROID 2
Möglichkeit 1	Eine Kombination aus den folgenden Zeichentypen: • Mindestens einen Großbuchstaben (A-Z) oder Kleinbuchstaben (a-z) • Mindestens eine Ziffer (0-9) oder ein Sonderzeichen (!@#$ %^&*()_-=+~` []{}|;:'"?/<>,.)	Alphanumerisch

Komplexitätsstufe	Komplexitätsanforderungen	
	Android 4	Android 2
Möglichkeit 2	Eine Kombination aus den folgenden Zeichentypen: • Mindestens einen Großbuchstaben (A-Z) oder Kleinbuchstaben (a-z) • Mindestens zwei Ziffer (0-9) oder ein Sonderzeichen (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Eine Kombination aus den folgenden Zeichentypen: • Alphanumerisch • Mindestens zwei Ziffer (0-9) oder ein Sonderzeichen (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Möglichkeit 3	Eine Kombination aus den folgenden Zeichentypen: • Mindestens einen Großbuchstaben (A-Z) oder Kleinbuchstaben (a-z) • Mindestens drei Ziffer (0-9) oder ein Sonderzeichen (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Eine Kombination aus den folgenden Zeichentypen: • Alphanumerisch • Mindestens drei Ziffer (0-9) oder ein Sonderzeichen (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Möglichkeit 4	Eine Kombination aus den folgenden Zeichentypen: • Mindestens einen Großbuchstaben (A-Z) oder Kleinbuchstaben (a-z) • Mindestens vier Ziffer (0-9) oder ein Sonderzeichen (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Eine Kombination aus den folgenden Zeichentypen: • Alphanumerisch • Mindestens vier Ziffer (0-9) oder ein Sonderzeichen (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Tabelle 6-8. iOS-Geräte

Komplexitätsstufe	Komplexitätsanforderungen
Möglichkeit 1	Eine Kombination aus den folgenden Zeichentypen: • Alphanumerisch • Mindestens ein Sonderzeichen (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Komplexitätsstufe	Komplexitätsanforderungen
Möglichkeit 2	Eine Kombination aus den folgenden Zeichentypen: • Alphanumerisch • Mindestens zwei Sonderzeichen (!@#$ %^&*()_-=+~`[]{}\\|;:'"?/<>,.)
Möglichkeit 3	Eine Kombination aus den folgenden Zeichentypen: • Alphanumerisch • Mindestens drei Sonderzeichen (!@#$ %^&*()_-=+~`[]{}\\|;:'"?/<>,.)
Möglichkeit 4	Eine Kombination aus den folgenden Zeichentypen: • Alphanumerisch • Mindestens vier Sonderzeichen (!@#$ %^&*()_-=+~`[]{}\\|;:'"?/<>,.)

Tabelle 6-9. Windows Phone-Geräte

Komplexitätsstufe	Komplexitätsanforderungen	
	Windows Phone 8	Windows Phone 7
Möglichkeit 1	Mindestens einen der folgenden Zeichentypen: • Großbuchstaben (A-Z) • Kleinbuchstaben (a-z) • Numerische Zeichen (0-9) • Sonderzeichen (!@#$%^&*()_-=+~`[]{}\\|;:'"?/<>,.)	Eine Kombination aus mindestens zwei der folgenden Zeichentypen: • Großbuchstaben (A-Z) • Kleinbuchstaben (a-z) • Numerische Zeichen (0-9) • Sonderzeichen (!@#$%^&*()_-=+~`[]{}\\|;:'"?/<>,.)

Komplexitätsstufe	Komplexitätsanforderungen	
	Windows Phone 8	Windows Phone 7
Möglichkeit 2	Eine Kombination aus mindestens zwei der folgenden Zeichentypen: • Großbuchstaben (A-Z) • Kleinbuchstaben (a-z) • Numerische Zeichen (0-9) • Sonderzeichen (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	Eine Kombination aus mindestens zwei der folgenden Zeichentypen: • Großbuchstaben (A-Z) • Kleinbuchstaben (a-z) • Numerische Zeichen (0-9) • Sonderzeichen (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Möglichkeit 3	Eine Kombination aus mindestens drei der folgenden Zeichentypen: • Großbuchstaben (A-Z) • Kleinbuchstaben (a-z) • Numerische Zeichen (0-9) • Sonderzeichen (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	Eine Kombination aus mindestens drei der folgenden Zeichentypen: • Großbuchstaben (A-Z) • Kleinbuchstaben (a-z) • Numerische Zeichen (0-9) • Sonderzeichen (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Möglichkeit 4	Eine Kombination aus allen folgenden Zeichentypen: • Großbuchstaben (A-Z) • Kleinbuchstaben (a-z) • Numerische Zeichen (0-9) • Sonderzeichen (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	Eine Kombination aus allen folgenden Zeichentypen: • Großbuchstaben (A-Z) • Kleinbuchstaben (a-z) • Numerische Zeichen (0-9) • Sonderzeichen (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

Tabelle 6-10. BlackBerry-Geräte

Komplexitätsstufe	Komplexitätsanforderungen
Möglichkeit 1	Mindestens einen Großbuchstaben (A-Z) oder Kleinbuchstaben (a-z)

Komplexitätsstufe	Komplexitätsanforderungen
Möglichkeit 2	Eine Kombination aus mindestens zwei der folgenden Zeichentypen: • Großbuchstaben (A-Z) • Kleinbuchstaben (a-z) • Numerische Zeichen (0-9) • Sonderzeichen (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Möglichkeit 3	Eine Kombination aus mindestens drei der folgenden Zeichentypen: • Großbuchstaben (A-Z) • Kleinbuchstaben (a-z) • Numerische Zeichen (0-9) • Sonderzeichen (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Möglichkeit 4	Eine Kombination aus allen folgenden Zeichentypen: • Großbuchstaben (A-Z) • Kleinbuchstaben (a-z) • Numerische Zeichen (0-9) • Sonderzeichen (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

Quarantäne für Messaging Security Agents

Entdeckt der Messaging Security Agent eine Bedrohung, Spam, unzulässige Anhänge und/oder unzulässige Inhalte in E-Mails, kann er die Nachricht in einen Quarantäne-Ordner verschieben. Dieser Vorgang kann als Alternative zum Löschen von Nachrichten/Anhängen dienen und verhindert, dass Benutzer infizierte Nachrichten öffnen und dadurch die Bedrohung verbreiten.

Standardmäßig befindet sich der Quarantäne-Ordner auf dem Messaging Security Agent unter

```
<Messaging Security Agent Installationsordner>\storage
\quarantine
```

Als zusätzliche Sicherheitsmaßnahme werden Dateien in Quarantäne verschlüsselt. Öffnen Sie verschlüsselte Dateien mit dem Tool 'Restore Encrypted Virus and Spyware' (`VSEncode.exe`). Weitere Informationen finden Sie unter *Verschlüsselte Dateien wiederherstellen auf Seite 14-18*.

In der Quarantäne-Datenbank finden Administratoren Informationen über die Nachrichten in Quarantäne

Mit der Quarantäne-Funktion können Sie:

- Die Wahrscheinlichkeit verringern, dass wichtige Nachrichten dauerhaft gelöscht werden, wenn diese irrtümlich von sehr strengen Filtern entdeckt wurden.
- Nachrichten überprüfen, die Content-Filter auslösen, und so den Schweregrad einer Richtlinienverletzung bestimmen.
- Nachweise über den Missbrauch des unternehmensinternen Messaging-Systems durch einen Mitarbeiter aufbewahren.

Hinweis

Verwechseln Sie den Quarantäne-Ordner nicht mit dem Spam-Ordner des Endbenutzers. Es handelt sich dabei um einen dateibasierten Ordner. Zum Verschieben einer E-Mail in Quarantäne sendet der Messaging Security Agent die Nachricht an den Quarantäne-Ordner. Der Endbenutzer-Spam-Ordner befindet sich für das Postfach jedes Benutzers im Informationsspeicher. In den Spam-Ordner des Endbenutzers gelangen nur E-Mails, die vom Anti-Spam-Quarantäne-Ordner an den Spam-Ordner eines Endbenutzers gesendet werden. Nachrichten, die aufgrund von Content-Filtern, Virenschutz, Anti-Spyware oder Richtlinien zum Sperren von Anhängen in Quarantäne verschoben werden, gelangen nicht in den Endbenutzer-Spam-Ordner.

Quarantäne-Verzeichnisse abfragen

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.
4. Klicken Sie auf **Quarantäne** > **Abfrage**.

   Ein neues Fenster wird angezeigt.
5. Aktualisieren Sie auf Anforderung folgende Einstellungen:
   - Datum und Uhrzeit
   - Gründe für das Verschieben in Quarantäne
     - **Alle Gründe**
     - **Bestimmte Typen**: Wählen Sie aus den Optionen Virensuche, Anti-Spam, Content-Filter, Sperren von Anhängen und/oder Nicht durchsuchbare Nachrichtenteile.
   - Erneut versenden – Status
     - **Nie erneut versendet**
     - **Mindestens einmal erneut versendet**
     - **Beides**
   - Erweiterte Kriterien
     - **Absender**: Nachrichten von festgelegten Absendern. Verwenden Sie bei Bedarf Platzhalter.
     - **Empfänger**: Nachrichten von festgelegten Empfängern. Verwenden Sie bei Bedarf Platzhalter.

- **Betreff**: Nachrichten mit einem bestimmten Betreff. Verwenden Sie bei Bedarf Platzhalter.
- **Sortieren nach**: Legen Sie die Sortierbedingung für die Ergebnisseite fest.
- **Anzeige**: Anzahl der Ergebnisse pro Seite.

6. Klicken Sie auf **Search**. Weitere Informationen finden Sie unter *Abfrageergebnisse anzeigen und Aktionen ausführen auf Seite 6-70*.

Abfrageergebnisse anzeigen und Aktionen ausführen

Im Fenster **Quarantäne-Abfrage – Ergebnisse** werden folgende Informationen über die Nachrichten angezeigt:

- **Zeitpunkt der Suche**
- **Absender**
- **Empfänger**
- **Betreff**
- **Grund**: Der Grund, weshalb die E-Mail in Quarantäne verschoben wurde.
- **Dateiname**: Name der gesperrten Datei in der E-Mail.
- **Quarantänepfad**: Der Speicherort der E-Mail. Administratoren können die Datei mit Hilfe des Programms VSEncoder.exe (siehe *Verschlüsselte Dateien wiederherstellen auf Seite 14-18*) entschlüsseln und zum Anzeigen die Dateierweiterung anschließend in `.eml` umbenennen.

  Warnung!

  Durch das Anzeigen infizierter Dateien kann sich die Bedrohung verbreiten.

- **Erneut versenden – Status**

Prozedur

1. Wenn Sie das Gefühl haben, dass eine Nachricht nicht sicher ist, löschen Sie diese.

   Warnung!

   Der Quarantäne-Ordner enthält E-Mail-Nachrichten, die ein hohes Infektionsrisiko darstellen. Behandeln Sie die E-Mail-Nachrichten im Quarantäne-Ordner mit äußerster Vorsicht, um eine versehentliche Infektion des Clients zu vermeiden.

2. Wenn Sie glauben, dass die Nachricht sicher ist, wählen Sie die Nachricht aus, und klicken Sie auf das Symbol 'Erneut versenden' ( ).

   Hinweis

   Wenn Sie eine Quarantäne-Nachricht, die ursprünglich über Microsoft Outlook versendet wurde, erneut versenden, erhält der Empfänger möglicherweise mehrere Kopien derselben Nachricht, da die Scan Engine beim Durchsuchen jede Nachricht in mehrere Abschnitte unterteilt.

3. Wenn Sie die Nachricht nicht erneut versenden können, ist das Konto des Systemadministrators auf dem Microsoft Exchange Server möglicherweise nicht vorhanden.

   a. Öffnen Sie mit dem Windows Registrierungseditor den folgenden Registrierungseintrag auf dem Server:

      ```
      HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for
      Exchange\CurrentVersion
      ```

   b. Bearbeiten Sie den Eintrag wie folgt:

      Warnung!

      Nicht ordnungsgemäß bearbeitete Systemeinträge können erhebliche Schäden auf Ihrem Computer verursachen. Bevor Sie die Änderungen vornehmen, sollten Sie deshalb alle wichtigen Daten sichern.

- `ResendMailbox` `{Administrator-Postfach}`

  Beispiel: `admin@example.com`

- `ResendMailboxDomain` `{Administratordomäne}`

  Beispiel: `beispiel.com`

- `ResendMailSender` `{E-Mail-Konto des Administrators}`

  Beispiel: `admin`

c. Schließen Sie den Registrierungseditor.

Quarantäne-Verzeichnisse warten

Mit dieser Funktion können Sie Nachrichten in Quarantäne manuell oder automatisch löschen. Dabei werden alle Nachrichten, erneut versendete Nachrichten oder Nachrichten, die nicht erneut versendet wurden, gelöscht.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.
4. Klicken Sie auf **Quarantäne** > **Wartung**.

   Ein neues Fenster wird angezeigt.
5. Aktualisieren Sie auf Anforderung folgende Einstellungen:
   - **Automatische Wartung aktivieren**: Nur für automatische Wartung verfügbar.
   - Diese Dateien löschen

- **Alle Dateien in Quarantäne**
- **Quarantäne-Dateien, die nie erneut versendet wurden**
- **Quarantäne-Dateien, die mindestens einmal erneut versendet wurden**

- **Aktion**: Die Anzahl der Tage, für die die Nachrichten gespeichert werden sollen. Wenn z. B. das aktuelle Datum 21. November lautet und Sie im Feld **Ausgewählte Dateien löschen, die älter sind als** den Wert `10` eingegeben haben, löscht der Messaging Security Agent beim automatischen Löschvorgang alle Dateien mit Datum vor dem 11. November.

6. Klicken Sie auf **Speichern**.

Quarantäne-Ordner konfigurieren

Konfigurieren Sie die Quarantäne-Ordner auf dem Exchange Server. Der Quarantäne-Ordner wird von der Suche ausgeschlossen.

Hinweis

Quarantäne-Ordner sind dateibasiert und befinden sich nicht im Informationsspeicher.

Der Messaging Security Agent verschiebt E-Mails gemäß den von Ihnen festgelegten Aktionen. Folgende Quarantäne-Ordner stehen zur Verfügung:

- **Virenschutz**: Verschiebt E-Mails, die Viren/Malware, Spyware/Grayware, Würmer, Trojaner und andere bösartige Bedrohungen enthalten, in Quarantäne.
- **Anti-Spam**: Verschiebt Spam- und Phishing-Mails in Quarantäne.
- **Sperren von Anhängen**: Verschiebt E-Mail-Nachrichten mit unzulässigen Anhängen in den Quarantäne-Ordner.
- **Content-Filter**: Verschiebt E-Mail-Nachrichten mit unzulässigen Inhalten in den Quarantäne-Ordner.

Standardmäßig haben alle Ordner dieselben Pfade (`<Messaging Security Agent-Installationsordner>\storage\quarantine`). Sie können die Pfade für einzelne oder alle Ordner ändern.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.
4. Klicken Sie auf **Quarantäne** > **Verzeichnis**.

   Ein neues Fenster wird angezeigt.
5. Legen Sie den Pfad für die folgenden Quarantäne-Ordner fest:
   - **Virenschutz**
   - **Anti-Spam**
   - **Content-Filter**
   - **Sperren von Anhängen**
6. Klicken Sie auf **Speichern**.

Einstellungen für die Benachrichtigung für Messaging Security Agents

Worry-Free Business Security kann Benachrichtigungen über diverse Alarme in Form von E-Mails versenden.

Sie können Benachrichtigungen so konfigurieren, dass diese nur für interne E-Mail-Nachrichten gelten, indem Sie benutzerdefinierbare, interne Nachrichtendefinitionen verwenden. Diese eignen sich besonders, wenn Ihr

Unternehmen über mehr als eine Domain verfügt und Sie die E-Mails von diesen Domains als interne E-Mails behandeln möchten. (z. B. beispiel.com und beispiel.net).

Die Empfänger auf Ihrer Liste für interne Nachrichtendefinitionen werden per E-Mail benachrichtigt, wenn Sie das Kontrollkästchen **Externe Empfänger nicht benachrichtigen** unter "Einstellungen für die Benachrichtigung" für **Virenschutz**, **Content-Filter** und **Sperren von Anhängen** aktiviert haben. Verwechseln Sie die Liste für interne Nachrichtendefinitionen nicht mit der Liste der zulässigen Absender.

Um zu vermeiden, dass alle E-Mail-Nachrichten von Adressen mit externen Domänen als Spam gekennzeichnet werden, fügen Sie die externen E-Mail-Adressen zu den Listen der **zulässigen Absender** für Anti-Spam hinzu.

Info über benutzerdefinierbare, interne Nachrichtendefinitionen

Messaging Security Agent teilt den E-Mail-Datenverkehr in zwei Kategorien ein: intern und extern. Der Agent bezieht vom Microsoft Exchange Server die Definition interner und externer Adressen. Alle internen Adressen haben eine gemeinsame Domain, während alle externen Adressen nicht zu dieser Domäne gehören.

Wenn beispielsweise die interne Domänenadresse “@trend_1.de” ist, ordnet Messaging Security Agent Adressen wie z. B. “abc@trend_1.de” und “xyz@trend_1.de” als interne Adressen ein. Der Agent behandelt alle anderen Adressen wie z. B. “abc@trend_2.de” und “maxmustermann@123.de” als extern.

Sie können nur eine Domain als interne Adresse für den Messaging Security Agent festlegen. Wenn Sie mit dem Microsoft Exchange System Manager Ihre Primäradresse auf einem Server ändern, ist diese neue Adresse für den Messaging Security Agent keine interne Adresse mehr, da er nicht erkennen kann, dass die Empfängerrichtlinie verändert wurde.

Sie verwenden beispielsweise zwei Domänenadressen für Ihr Unternehmen: @beispiel_1.de und @beispiel2.de. Legen Sie @beispiel_1.de als Primäradresse fest. Der Messaging Security Agent stuft Nachrichten mit der Primäradresse als interne Nachrichten ein (so werden beispielsweise abc@beispiel_1.de oder xyz@beispiel_1.de als interne Adressen erkannt).

Später ändern Sie die Primäradresse mit Hilfe des Microsoft Exchange System Managers in @beispiel_2.de. Der Microsoft Exchange Server erkennt nun Adressen wie abc@beispiel_2.de und xyz@beispiel_2.de als interne Adressen.

Einstellungen für die Benachrichtigung für Messaging Security Agents konfigurieren

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.
4. Klicken Sie auf **Aktionen** > **Einstellungen für die Benachrichtigung**.

   Ein neues Fenster wird angezeigt.
5. Aktualisieren Sie auf Anforderung folgende Einstellungen:
   - **E-Mail-Adresse**: Die Adresse, die Worry-Free Business Security zum Senden von Benachrichtigungen verwendet.
   - **Definition von internen Nachrichten**
     - **Standard**: Worry-Free Business Security behandelt E-Mail-Nachrichten von derselben Domäne als interne E-Mails.
     - **Benutzerdefiniert**: Geben Sie individuelle E-Mail-Adressen oder Domains an, um sie als interne E-Mail-Nachrichten zu behandeln.
6. Klicken Sie auf **Speichern**.

Spam-Wartung konfigurieren

Im Fenster **Spam-Wartung** können Sie Einstellungen für die End User Quarantine (EUQ) oder für die Quarantäne auf dem Server konfigurieren.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.
4. Klicken Sie auf **Aktionen** > **Spam-Wartung**.

   Ein neues Fenster wird angezeigt.
5. Klicken Sie auf **End User Quarantine Tool aktivieren**.

   Wenn Sie das Tool aktivieren, wird für jede Client-Mailbox ein Quarantäne-Ordner auf dem Server erstellt. In der Ordnerstruktur von Outlook wird ein Ordner `Spam-Mail` angezeigt. Nach der Aktivierung und dem Erstellen der Spam-Ordner filtert die EUQ Spam-Mails aus und legt sie im Spam-Mail-Ordner des Benutzers ab. Weitere Informationen finden Sie unter *Das Tool End User Quarantine verwalten auf Seite 6-78*.

   Tipp

   Bei Auswahl dieser Option sollten Sie die Optionen der Trend Micro Anti-Spam Symbolleiste auf den Agents deaktivieren, um die Leistung auf den Clients zu optimieren.

   Deaktivieren Sie das Tool **End User Quarantine aktivieren**, um die End User Quarantine für alle Postfächer auf dem Microsoft Exchange Server zu deaktivieren. Wenn Sie die EUQ deaktivieren, bleiben die Spam-Mail-Ordner der Benutzer bestehen, aber als Spam gekennzeichnete Nachrichten werden nicht in die Spam-Mail-Ordner verschoben.

6. Klicken Sie auf **Spam-Ordner erstellen und Spam-Nachrichten löschen**, um (sofort) die entsprechenden Spam-Mail-Ordner für neu angelegte oder für bereits vorhandene Mail-Clients, die ihre Spam-Mail-Ordner gelöscht haben, zu erstellen. Für bereits vorhandene Mail-Clients mit Spam-Mail-Ordner löscht das Tool diejenigen Spam-Nachrichten, die älter sind als die Angaben unter Einstellungen für den Client-Spam-Ordner.
7. Ändern Sie unter **Alle Spam-Nachrichten löschen, die älter sind als {Zahl} Tage** die Anzahl der Tage, die der Messaging Security Agent Spam-Mails aufbewahren soll. Der voreingestellte Wert ist 14 Tage, die Höchstdauer 30 Tage.
8. So deaktivieren Sie das End User Quarantine Tool für ausgewählte Benutzer:
   a. Geben Sie unter **Ausnahmeliste des End User Quarantine Tools** die E-Mail-Adresse des Endbenutzers ein, für den Sie die EUQ deaktivieren möchten.
   b. Klicken Sie auf **Hinzufügen**.

      Die E-Mail-Adresse des Endbenutzers wird zur Liste der Adressen hinzugefügt, für die die EUQ deaktiviert ist.

      Um einen Endbenutzer aus der Liste zu entfernen und den EUQ Dienst wiederherzustellen, wählen Sie die E-Mail-Adresse des Endbenutzers aus der Liste aus, und klicken Sie auf **Löschen**.
9. Klicken Sie auf **Speichern**.

Das Tool End User Quarantine verwalten

Während der Installation richtet der Messaging Security Agent im Server-Postfach für jeden Endbenutzer einen `Spam-Mail`-Ordner ein. Gehen Spam-Nachrichten ein, werden diese vom System gemäß der vom Messaging Security Agent vordefinierten Spam-Filterregeln in diesen Quarantäne-Ordner verschoben. Der Endbenutzer kann verdächtige E-Mails in diesem Spam-Ordner öffnen, lesen oder löschen. Weitere Informationen finden Sie unter *Spam-Wartung konfigurieren auf Seite 6-77*.

Administratoren können den Spam-Mail-Ordner auch auf dem Microsoft Exchange Server einrichten. Wenn der Administrator ein Postfachkonto einrichtet, wird das Postfach nicht direkt im Microsoft Exchange Server erstellt, sondern erst unter folgenden Bedingungen:

- Ein Endbenutzer meldet sich zum ersten Mal an seinem Postfach an.
- Die erste E-Mail geht im Postfach ein.

Der Administrator muss zunächst das Postfach einrichten, bevor die EUQ den Spam-Ordner erstellen kann.

Der Ordner Spam-Mail auf dem Client

Endbenutzer können E-Mails öffnen, die in den Spam-Ordner verschoben wurden. Beim Öffnen einer dieser Nachrichten werden in der eigentlichen E-Mail zwei Schaltflächen angezeigt: **Zulässiger Absender** und **Liste der zulässigen Absender anzeigen**.

- Öffnet ein Endbenutzer eine E-Mail im Spam-Mail-Ordner und klickt auf **Zulässiger Absender**, wird die Adresse des Absenders dieser E-Mail zur Liste der **zulässigen Absender** dieses Endbenutzers hinzugefügt.
- Mit einem Klick auf **Liste der zulässigen Absender anzeigen** wird ein weiteres Fenster geöffnet, in dem der Endbenutzer seine Liste der zulässigen Absender nach E-Mail-Adresse oder Domäne anzeigen und ändern kann.

Zulässige Absender

Klickt der Endbenutzer nach Eingang einer E-Mail, die in den Ordner Spam-Mail verschoben wurde, auf **Absender zulassen**, verschiebt der Messaging Security Agent die Nachricht in den lokalen Posteingang des Endbenutzers und fügt die Adresse des Absenders zur persönlichen Liste der zulässigen Absender dieses Endbenutzers hinzu. Dieses Ereignis wird vom Messaging Security Agent protokolliert.

Gehen auf dem Microsoft Exchange Server Nachrichten von Adressen ein, die in der Liste der zulässigen Absender des Endbenutzers enthalten sind, werden diese unabhängig vom Header oder vom Inhalt der Nachricht in den Posteingang des Endbenutzers verschoben.

Hinweis

Der Messaging Security Agent stellt auch für Administratoren eine Liste zulässiger oder gesperrter Absender bereit. Dabei bearbeitet er zuerst die Administratorliste der zulässigen oder gesperrten Absender und anschließend die Liste des Endbenutzers.

Die Verwaltungsfunktion der End User Quarantine

Die Messaging Security Agent Verwaltungsfunktion führt alle 24 Stunden standardmäßig um 2:30 Uhr die folgenden Tasks aus:

- Automatisches Löschen abgelaufener Spam-Nachrichten
- Neuerstellung des gelöschten Spam-Ordners
- Erstellung von Spam-Ordnern für neu eingerichtete E-Mail-Konten
- Wartung der E-Mail-Regeln

Die Verwaltungsfunktion ist Teil des Messaging Security Agents und muss nicht konfiguriert werden.

Trend Micro Support und Fehlerbehebung

Der Support und die Fehlerbehebung können Ihnen beim Debuggen oder beim Melden des Status der Messaging Security Agent Prozesse behilflich sein. Im Falle unerwarteter Probleme können Sie Debugger-Berichte erstellen und diese zur Analyse an den technischen Support von Trend Micro senden.

Jeder Messaging Security Agent fügt Meldungen in das Programm ein und zeichnet die Aktion nach der Ausführung in Protokolldateien auf. Sie können diese Protokolle an die Mitarbeiter des technischen Supports von Trend Micro senden, damit diese Fehler im tatsächlichen Programmablauf in Ihrer Umgebung suchen und beseitigen können.

Mit dem Debugger können Sie Protokolle in den folgenden Modulen erstellen:

- Messaging Security Agent Master-Dienst
- Messaging Security Agent Remote-Konfigurationsserver
- Messaging Security Agent Systemüberwachung
- API zur Virensuche (VSAPI)
- Simple Mail Transfer Protocol (SMTP)
- Common Gateway Interface (CGI)

Der MSA speichert die Protokolle standardmäßig im folgenden Verzeichnis:

```
<Messaging Security Agent Installationsordner>\Debug
```

Ausgabe in einem Texteditor anzeigen.

Berichte des System-Debuggers erstellen

Erstellen Sie Debugger-Berichte, um den Support von Trend Micro bei der Behebung Ihres Problems zu unterstützen.

Prozedur

1. Navigieren Sie zu **Geräte**.
2. Wählen Sie einen Messaging Security Agent.
3. Klicken Sie auf **Richtlinie konfigurieren**.

   Ein neues Fenster wird angezeigt.
4. Klicken Sie auf **Aktionen** > **Support und Fehlerbehebung**.

   Ein neues Fenster wird angezeigt.
5. Wählen Sie die zu überwachenden Module aus:
   - Messaging Security Agent **Master-Dienst**
   - Messaging Security Agent **Remote-Konfigurationsserver**

- Messaging Security Agent **Systemüberwachung**
- **API zur Virensuche (VSAPI)** für Exchange Server 2003, 2007 oder 2010
- **Suche in der Sicherungsschicht** für Exchange Server 2013
- **Simple Mail Transfer Protocol (SMTP)** für Exchange Server 2003
- **Übertragungsdienst** für Exchange Server 2007, 2010 oder 2013
- **Common Gateway Interface (CGI)**

6. Klicken Sie auf **Übernehmen**.

   Der Debugger beginnt, die Daten für die ausgewählten Module zu sammeln.

Echtzeitmonitor

Der Echtzeitmonitor zeigt aktuelle Informationen über den ausgewählten Microsoft Exchange Server und den darauf installierten Messaging Security Agent an. Er liefert eine Schutzstatistik und Informationen über durchsuchte Nachrichten sowie die Anzahl der entdeckten Viren- und Spam-Vorkommnisse, der gesperrten Anhänge und der Inhaltsverstöße. Ebenso überprüft er, ob der Agent ordnungsgemäß funktioniert.

Mit dem Echtzeitmonitor arbeiten

Prozedur

1. So rufen Sie über die Webkonsole den Echtzeitmonitor auf:
   a. Navigieren Sie zu **Geräte**.
   b. Wählen Sie einen Messaging Security Agent.
   c. Klicken Sie auf **Richtlinie konfigurieren**.

Ein neues Fenster wird angezeigt.

d. Klicken Sie oben rechts im Fenster auf den Link **Echtzeitmonitor**.

2. Klicken Sie auf **Alle Programme** > **Trend Micro Messaging Security Agent** > **Echtzeitmonitor**, um den Echtzeitmonitor über das Windows Start-Menü aufzurufen.

3. Klicken Sie auf **Zurücksetzen**, um die Schutzstatistik auf Null zurückzusetzen.

4. Klicken Sie auf **Inhalt löschen**, um veraltete Informationen über durchsuchte Nachrichten zu löschen.

Einen Disclaimer zu ausgehenden E-Mail-Nachrichten hinzufügen

Sie können einen Disclaimer nur zu ausgehenden E-Mail-Nachrichten hinzufügen.

Prozedur

1. Erstellen Sie eine Textdatei, und fügen Sie den Disclaimer-Text zu dieser Datei hinzu.

2. Bearbeiten Sie die folgenden Schlüssel in der Registrierung:

   - Erster Schlüssel:

     Pfad: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

     Schlüssel: `EnableDisclaimer`

     Typ: `REG_DWORD`

     Datenwert: `0 - Deaktivieren, 1 - Aktivieren`

- Zweiter Schlüssel:

  Pfad: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

  Schlüssel: `DisclaimerSource`

  Typ: `REG_SZ`

  Wert: Der vollständige Pfad der Disclaimer-Inhaltsdatei.

  Zum Beispiel `C:\Data\Disclaimer.txt`.

  Hinweis

  Standardmäßig erkennt Worry-Free Business Security, ob eine ausgehende E-Mail an interne oder externe Domänen gesendet wird, und fügt zu jeder E-Mail an externe Domänen einen Disclaimer hinzu. Der Benutzer kann die Standardeinstellung überschreiben, und einen Disclaimer zu jeder ausgehenden E-Mail-Nachricht mit Ausnahme von E-Mail-Nachrichten an die Domänen hinzuzufügen, die im folgenden Registrierungsschlüssel enthalten sind:

- Dritter Schlüssel:

  Pfad: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

  Schlüssel: `InternalDomains`

  Typ: `REG_SZ`

  Wert: Geben Sie die auszuschließenden Domänennamen ein. Trennen Sie mehrere Einträge durch einen Strichpunkt (;).

  Beispiel: `domain1.org;domain2.org`

  Hinweis

  Diese Domänennamen sind die DNS-Namen der Exchange Server.

Kapitel 7

Suche verwalten

In diesem Kapitel wird die Durchführung von Suchen auf den Security Agents und Messaging Security Agents (nur Advanced) beschrieben, um Ihr Netzwerk und Clients vor Bedrohungen zu schützen.

Info über Suchtypen

Während einer Suche führt die Trend Micro Scan Engine zusammen mit der Pattern-Datei die erste Erkennungsstufe durch und verwendet dafür einen als Pattern-Abgleich bezeichneten Prozess. Da jede Bedrohung eine eindeutige Signatur (eine charakteristische Zeichenfolge) enthält, die sie von anderem Code unterscheidet, sind inaktive Teile dieses Codes in der Pattern-Datei erfasst. Die Scan Engine vergleicht dann bestimmte Teile jeder durchsuchten Datei mit dem Muster in der Pattern-Datei und sucht nach Übereinstimmungen.

Entdeckt die Scan Engine eine Datei mit einem Virus oder anderer Malware, wird eine Aktion, wie Säubern, Quarantäne, Löschen oder Durch Text/Datei ersetzen durchgeführt (nur Advanced). Bei der Einrichtung der Such-Tasks können Sie diese Aktionen festlegen.

Worry-Free Business Security bietet **drei Suchtypen**. Jeder Suchtyp hat ein anderes Ziel und wird anders eingesetzt. Die Konfiguration ist aber bei allen drei Typen fast identisch.

- Echtzeitsuche. Weitere Informationen finden Sie unter *Echtzeitsuche auf Seite 7-3*.
- Manuelle Suche. Weitere Informationen finden Sie unter *Manuelle Suche auf Seite 7-3*.
- Zeitgesteuerte Suche. Weitere Informationen finden Sie unter *Zeitgesteuerte Suche auf Seite 7-7*.

Bei der Suche nach Sicherheitsrisiken wenden Security Agents eine von zwei Suchmethoden an:

- Smart Scan
- Herkömmliche Suche

Weitere Informationen finden Sie unter *Suchmethoden auf Seite 5-3*.

Echtzeitsuche

Die Echtzeitsuche wird kontinuierlich und dauerhaft ausgeführt.

Jedes Mal, wenn eine Datei geöffnet, heruntergeladen, kopiert oder geändert wird, wird sie von der Echtzeitsuche im **Security Agent** auf Bedrohungen durchsucht. Informationen zur Konfiguration der Echtzeitsuche finden Sie unter *Echtzeitsuche für Security Agents konfigurieren auf Seite 5-7*.

Bei E-Mail-Nachrichten überwacht die Echtzeitsuche im **Messaging Security Agent** (nur Advanced) alle bekannten Vireneintrittspunkte und durchsucht den gesamten eingehenden Nachrichtenverkehr, alle SMTP-Nachrichten, Dokumente in Freigabeordnern sowie von anderen Microsoft Exchange Servern replizierte Dateien in Echtzeit. Informationen zur Konfiguration der Echtzeitsuche finden Sie unter *Die Echtzeitsuche für Messaging Security Agents konfigurieren auf Seite 6-6*.

Manuelle Suche

Die manuelle Suche ist eine Suche auf Anforderung.

Mit der manuellen Suche auf **Security Agents** werden Bedrohungen aus Dateien entfernt und gegebenenfalls vorhandene alte Infektionen beseitigt, um das Risiko einer Neuinfektion zu reduzieren.

Die manuelle Suche auf **Messaging Security Agents** (nur Advanced) durchsucht alle Dateien im Informationsspeicher Ihres Microsoft Exchange Servers.

Die Dauer der Suche hängt von den Hardware-Ressourcen des Clients und der Anzahl der zu durchsuchenden Dateien ab. Der Security Server Administrator kann eine laufende manuelle Suche anhalten, falls die Suche remote über die Webkonsole ausgeführt wurde. Benutzer können die Suche anhalten, wenn sie direkt auf dem Client ausgeführt wurde.

Tipp

Trend Micro empfiehlt manuelle Suchen nach jedem Virenausbruch.

Manuelle Suche durchführen

In diesem Verfahren wird beschrieben, wie Security Server Administratoren über die Webkonsole manuelle Suchen auf **Security Agents** und **Messaging Security Agents** (nur Advanced) durchführen können.

Hinweis

Die manuelle Suche kann außerdem direkt über Clients ausgeführt werden, durch einen Rechtsklick auf das Security Agent Symbol in der Windows Task-Leiste und einen Klick auf **Jetzt durchsuchen**. Manuelle Suchen können nicht direkt auf Microsoft Exchange Servern durchgeführt werden.

Prozedur

1. Navigieren Sie zu **Suchen** > **Manuelle Suche**.
2. (Optional) Passen Sie die Sucheinstellungen an, bevor Sie eine manuelle Suche durchführen.

Anleitungen und Hinweise	Empfohlene Sucheinstellungen
Klicken Sie auf eine Desktop- oder Servergruppe, um die Sucheinstellungen für den **Security Agent** anzupassen. Weitere Informationen finden Sie unter *Suchziele und Aktionen für Security Agents auf Seite 7-10*. **Hinweis** Die Sucheinstellungen für Security Agents werden auch verwendet, wenn Benutzer manuelle Suchen direkt von Clients durchführen. Wenn Sie den Benutzern die Berechtigung zum Konfigurieren ihrer eigenen Sucheinstellungen gewähren, werden während der Suche jedoch die benutzerkonfigurierten Einstellungen verwendet.	Ziel • Alle durchsuchbaren Dateien: alle durchsuchbaren Dateien werden berücksichtigt. Zu den nicht durchsuchbaren Dateien gehören kennwortgeschützte und verschlüsselte Dateien sowie Dateien, die die vom Benutzer festgelegten Suchkriterien nicht erfüllen. • Komprimierte Dateien bis zu Ebene 1 durchsuchen: Dateien mit einer Komprimierungsebene werden durchsucht. Die Standardeinstellung ist "Aus" für die Standard-Servergruppe und "Ein" für die Standard-Desktopgruppe.
	Ausschlüsse • Verzeichnisse, in denen Trend Micro Produkte installiert sind, werden von der Suche ausgeschlossen.
	Erweiterte Einstellungen • Liste der zulässigen Spyware/Grayware (nur für Anti-Spyware) ändern

Anleitungen und Hinweise	Empfohlene Sucheinstellungen
Erweitern Sie einen Agent und klicken Sie auf folgende Elemente, um die Sucheinstellungen für den **Messaging Security Agent** anzupassen: • **Virenschutz**: Zur Suche nach Viren und anderen Arten von Malware. Weitere Informationen finden Sie unter *Suchziele und Aktionen für Messaging Security Agents auf Seite 7-18*. • **Content-Filter**: Zur Suche nach unzulässigem Inhalt in E-Mails. Weitere Informationen finden Sie unter *Content-Filter-Regeln verwalten auf Seite 6-17*. • **Sperren von Anhängen**: Zur Suche nach unzulässigen Anhängen in E-Mails. Weitere Informationen finden Sie unter *Das Sperren von Anhängen konfigurieren auf Seite 6-50*.	• Der Agent durchsucht alle durchsuchbaren Dateien. Dabei wird auch der Nachrichtentext einer E-Mail in die Suche einbezogen. • Beim Fund einer mit einem Virus oder anderer Malware infizierten Datei säubert der Agent diese Datei. Kann die Datei nicht gesäubert werden, wird sie durch Text oder eine Datei ersetzt. • Beim Fund einer mit einem Trojaner oder Wurm infizierten Datei ersetzt der Agent diesen Trojaner oder Wurm durch einen Text oder eine Datei. • Beim Fund einer mit einem Packer infizierten Datei ersetzt der Agent diesen Packer durch einen Text oder eine Datei. • Der Agent säubert keine infizierten komprimierten Dateien. Dadurch verkürzt sich die Dauer der Echtzeitsuche.

3. Wählen Sie die Gruppen oder Messaging Security Agents, die durchsucht werden sollen.

4. Klicken Sie auf **Jetzt durchsuchen**.

   Der Security Server benachrichtigt die Agents, damit sie eine manuelle Suche durchführen. Im Fenster Ergebnisse der Suchbenachrichtigung wird die Anzahl der Agents angezeigt, die die Benachrichtigung erhalten oder nicht erhalten haben.

5. Klicken Sie auf **Suche beenden**, um laufende Suchen abzubrechen.

   Der Security Server benachrichtigt die Agents erneut, damit sie die manuelle Suche beenden. Im Fenster Ergebnisse der Suchbenachrichtigung zum Beenden der Suche wird die Anzahl der Agents angezeigt, die die Benachrichtigung erhalten oder nicht erhalten

haben. Eventuell erhalten Security Agents die Benachrichtigung nicht, weil sie nach dem Start der Suche offline gesetzt wurden oder Netzwerkstörungen eingetreten sind.

Zeitgesteuerte Suche

Die zeitgesteuerte Suche ist vergleichbar mit der manuellen Suche, durchsucht jedoch alle Dateien und E-Mail-Nachrichten (nur Advanced) im angegebenen Zeitintervall und zum festgesetzten Zeitpunkt. Verwenden Sie die zeitgesteuerte Suche, um die routinemäßige Suche auf den Clients zu automatisieren und die Verwaltung des Bedrohungsschutzes zu optimieren.

Tipp

Führen Sie zeitgesteuerte Suchen bei geringem Netzaufkommen durch, um potenzielle Störungen für Nutzer und Netzwerk zu minimieren.

Zeitgesteuerte Suchen konfigurieren

Trend Micro empfiehlt, die zeitgesteuerte Suche nicht gleichzeitig mit einem zeitgesteuerten Update durchzuführen. Die zeitgesteuerte Suche könnte vorzeitig beendet werden. Dies gilt auch, wenn Sie eine manuelle Suche starten, solange die zeitgesteuerte Suche noch ausgeführt wird. Die zeitgesteuerte Suche wird dann unterbrochen, später jedoch gemäß dem Zeitplan wieder normal ausgeführt.

Prozedur

1. Navigieren Sie zu **Suche** > **Zeitgesteuerte Suche**.
2. Klicken Sie auf die Registerkarte **Zeitplan**.
   a. Konfigurieren Sie das Suchintervall (täglich, wöchentlich oder monatlich) und den Zeitpunkt. Jede Gruppe und jeder Messaging Security Agent kann über einen eigenen Zeitplan verfügen.

Hinweis

Wenn Sie bei monatlichen Suchen 31, 30 oder 29 Tage auswählen und ein Monat weniger Tage hat, wird in diesem Monat keine Suche durchgeführt.

b. (Optional) Wählen Sie **Client nach einer zeitgesteuerten Suche herunterfahren**.

c. Klicken Sie auf **Speichern**.

3. Klicken Sie auf die Registerkarte **Einstellungen** und konfigurieren Sie alle erforderlichen Einstellungen für die zeitgesteuerte Suche.

Anleitungen und Hinweise	Empfohlene Sucheinstellungen
Klicken Sie auf eine Desktop- oder Servergruppe, um die Sucheinstellungen für den **Security Agent** anzupassen. Weitere Informationen finden Sie unter *Suchziele und Aktionen für Security Agents auf Seite 7-10*. **Hinweis** Wenn Sie Benutzern Rechte zur Konfiguration ihrer eigenen Sucheinstellungen erteilen, werden diese benutzerdefinierten Einstellungen bei der Suche verwendet.	Ziel • Alle durchsuchbaren Dateien:alle durchsuchbaren Dateien werden berücksichtigt. Zu den nicht durchsuchbaren Dateien gehören kennwortgeschützte und verschlüsselte Dateien sowie Dateien, die die vom Benutzer festgelegten Suchkriterien nicht erfüllen. • Komprimierte Dateien bis zu Ebene 2 durchsuchen: Durchsucht komprimierte Dateien mit einer oder zwei Komprimierungsebenen.
	Ausschlüsse • Verzeichnisse, in denen Trend Micro Produkte installiert sind, werden von der Suche ausgeschlossen.
	Erweiterte Einstellungen • Liste der zulässigen Spyware/ Grayware (nur für Anti-Spyware) ändern

Anleitungen und Hinweise	Empfohlene Sucheinstellungen
Erweitern Sie einen Agent und klicken Sie auf folgende Elemente, um die Sucheinstellungen für den **Messaging Security Agent** anzupassen: • **Virenschutz**: Zur Suche nach Viren und anderen Arten von Malware. Weitere Informationen finden Sie unter *Suchziele und Aktionen für Messaging Security Agents auf Seite 7-18*. • **Content-Filter**: Zur Suche nach unzulässigem Inhalt in E-Mails. Weitere Informationen finden Sie unter *Content-Filter-Regeln verwalten auf Seite 6-17*. • **Sperren von Anhängen**: Zur Suche nach unzulässigen Anhängen in E-Mails. Weitere Informationen finden Sie unter *Das Sperren von Anhängen konfigurieren auf Seite 6-50*.	• Der Agent führt jeden Sonntag um 5.00 Uhr eine Suche durch. • Passen Sie diesen Zeitplan so an, dass die Suche auf Ihren Clients bei geringem Netzaufkommen durchgeführt wird. Der Agent durchsucht alle durchsuchbaren Dateien. Dabei wird auch der Nachrichtentext einer E-Mail in die Suche einbezogen. • Beim Fund einer mit einem Virus oder anderer Malware infizierten Datei säubert der Agent diese Datei. Kann die Datei nicht gesäubert werden, wird sie durch Text oder eine Datei ersetzt. • Beim Fund einer mit einem Trojaner oder Wurm infizierten Datei ersetzt der Agent diesen Trojaner oder Wurm durch einen Text oder eine Datei. • Beim Fund einer mit einem Packer infizierten Datei ersetzt der Agent diesen Packer durch einen Text oder eine Datei. • Der Agent säubert keine infizierten komprimierten Dateien.

4. Wählen Sie die Gruppen und/oder Messaging Security Agents aus, die die Einstellungen für die zeitgesteuerte Suche anwenden sollen.

Hinweis

Deaktivieren Sie die zeitgesteuerte Suche für die Gruppe oder den Messaging Security Agent, indem Sie das entsprechende Kontrollkästchen deaktivieren.

5. Klicken Sie auf **Speichern**.

Suchziele und Aktionen für Security Agents

Konfigurieren Sie die folgenden Einstellungen für jeden Suchtyp (manuelle Suche, zeitgesteuerte Suche und Echtzeitsuche):

Ziel (Registerkarte)

Wählen Sie eine Suchmethode:

- **Alle durchsuchbaren Dateien**: Alle durchsuchbaren Dateien werden berücksichtigt. Zu den nicht durchsuchbaren Dateien gehören kennwortgeschützte und verschlüsselte Dateien sowie Dateien, die die vom Benutzer festgelegten Suchkriterien nicht erfüllen.

  Hinweis

  Diese Option bietet die höchstmögliche Sicherheit. Das Durchsuchen jeder Datei erfordert allerdings viel Zeit und viele Ressourcen und ist möglicherweise in manchen Fällen gar nicht notwendig. Deshalb können Sie bei Bedarf die Anzahl der durchsuchten Dateien begrenzen.

- **IntelliScan: Verwendet True-File-Type-Erkennung**: Durchsucht Dateien auf Grundlage des ursprünglichen Dateityps. Weitere Informationen finden Sie unter *IntelliScan auf Seite D-2*.

- **Dateien mit diesen Erweiterungen durchsuchen**: Legen Sie manuell fest, welche Dateien anhand der Dateierweiterung durchsucht werden sollen. Trennen Sie mehrere Einträge mit Kommas.

Wählen Sie einen Auslöser für die Suche aus:

- **Lesen**: Durchsucht Dateien, deren Inhalt gelesen wird. Dateien werden gelesen, wenn sie geöffnet, ausgeführt, kopiert oder verschoben werden.

- **Schreiben**: Durchsucht Dateien, deren Inhalt geschrieben wird. Der Inhalt einer Datei wird geschrieben, wenn die Datei geändert, gespeichert, heruntergeladen oder von einem anderen Speicherort kopiert wird.

- **Lesen oder Schreiben**

Suchausschlüsse

Die folgenden Einstellungen können konfiguriert werden:

- Ausschlüsse aktivieren oder deaktivieren
- Trend Micro Produktverzeichnisse von der Suche ausschließen
- Andere Verzeichnisse von der Suche ausschließen

  Alle in dem angegebenen Verzeichnispfad enthaltenen Unterverzeichnisse werden ebenfalls ausgeschlossen.
- Dateinamen oder Dateinamen mit vollständiger Pfadangabe von der Suche ausschließen
- Dateierweiterungen ausschließen

  Platzhalter wie z. B. „*“ sind als Dateierweiterung nicht zulässig.

Hinweis

(Nur Advanced) Wenn auf einem Client Microsoft Exchange Server ausgeführt wird, sollten Sie alle Microsoft Exchange Server-Ordner von der Suche ausschließen. Um Ordner des Microsoft Exchange Servers generell von der Suche auszuschließen, navigieren Sie zu **Administration** > **Allgemeine Einstellungen** > **Desktop/Server {Registerkarte}** > **Allgemeine Sucheinstellungen** und wählen Sie anschließend die Option **Die Ordner des Microsoft Exchange Servers ausschließen, wenn auf Microsoft Exchange Server installiert** aus.

Erweiterte Einstellungen

SUCHTYP	OPTIONEN
Echtzeitsuche	**POP3-Nachrichten durchsuchen**: Standardmäßig kann Mail Scan nur neue Nachrichten im Posteingang oder Junk-Mail-Ordner durchsuchen, die über Port 110 versendet wurden. Es unterstützt sichere POP3 (SSL-POP3) nicht. • Microsoft Outlook 2007, 2010 oder 2013 • Mozilla Thunderbird 1.5 oder höher Mail Scan findet weder Sicherheitsrisiken noch Spam in IMAP-Nachrichten. Verwenden Sie den Messaging Security Agent (nur Advanced), um IMAP-Nachrichten nach Sicherheitsrisiken und Spam zu durchsuchen.
Echtzeitsuche, manuelle Suche	**Verbundene Laufwerke und freigegebene Ordner im Netzwerk durchsuchen**: Wählen Sie diese Option aus, um Verzeichnisse zu durchsuchen, die sich physisch auf anderen Computern befinden, aber als Netzwerklauf auf dem lokalen Computer eingebunden sind.
Echtzeitsuche	**Diskettenlaufwerke beim Herunterfahren des Systems durchsuchen**
Echtzeitsuche	**IntelliTrap aktivieren**: IntelliTrap entdeckt in komprimierten Dateien bösartigen Code, wie Bots. Weitere Informationen finden Sie unter *IntelliTrap auf Seite D-3*.
Echtzeitsuche	**Verschiedene Varianten von Quarantäne-Malware in Speicher entdeckt**: Wenn die Echtzeitsuche und die Verhaltensüberwachung aktiviert sind und diese Option ausgewählt wird, wird der ausgeführte Prozess im Arbeitsspeicher auf komprimierte Malware untersucht. Jegliche komprimierte Malware, die durch die Verhaltensüberwachung erkannt wird, wird in Quarantäne verschoben.
Echtzeitsuche, manuelle Suche, zeitgesteuerte Suche	**Komprimierte Dateien bis zu folgender Ebene durchsuchen**: Eine komprimierte Datei hat für jeden Komprimierungsvorgang eine Ebene. Wenn eine infizierte Datei mehrere Komprimierungsebenen hat, muss die angegebene Anzahl von Ebenen durchsucht werden, um die Infektion zu erkennen. Das Durchsuchen mehrerer Ebenen erfordert jedoch mehr Zeit und Ressourcen.

Suchtyp	Optionen
Echtzeitsuche, manuelle Suche, zeitgesteuerte Suche	**Liste der zulässigen Spyware/Grayware bearbeiten**: Diese Einstellung kann nicht über die Agent-Konsole konfiguriert werden.
Manuelle Suche, Zeitgesteuerte Suche	**CPU-Auslastung/Suchgeschwindigkeit**: Der Security Agent kann nach dem Durchsuchen einer Datei und vor dem Durchsuchen der nächsten eine Pause machen. Wählen Sie unter folgenden Optionen: • **Hoch**: Ohne Pause zwischen den Suchläufen • **Mittel**: Pause zwischen den Suchläufen, wenn die CPU-Auslastung über 50 % liegt, sonst keine Pause • **Niedrig**: Pause zwischen den Suchläufen, wenn die CPU-Auslastung über 20 % liegt, sonst keine Pause
Manuelle Suche, Zeitgesteuerte Suche	**Erweitertes Cleanup ausführen**: Der Security Agent beendet Aktivitäten, die von einer bösartigen Sicherheitssoftware, auch bekannt als FakeAV, ausgeführt werden. Der Agent setzt ebenfalls erweiterte Cleanup-Regeln zur proaktiven Erkennung und zum Beenden von Anwendungen ein, die ein FakeAV-Verhalten zeigen. **Hinweis** Das erweiterte Cleanup bietet zwar proaktiven Schutz, löst aber auch viele Fehlalarme aus.

Liste der zulässigen Spyware/Grayware

Einige Anwendungen werden von Trend Micro als Spyware/Grayware eingestuft – nicht, weil sie für das System, auf dem sie installiert sind, schädlich sind, sondern weil Sie den Client oder das Netzwerk möglicherweise Angriffen durch Malware oder Hacker aussetzen.

Worry-Free Business Security enthält eine Liste mit potenziell gefährlichen Anwendungen und verhindert standardmäßig, dass diese auf Clients ausgeführt werden.

Damit Anwendungen, die von Trend Micro als Spyware oder Grayware eingestuft wurden, auf Clients ausgeführt werden können, müssen Sie

zunächst den Namen der Anwendung zur Liste der zulässigen Spyware/ Grayware hinzufügen.

Aktion (Registerkarte)

Security Agents können gegen Viren/Malware folgende Aktionen durchführen:

TABELLE 7-1. Viren-/Malware-Suchaktionen

AKTION	BESCHREIBUNG
Löschen	Die infizierte Datei wird gelöscht.
Quarantäne	Die infizierte Datei wird umbenannt und anschließend in das temporäre Quarantäne-Verzeichnis auf dem Client verschoben. Der Security Agent sendet die Datei anschließend an das festgelegte Quarantäne-Verzeichnis, das sich standardmäßig auf dem Security Server befindet. Der Security Agent verschlüsselt Dateien in Quarantäne, die an dieses Verzeichnis gesendet wurden. Mit dem VSEncrypt-Tool können Sie beliebige Dateien in der Quarantäne wiederherstellen.
Säubern	Die infizierte Datei wird gesäubert, bevor der vollständige Zugriff möglich ist. Lässt sich die Datei nicht säubern, führt der Security Agent zusätzlich eine der folgenden Aktionen aus: Quarantäne, Löschen, Umbenennen und Übergehen. Diese Aktion kann auf alle Arten von Malware angewendet werden, außer wahrscheinliche Viren/Malware. **Hinweis** Einige Dateien lassen sich nicht säubern. Weitere Informationen finden Sie unter *Dateien, die nicht gesäubert werden können auf Seite D-27*.
Umbenennen	Die Erweiterung der infizierten Datei wird in `'vir'` geändert. Der Benutzer kann die umbenannte Datei erst öffnen, wenn sie mit einer bestimmten Anwendung verknüpft wird. Beim Öffnen der umbenannten, infizierten Datei wird der Virus/die Malware möglicherweise ausgeführt.

Aktion	Beschreibung
Übergehen	Nur bei manueller und zeitgesteuerter Suche. Der Security Agent kann diese Suchaktion während der Echtzeitsuche nicht verwenden. Beim Versuch, eine infizierte Datei zu öffnen oder auszuführen, könnte der Virus oder die Malware ausgeführt werden, wenn keine Suchaktion durchgeführt wird. Alle anderen Suchaktionen können bei der Echtzeitsuche verwendet werden.
Zugriff verweigern	Nur bei Echtzeitsuche. Beim Versuch, eine infizierte Datei zu öffnen oder auszuführen, wird dieser Vorgang durch den Security Agent sofort unterbunden. Die infizierte Datei kann manuell gelöscht werden.

Die vom Security Agent durchgeführte Suchaktion hängt vom Suchtyp ab, der die Spyware/Grayware entdeckt. Während bestimmte Aktionen für jeden Viren-/Malware-Typ konfiguriert werden können, kann für alle Typen von Spyware/Grayware nur eine Aktion konfiguriert werden. Sobald der Security Agent beispielsweise bei der manuellen Suche (Suchtyp) Spyware/Grayware entdeckt, werden die betroffenen Systemressourcen gesäubert (Aktion).

Der Security Agent kann gegen Spyware/Grayware folgende Aktionen durchführen:

Tabelle 7-2. Spyware-/Grayware-Suchaktionen

Aktion	Beschreibung
Säubern	Es werden Prozesse beendet oder Registrierungseinträge, Dateien, Cookies und Verknüpfungen gelöscht.
Übergehen	Der Fund von Spyware/Grayware wird in den Protokollen gespeichert, aber keine Aktion durchgeführt. Diese Aktion kann nur bei manueller und zeitgesteuerter Suche durchgeführt werden. Während der Echtzeitsuche wird die Aktion „Zugriff verweigern“ ausgeführt. Der Security Agent führt keine Aktion aus, wenn sich die erkannte Spyware/Grayware auf der Liste der zulässigen Software befindet.
Zugriff verweigern	Verweigert den Zugriff (Kopieren, Öffnen) auf die entdeckten Spyware-/Grayware-Komponenten. Diese Aktion kann nur bei der Echtzeitsuche durchgeführt werden. Während der manuellen Suche und der zeitgesteuerten Suche wird die Aktion Übergehen ausgeführt.

ActiveAction

Unterschiedliche Viren-/Malware-Typen erfordern unterschiedliche Suchaktionen. Unterschiedliche Suchaktionen benutzerdefiniert festzulegen, setzt jedoch grundlegendes Wissen über Viren/Malware voraus und kann äußerst zeitaufwendig sein. Der Security Agent verwendet ActiveAction, um diesen Problemen entgegenzuwirken.

In ActiveAction sind mehrere bereits vorkonfigurierte Aktionen für die Suche nach Viren/Malware zusammengefasst. ActiveAction sollten Sie verwenden, wenn Sie mit der Konfiguration von Suchaktionen nicht vertraut sind oder nicht genau wissen, welche Suchaktion sich für einen bestimmten Viren-/Malware-Typ am besten eignet.

Welche Vorteile bietet die Verwendung von ActiveAction?

- ActiveAction verwendet von Trend Micro empfohlene Suchaktionen. Der zeitliche Aufwand für die Konfiguration der Suchaktionen entfällt dadurch.
- Die Angriffsstrategien der Viren/Malware gegen Endpunkte ändern sich permanent. Die ActiveAction Einstellungen werden aktualisiert, um vor den neuesten Bedrohungen und Methoden von Viren-/Malware-Angriffen zu schützen.

Die folgende Tabelle zeigt, wie ActiveAction mit den jeweiligen Viren-/Malware-Arten verfährt:

Tabelle 7-3. Von Trend Micro empfohlene Suchaktionen gegen Viren und Malware

Viren-/Malware-Typ	Echtzeitsuche		Manuelle Suche/ Zeitgesteuerte Suche	
	Erste Aktion	Zweite Aktion	Erste Aktion	Zweite Aktion
Scherzprogramm	Quarantäne	Löschen	Quarantäne	Löschen
Trojaner/Würmer	Quarantäne	Löschen	Quarantäne	Löschen
Packer	Quarantäne	n. v.	Quarantäne	n. v.

Viren-/Malware-Typ	Echtzeitsuche		Manuelle Suche/ Zeitgesteuerte Suche	
	Erste Aktion	Zweite Aktion	Erste Aktion	Zweite Aktion
Wahrscheinlich Virus/Malware	Übergehen	n. v.	Übergehen oder vom Benutzer konfigurierte Aktion	n. v.
Virus	Säubern	Quarantäne	Säubern	Quarantäne
Testviren	Zugriff verweigern	n. v.	n. v.	n. v.
Andere Malware	Säubern	Quarantäne	Säubern	Quarantäne

Hinweis

- Einige Dateien lassen sich nicht säubern. Weitere Informationen finden Sie unter *Dateien, die nicht gesäubert werden können auf Seite D-27*.
- ActiveAction ist nicht für die Suche nach Spyware/Grayware verfügbar.
- Die Standardwerte für diese Einstellungen können sich ändern, wenn neue Pattern-Dateien verfügbar werden.

Erweiterte Einstellungen

Suchtyp	Optionen
Echtzeitsuche, zeitgesteuerte Suche	**Warnung bei Viren-/Spyware-Fund auf Desktop oder Server anzeigen**
Echtzeitsuche, zeitgesteuerte Suche	**Warnung auf dem Desktop oder Server anzeigen, wenn ein mutmaßlicher Virus bzw. mutmaßliche Spyware erkannt wird**
Manuelle Suche, Echtzeitsuche, zeitgesteuerte Suche	**Cleanup bei Viren-/Malwareverdacht durchführen**: Nur verfügbar, wenn Sie ActiveAction wählen und die Aktion für Viren-/ Malwareverdacht anpassen.

Suchziele und Aktionen für Messaging Security Agents

Konfigurieren Sie die folgenden Einstellungen für jeden Suchtyp (manuelle Suche, zeitgesteuerte Suche und Echtzeitsuche):

Ziel (Registerkarte)

- Suchziele
- Zusätzliche Einstellungen für die Suche nach Bedrohungen
- Suchausschlüsse

Aktion (Registerkarte)

- Suchaktionen/ActiveAction
- Benachrichtigungen
- Erweiterte Einstellungen

Suchziele

Suchziele auswählen:

- **Alle angehängten Dateien**: Nur verschlüsselte oder kennwortgeschützte Dateien werden ausgeschlossen.

  Hinweis

  Diese Option bietet die höchstmögliche Sicherheit. Das Durchsuchen jeder Datei erfordert allerdings viel Zeit und viele Ressourcen und ist möglicherweise in manchen Fällen gar nicht notwendig. Deshalb können Sie bei Bedarf die Anzahl der durchsuchten Dateien begrenzen.

- **IntelliScan**: Durchsucht Dateien auf Grundlage des ursprünglichen Dateityps. Weitere Informationen finden Sie unter *IntelliScan auf Seite D-2*.
- **Ausgewählte Dateitypen**: Worry-Free Business Security durchsucht Dateien des ausgewählten Dateityps und mit den ausgewählten

Erweiterungen. Trennen Sie mehrere Einträge durch Strichpunkte (;) voneinander.

Andere Optionen auswählen:

- **IntelliTrap aktivieren**: IntelliTrap entdeckt in komprimierten Dateien bösartigen Code, wie Bots. Weitere Informationen finden Sie unter *IntelliTrap auf Seite D-3*.
- **Nachrichtentext durchsuchen**: Durchsucht den Nachrichtentext einer E-Mail, die eingebettete Bedrohungen enthalten könnte.

Zusätzliche Einstellungen für die Suche nach Bedrohungen

Wählen Sie andere Bedrohungen aus, die der Agent durchsuchen sollte. Weitere Informationen zu diesen Bedrohungen finden Sie unter *Bedrohungen verstehen auf Seite 1-8*.

Wählen Sie zusätzliche Optionen aus:

- **Infizierte Datei vor dem Säubern sichern**: Worry-Free Business Security erstellt vor dem Säubern eine Sicherungskopie der infizierten Datei. Die gesicherte Datei wird verschlüsselt und im folgenden Verzeichnis auf dem Client gespeichert:

  ```
  <Messaging Security Agent Installationsordner>\storage
  \backup
  ```

  Sie können das Verzeichnis im Unterabschnitt **Backup-Einstellung** des Abschnitts **Erweiterte Optionen** ändern.

  Informationen zum Entschlüsseln der Datei finden Sie unter *Verschlüsselte Dateien wiederherstellen auf Seite 14-18*.

- **Säubern Sie keine komprimierten Dateien, um die Leistung nicht zu beeinträchtigen.**

Suchausschlüsse

Gehen Sie in der Registerkarte **Ziele** zum Bereich **Ausschlüsse**, und wählen Sie aus den folgenden Kriterien aus, die der Agent verwendet, um E-Mail-Nachrichten von der Suche auszuschließen:

- **Der Nachrichtentext größer ist als**: Der Messaging Security Agent durchsucht E-Mail-Nachrichten nur, wenn der Text der Nachricht kleiner oder gleich dem angegebenen Wert ist.
- **Der Anhang größer ist als**: Der Messaging Security Agent durchsucht E-Mail-Nachrichten nur, wenn die angehängte Datei kleiner oder gleich dem angegebenen Wert ist.

Tipp

Trend Micro empfiehlt maximal 30 MB.

- **Die Anzahl der dekomprimierten Dateien höher ist als**: Liegt in der komprimierten Datei die Zahl der dekomprimierten Dateien über diesem Wert, durchsucht der Messaging Security Agent nur Dateien bis zur festgelegten Obergrenze.
- **Die dekomprimierte Datei größer ist als**: Der Messaging Security Agent durchsucht nur komprimierte Dateien, die nach der Dekomprimierung kleiner oder gleich diesem Wert sind.
- **Die Anzahl der Komprimierungsebenen höher ist als**: Der Messaging Security Agent durchsucht nur komprimierte Dateien, die weniger oder ebenso viele Kompressionsebenen angegeben haben. Wenn Sie z. B. die Komprimierungsebenen auf 5 beschränken, durchsucht der Messaging Security Agent die ersten 5 Ebenen von komprimierten Dateien. Komprimierte Dateien mit 6 oder mehr Ebenen werden nicht durchsucht.
- **Die dekomprimierte Datei ist 'x'-mal größer als die komprimierte Datei**: Der Messaging Security Agent durchsucht komprimierte Dateien nur, wenn das Verhältnis zwischen der Größe der dekomprimierten Datei und der Größe der komprimierten Datei kleiner als dieser Wert ist. Diese Funktion verhindert, dass der Messaging Security Agent eine komprimierte Datei durchsucht, die einen Denial-of-Service (DoS)-Angriff auslösen könnte. Bei einem DoS-Angriff werden die Ressourcen eines Mail-Servers mit unnötigen Aufgaben überflutet. Dies wird verhindert, wenn der Messaging Security Agent keine Dateien durchsuchen muss, die nach der Dekomprimierung sehr groß sind.

Beispiel: In der unten stehenden Tabelle wurde 100 als Wert für 'x' eingegeben.

Dateigrösse (nicht komprimiert)	Dateigrösse (nicht komprimiert)	Ergebnis
500 KB	10 KB (Verhältnis 50:1)	Durchsucht
1.000 KB	10 KB (Verhältnis 100:1)	Durchsucht
1.001 KB	10 KB (Verhältnis ist höher als 100:1)	Nicht durchsucht*
2.000 KB	10 KB (Verhältnis 200:1)	Nicht durchsucht*

* Der Messaging Security Agent führt die Aktion aus, die Sie für ausgeschlossene Dateien konfiguriert haben.

Suchaktionen

Administratoren können den Messaging Security Agent so konfigurieren, dass er Aktionen je nach Art der Bedrohung (Viren/Malware, Trojaner, Würmer) durchführt. Wenn Sie benutzerdefinierte Aktionen verwenden, können Sie für jeden Bedrohungstyp eine eigene Aktion festlegen.

Tabelle 7-4. Messaging Security Agent – benutzerdefinierte Aktionen

Aktion	Beschreibung
Säubern	Bösartiger Code wird aus infizierten Nachrichtentexten und -anhängen entfernt. Der verbleibende Nachrichtentext sowie alle nicht infizierten Dateien und gesäuberten Dateien werden an die beabsichtigten Empfänger weitergeleitet. Bei Viren und Malware empfiehlt Trend Micro Säubern als Standardsuchaktion. In einigen Fällen kann der Messaging Security Agent eine Datei nicht säubern Während einer manuellen oder zeitgesteuerten Suche aktualisiert der Messaging Security Agent den Informationsspeicher und ersetzt die ursprüngliche durch die gesäuberte Datei.

Aktion	Beschreibung
Durch Text/Datei ersetzen	Entfernt den infizierten Inhalt und ersetzt ihn durch Text oder eine Datei. Die E-Mail wird dem beabsichtigten Empfänger zugestellt, wobei dieser in der Textdatei darüber informiert wird, dass der ursprüngliche Inhalt der E-Mail infiziert war und daher ersetzt wurde. Bei Content-Filter und Prävention vor Datenverlust können Sie den Text nur in den Feldern für Textkörper oder Anhang ersetzen (und nicht Von, An, CC oder Betreff).
Gesamte Nachricht in Quarantäne	(Nur Echtzeitsuche) Nur der infizierte Inhalt wird in den Quarantäne-Ordner verschoben, und der Empfänger erhält die Nachricht ohne diesen Inhalt. Bei Content-Filter, Prävention vor Datenverlust und Sperren von Anhängen wird die gesamte Nachricht in den Quarantäne-Ordner verschoben.
Nachrichtenteil in Quarantäne	(Nur Echtzeitsuche) Nur der infizierte oder gefilterte Inhalt wird in den Quarantäne-Ordner verschoben, und der Empfänger erhält die Nachricht ohne diesen Inhalt.
Gesamte Nachricht löschen	(Nur Echtzeitsuche) Die gesamte Nachricht wird gelöscht. Der ursprüngliche Empfänger erhält die Nachricht nicht.
Bestanden	Infektionen mit bösartigen Dateien werden in den Virenprotokollen aufgezeichnet, es wird jedoch keine Aktion durchgeführt. Ausgeschlossene, verschlüsselte oder kennwortgeschützte Dateien werden dem Empfänger zugestellt, die Protokolle werden nicht aktualisiert. Bei Content-Filter wird die Nachricht unverändert gesendet.
Archivieren	Die Nachricht wird in das Archiv verschoben und an den Absender zurückgesendet.
Quarantäne-Nachrichten in den Spam-Ordner auf dem Server verschieben	Die gesamte Nachricht wird in den Quarantäne-Ordner auf dem Security Server verschoben.

Aktion	Beschreibung
Nachricht in den Spam-Ordner des Benutzers verschieben	Die gesamte Nachricht wird in den Spam-Ordner des Benutzers verschoben. Der Ordner befindet sich im Informationsspeicher auf dem Server.
Markieren und senden	Es wird eine Markierung in den Header eingefügt, die die Nachricht als Spam kennzeichnet. Anschließend wird sie an den beabsichtigten Empfänger gesendet.

Ergänzend zu diesen Aktionen können Sie das Folgende konfigurieren:

- **Aktion bei Massenmail-Verhalten aktivieren**: Wählen Sie für Bedrohungen mit Massenmail-Verhalten zwischen den Aktionen Säubern, Durch Text/Datei ersetzen, Ganze Nachricht löschen, Übergehen oder Nachrichtenteil in Quarantäne.
- **Folgende Aktion ausführen, wenn die Säuberung fehlgeschlagen ist**: Legen Sie fest, welche Zweitaktion bei fehlgeschlagenem Säubern durchgeführt werden soll. Wählen Sie zwischen Durch Text/Datei ersetzen, Ganze Nachricht löschen, Übergehen oder Nachrichtenteil in Quarantäne.

ActiveAction

Die folgende Tabelle zeigt, wie ActiveAction mit den jeweiligen Viren-/Malware-Arten verfährt:

Tabelle 7-5. Von Trend Micro empfohlene Suchaktionen gegen Viren und Malware

Viren-/Malware-Typ	Echtzeitsuche		Manuelle Suche/ Zeitgesteuerte Suche	
	Erste Aktion	Zweite Aktion	Erste Aktion	Zweite Aktion
Virus	Säubern	Gesamte Nachricht löschen	Säubern	Durch Text/ Datei ersetzen
Trojaner/Würmer	Durch Text/ Datei ersetzen	n. v.	Durch Text/ Datei ersetzen	n. v.

Viren-/Malware-Typ	Echtzeitsuche		Manuelle Suche/ Zeitgesteuerte Suche	
	Erste Aktion	Zweite Aktion	Erste Aktion	Zweite Aktion
Packer	Nachrichtenteil in Quarantäne	n. v.	Nachrichtenteil in Quarantäne	n. v.
Anderer bösartiger Code	Säubern	Gesamte Nachricht löschen	Säubern	Durch Text/ Datei ersetzen
Weitere Bedrohungen	Nachrichtenteil in Quarantäne	n. v.	Durch Text/ Datei ersetzen	n. v.
Massenmail-Verhalten	Gesamte Nachricht löschen	n. v.	Durch Text/ Datei ersetzen	n. v.

Benachrichtigungen von Suchaktionen

Wählen Sie die Option **Empfänger benachrichtigen**, damit der Messaging Security Agent die beabsichtigten Empfänger benachrichtigt, wenn Maßnahmen gegen eine bestimmte E-Mail-Nachricht durchgeführt werden. Aus verschiedenen Gründen ist es nicht ratsam, externe E-Mail-Empfänger zu benachrichtigen, dass eine Nachricht gesperrt wurde, die vertrauliche Informationen enthielt. Wählen Sie die Option **Externe Empfänger nicht benachrichtigen**, damit nur interne Nachrichten-Empfänger benachrichtigt werden. Legen Sie interne Adressen unter **Aktionen** > **Einstellungen für die Benachrichtigung** > **Interne Nachrichtendefinition** fest.

Sie können auch das Senden von Benachrichtigungen an die externen Empfänger von Spoofing-Mails deaktivieren.

Erweiterte Einstellungen (Suchaktionen)

Einstellungen	Details

Makros	Makroviren sind anwendungsspezifische Viren, die Makro-Dienstprogramme für Anwendungen infizieren. Die erweiterte Makrosuche verwendet die heuristische Suche zum Erkennen von Makroviren oder Entfernen aller erkannten Makrocodes. Die heuristische Suche ist eine Bewertungsmethode zum Erkennen von Viren, bei der die Suche nach bösartigem Makrocode anhand der Pattern-Erkennung und regelbasierter Techniken erfolgt. Diese Methode eignet sich besonders für die Entdeckung neuer Viren und Bedrohungen, deren Virensignatur noch nicht bekannt ist.
	
	Welche Aktionen der Messaging Security Agent gegen bösartigen Makro-Code ausführt, hängt von der Aktion ab, die Sie konfiguriert haben.
	
	• **Heuristische Stufe**
	  • Stufe 1 verwendet die genauesten Kriterien, erkennt allerdings die wenigsten Makrocodes.
	  • Stufe 4 erkennt die meisten Makrocodes, verwendet dazu jedoch die umfassendsten Kriterien und kann daher sicheren Makrocode als bösartigen Makrocode identifizieren.
	
	Tipp
	Trend Micro empfiehlt die heuristische Stufe 2. Diese bietet eine hohe Erkennungsstufe für unbekannte Makroviren, eine hohe Suchgeschwindigkeit und verwendet nur Regeln, die zum Überprüfen von Makroviren-Zeichenketten nötig sind. Bei Stufe 2 kommt es außerdem relativ selten vor, dass sicherer Code als bösartiger Makrocode identifiziert wird.
	
	• **Alle entdeckten Makros entfernen**: Entfernt alle Makrocodes, die auf durchsuchten Dateien erkannt wurden

Nicht durchsuchbare Nachrichtenteile	Legen Sie die Bedingungen für die Aktion und die Benachrichtigung bei verschlüsselten und/oder kennwortgeschützten Dateien fest. Wählen Sie als Aktion "Durch Text/Datei ersetzen", "Gesamte Nachricht in Quarantäne", "Gesamte Nachricht löschen", "Übergehen" oder "Nachrichtenteil in Quarantäne" aus.

Einstellungen	Details
Ausgeschlossene Nachrichtenteile	Legen Sie die Bedingungen für die Aktion und die Benachrichtigung bei ausgeschlossenen Nachrichtenteilen fest. Wählen Sie als Aktion "Durch Text/Datei ersetzen", "Gesamte Nachricht in Quarantäne", "Gesamte Nachricht löschen", "Übergehen" oder "Nachrichtenteil in Quarantäne" aus.
Backup-Einstellung	Der Ort, an dem die Sicherungskopie oder die infizierten Dateien gespeichert werden, bevor der Agent sie gesäubert hat.
Einstellungen für das Ersetzen	Konfigurieren Sie den Text und die Datei für den Ersatztext. Bei der Aktion **Durch Text/Datei ersetzen** ersetzt Worry-Free Business Security die Bedrohung mit diesem Text oder dieser Datei.

Kapitel 8

Updates verwalten

In diesem Kapitel werden die Komponenten und Update-Verfahren von Worry-Free Business Security beschrieben.

Update-Übersicht

Alle Komponenten-Updates stammen vom Trend Micro ActiveUpdate Server. Wenn Updates verfügbar sind, lädt der Security Server die aktualisierten Komponenten herunter und verteilt sie an die Security Agents und Messaging Security Agents (nur Advanced).

Wird mit einem Security Server eine große Anzahl von Security Agents verwaltet, können die Updates einen Großteil der Servercomputer-Ressourcen verbrauchen und somit die Stabilität und Leistung des Servers beeinflussen. Um diesem Problem zu begegnen, besitzt Worry-Free Business Security eine **Update-Agent**-Funktion, die bestimmten Security Agents ermöglicht, bei der Verteilung von Updates an andere Security Agents mitzuwirken.

In der folgenden Tabelle sind die Optionen aufgeführt, die für das Komponenten-Update bei Security Servern und Agents verfügbar sind, sowie Empfehlungen, wann diese am besten zur Anwendung kommen:

Tabelle 8-1. Update-Optionen

Update-Reihenfolge	Beschreibung	Empfehlung
1. ActiveUpdate Server oder benutzerdefinierte Update-Adresse 2. Security Server 3. Agents	Der Trend Micro Security Server erhält vom ActiveUpdate Server oder einer benutzerdefinierten Update-Adresse aktualisierte Komponenten und verteilt diese unmittelbar an Agents (Security Agents und Messaging Security Agents).	Verwenden Sie diese Methode, wenn es zwischen dem Security Server und den Agents keine Netzwerkabschnitte mit geringer Bandbreite gibt.

Update-Reihenfolge	Beschreibung	Empfehlung
1. ActiveUpdate Server oder benutzerdefinierte Update-Adresse 2. Security Server 3. Update Agents, Messaging Security Agents, Security Agents ohne Update Agents 4. Alle anderen Security Agents	Der Trend Micro Security Server empfängt vom ActiveUpdate Server oder einer benutzerdefinierten Update-Adresse aktualisierte Komponenten und verteilt diese unmittelbar an: • Update Agents • Messaging Security Agents • Security Agents ohne Update Agents Anschließend verteilen die Update Agents die Komponenten an ihre entsprechenden Security Agents. Wenn diese Security Agents nicht aktualisieren können, erfolgt die Aktualisierung direkt vom Security Server.	Verwenden Sie diese Methode zum Ausgleich der Netzwerkbelastung, wenn einige der Netzwerkabschnitte zwischen Security Server und Security Agents eine geringe Bandbreite aufweisen.
1. ActiveUpdate Server 2. Security Agents	Security Agents, die nicht direkt von einer beliebigen Adresse aktualisieren können, aktualisieren direkt vom ActiveUpdate Server. **Hinweis** Messaging Security Agents aktualisieren niemals direkt vom ActiveUpdate Server. Wenn keine Adresse verfügbar ist, beendet der Messaging Security Agent den Update-Vorgang.	Dieser Mechanismus dient nur als letzter Ausweg und erfordert Folgendes: **Trend Micro ActiveUpdate als sekundäre Update-Adresse verwenden** unter Update-Berechtigungen aktivieren

Update-Komponenten

Worry-Free Business Security verwendet Komponenten, mit denen Agents vor den neuesten Bedrohungen geschützt sind. Halten Sie diese Komponenten mit manuellen oder zeitgesteuerten Updates auf dem neuesten Stand.

Sie können die Komponentenliste mit den folgenden Schritten anzeigen:

- Navigieren Sie zu **Updates** > **Manuell**.
- Navigieren Sie zu **Live-Status** und klicken Sie im Agent-Status-Widget auf **Komponentenstatus überprüfen**.

In den folgenden Tabellen werden die Komponenten aufgelistet, die der Security Server vom ActiveUpdate Server heruntergeladen hat:

TABELLE 8-2. Messaging Komponenten (nur Advanced)

KOMPONENTE	VERTEILT AN	BESCHREIBUNG
Messaging Security Agent Anti-Spam-Pattern	Messaging Security Agents	Das Anti-Spam-Pattern erkennt neueste Spam in E-Mail-Nachrichten und E-Mail-Anhängen.
Messaging Security Agent Anti-Spam-Engine 32/64 Bit	Messaging Security Agents	Die Anti-Spam-Engine erkennt Spam in E-Mail-Nachrichten und -Anhängen.
Messaging Security Agent Scan Engine 32/64 Bit	Messaging Security Agents	Die Scan Engine erkennt Internet-Würmer, Massenmail-Viren, Trojaner, Phishing-Sites, Spyware, Sicherheitslücken und Viren in E-Mail-Nachrichten und -Anhängen.
Messaging Security Agent URL-Filter-Engine 32/64 Bit	Messaging Security Agents	Die URL-Filter-Engine erleichtert die Kommunikation zwischen Worry-Free Business Security und dem Trend Micro URL-Filterdienst, der URLs bewertet und die Ergebnisse an Worry-Free Business Security weiterleitet.

Tabelle 8-3. Virenschutz und Smart Scan

Komponente	Verteilt an	Beschreibung
Viren-Pattern	Security Agents, die die herkömmliche Suche verwenden	Das Viren-Pattern enthält Informationen, die Security Agents dabei unterstützen, die neuesten Viren-/Malware-Bedrohungen und kombinierten Bedrohungen zu erkennen. Mehrmals pro Woche und bei jeder Entdeckung besonders schädlicher Viren- oder Malware-Programme erstellt und veröffentlicht Trend Micro ein neues Viren-Pattern.
IntelliTrap Pattern	Security Agents	Das IntelliTrap Pattern erkennt in Echtzeit komprimierte Dateien, die als ausführbare Dateien gepackt sind. Weitere Informationen finden Sie unter *IntelliTrap auf Seite D-3*.
IntelliTrap Ausnahme-Pattern	Security Agents	Das IntelliTrap Ausnahme-Pattern enthält eine Liste „zulässiger“ komprimierter Dateien.
Viren-Scan-Engine (32/64 Bit)	Security Agents	Die Viren-Scan-Engine bildet den Kern aller Trend Micro-Produkte. Sie wurde ursprünglich als Reaktion auf die ersten dateibasierten Viren entwickelt. In ihrer heutigen Form kann sie verschiedene Viren- und Malware-Typen erkennen. Die Viren-Scan-Engine erkennt auch kontrollierte Viren, die zu Forschungszwecken entwickelt und verwendet werden. Die Scan Engine und die Pattern-Datei analysieren Dateien nicht Byte für Byte, sondern erkennen gemeinsam Folgendes: • Charakteristische Merkmale im Virencode • Die genaue Position in einer Datei, an der sich der Virus versteckt

Komponente	Verteilt an	Beschreibung
Smart-Scan-Pattern	Nicht an Security Agents verteilt. Dieses Pattern verbleibt auf dem Security Server und wird bei der Reaktion auf Suchanfragen von Security Agents verwendet.	Im Smart Scan modus verwenden Security Agents zwei einfache Pattern, die zusammen denselben Schutz wie herkömmliche Anti-Malware- und Anti-Spyware-Pattern bieten. Die Mehrheit der Pattern-Definitionen befindet sich im **Smart-Scan-Pattern**. Das **Agent-Pattern von Smart Scan** enthält alle anderen Pattern, die sich nicht im Smart-Scan-Pattern befinden. Der Security Agent sucht mit Hilfe des **Agent-Pattern von Smart Scan** nach Sicherheitsbedrohungen. Security Agents, die das Risiko der Datei während der Suche nicht ermitteln können, überprüfen das Risiko durch Senden einer Suchanfrage an den Scan Server, einen auf dem Security Server gehosteten Dienst. Der Suchserver überprüft das Risiko mit dem**Pattern der intelligenten Suche**. Der Security Agent legt das vom Scan Server gelieferte Suchabfrageergebnis zur Verbesserung der Suchleistung in einem Zwischenspeicher ab.
Agent-Pattern von Smart Scan	Security Agents, die die Smart Scan verwenden	
Damage Cleanup Template	Security Agents	Damage Cleanup Template: Die Damage Cleanup Engine verwendet dieses Template, um z. B. Trojaner-Dateien oder -Prozesse zu erkennen und zu beseitigen.
Damage-Cleanup Engine 32/64 Bit	Security Agents	Die Damage Cleanup Engine sucht und entfernt Trojaner und Trojaner-Prozesse.
Speicher-Inspektions-Pattern	Security Agents	Diese Technologie bietet eine erweiterte Virenprüfung für polymorphe und Mutationsviren und vergrößert Viren-Pattern-basierte Scans durch Emulieren von Dateiausführungen. Die Ergebnisse werden dann in einer kontrollierten Umgebung und mit geringen Auswirkungen auf die Systemleistung auf Nachweise böswilliger Absichten kontrolliert.

Komponente	Verteilt an	Beschreibung
Maschine für Kontextbezogene Intelligenz 32/64-Bit	Security Agents	Die Maschine für Kontextbezogene Intelligenz überwacht von selten vorkommenden Dateien ausgeführte Prozesse und extrahiert Verhaltensfunktionen, die vom Abfragehandhabung für kontextbezogene Intelligenz zu Analysezwecken an das Modul für 'Vorausschauendes Maschinenlernen' gesendet werden.
Kontextintelligenz-Pattern	Security Agents	Das Kontextintelligenz-Pattern enthält eine Liste "geduldeter" Verhaltensweisen, die für bekannte Bedrohungen nicht relevant sind.
Abfragehandhabung für kontextbezogene Intelligenz 32/64-Bit	Security Agents	Der Abfragehandhabung für kontextbezogene Intelligenz verarbeitet von der Maschine für Kontextbezogene Intelligenz erkanntes Verhalten und sendet den Bericht an das Modul für 'Vorausschauendes Maschinenlernen'.
Fortgeschrittenes Bedrohungssuchmaschine 32/64-Bit	Security Agents	Die Fortgeschrittenes Bedrohungssuchmaschine extrahiert Dateifunktionen aus selten vorkommenden Dateien und sendet die Daten an das Modul für 'Vorausschauendes Maschinenlernen'.
Pattern der erweiterten Bedrohungskorrelation	Security Agents	Das Pattern der erweiterten Bedrohungskorrelation enthält eine Liste mit Dateifunktionen, die für bekannte Bedrohungen nicht relevant sind.
Early Boot Cleanup Driver 32-/64-Bit	Security Agents	Der Trend Micro Early Boot Cleanup Driver lädt vor den Betriebssystemtreibern, was das Erkennen und Sperren von Boot-Rootkits ermöglicht. Nachdem der Security Agent geladen wurde, werden vom Trend Micro Early Boot Cleanup Driver die Damage Cleanup Services zum Säubern des Rootkits aufgerufen.

Tabelle 8-4. Anti-spyware

Komponente	Verteilt an	Beschreibung
Spyware/Grayware Scan Engine Version 6 (32/64 Bit)	Security Agents	Die Spyware/Grayware Scan Engine sucht anhand der entsprechenden Suchaktionen nach Spyware/Grayware.
Spyware-/Grayware-Pattern V. 6	Security Agents	Das Spyware-/Grayware-Pattern erkennt Spyware/Grayware in Dateien und Programmen, Speichermodulen, der Windows Registrierung und in URL-Verknüpfungen.
Spyware/Grayware-Pattern	Security Agents	

Tabelle 8-5. Netzwerkvirus

Komponente	Verteilt an	Beschreibung
Pattern der allgemeinen Firewall	Security Agents	Der Pattern der allgemeinen Firewall hilft Agents ähnlich der Viren-Pattern bei der Identifizierung von Virensignaturen, typischen Abfolgen von Bits und Bytes, die auf einen Netzwerkvirus hindeuten.

Tabelle 8-6. Verhaltensüberwachung und Gerätesteuerung

Komponente	Verteilt an	Beschreibung
Erkennungs-Pattern der Verhaltensüberwachung (32/64 Bit)	Security Agents	Dieses Pattern enthält die Regeln für die Erkennung von verdächtigem Bedrohungsverhalten.
Kerntreiber der Verhaltensüberwachung 32/64 Bit	Security Agents	Dieser Treiber im Kernelmodus überwacht Systemereignisse und leitet sie an den Kerndienst der Verhaltensüberwachung zwecks Durchsetzung von Sicherheitsrichtlinien weiter.

Komponente	Verteilt an	Beschreibung
Kerndienst der Verhaltensüberwachung 32/64 Bit	Security Agents	Dieser Dienst im Benutzermodus beinhaltet folgende Funktionen: • Bietet Rootkit-Erkennung • Reguliert den Zugriff auf externe Geräte • Schützt Dateien, Registrierungsschlüssel und Dienste
Pattern zur Konfiguration der Verhaltensüberwachung	Security Agents	Der Treiber der Verhaltensüberwachung verwendet dieses Pattern, um normale Systemereignisse zu erkennen und diese bei der Durchsetzung von Sicherheitsrichtlinien auszuschließen.
Schadensbehebungsmuster	Security Agents	Das Schadensbehebungsmuster enthält Richtlinien, die zur Überwachung von verdächtigem Bedrohungsverhalten verwendet werden.
Pattern für digitale Signaturen	Security Agents	Dieses Muster enthält eine Liste mit gültigen digitalen Signaturen, die vom Kerndienst der Verhaltensüberwachung verwendet werden, um festzulegen, ob ein für ein Systemereignis verantwortliches Programm sicher ist.
Pattern der Richtliniendurchsetzung	Security Agents	Der Kerndienst der Verhaltensüberwachung überprüft Systemereignisse hinsichtlich der Richtlinien in diesem Pattern.
Auslöse-Pattern zum Durchsuchen des Speichers (32/64 Bit)	Security Agents	Der Dienst zum Auslösen der Arbeitsspeicherabfrage führt andere Scan Engines aus, wenn entdeckt wird, dass der Prozess im Speicher entpackt ist.
Muster der Programmsinspektionsüberwachung	Security Agents	Das Muster der Programmsinspektionsüberwachung überwacht und speichert Prüfpunkte, die zur Verhaltensüberwachung verwendet werden.
Bedrohungsverfolgungs-Pattern 32/64 Bit	Security Agents	Das Bedrohungsverfolgungs-Pattern erkennt Angriffe mit dateiloser Malware.

TABELLE 8-7. Browserangriffe

KOMPONENTE	VERTEILT AN	BESCHREIBUNG
Pattern für die Prävention von Angriffen auf Browser	Security Agents	Dieses Pattern identifiziert die aktuellsten Webbrowserangriffe und verhindert, dass die Angriffe zur Gefährdung des Webbrowsers verwendet werden.
Einheitliches Skriptanalysemuster	Security Agents	Dieses Pattern analysiert die Skripte in Webseiten und identifiziert schädliche Skripte.

TABELLE 8-8. Vorausschauendes Maschinenlernen

KOMPONENTE	VERTEILT AN	BESCHREIBUNG
Lokales Dateimodell für 'Vorausschauendes Maschinenlernen'	Security Agents	Das lokale Dateimodell für "Vorausschauendes Maschinenlernen" erkennt Bedrohungen durch portierbare ausführbare Dateien, wenn Endpunkte vom Internet getrennt werden.

Info über Hotfixes, Patches und Service Packs

Nach der Veröffentlichung eines Produkts entwickelt Trend Micro oft Folgendes zur Problembehebung, Leistungsverbesserung oder Funktionserweiterung:

- *Kritischer Patch auf Seite D-2*
- *Hotfix auf Seite D-2*
- *Patch auf Seite D-9*
- *Service Pack auf Seite D-26*

Ihr Händler oder Ihr Support-Anbieter informiert Sie ggf. bei Verfügbarkeit dieser Produkte. Weitere Informationen über neu veröffentlichte Hotfixes, Patches und Service Packs finden Sie auch auf der Trend Micro Website unter:

http://downloadcenter.trendmicro.com/index.php?regs=DE

Jede Veröffentlichung enthält eine Readme-Datei mit Informationen zur Installation, Verteilung und Konfiguration. Lesen Sie die Readme vor der Installation aufmerksam durch.

Security Server-Updates

Automatische Updates

Der Security Server führt automatisch folgende Updates durch:

- Sofort nach der Installation empfängt der Security Server Updates über den Trend Micro ActiveUpdate Server.
- Bei jedem Start des Security Servers werden die Komponenten aktualisiert.
- Standardmäßig werden zeitgesteuerte Updates stündlich ausgeführt (das Zeitintervall für die Updates kann auf der Webkonsole geändert werden).

Manuelle Updates

Sie können über die Webkonsole manuelle Updates ausführen, falls ein Update dringend ist.

Server Update-Hinweise und -Empfehlungen

- Nach einem Update verteilt der Security Server die Komponenten-Updates automatisch an die Agents. Weitere Informationen zum den Komponenten, die an die Agents verteilt werden, finden Sie unter *Update-Komponenten auf Seite 8-4*.
- Ein reiner IPv6-Security Server kann die folgenden Aufgaben nicht ausführen:
  - Beziehen Sie Updates direkt vom Trend Micro ActiveUpdate Server oder einer reinen, benutzerdefinierten IPv4-Update-Adresse.
  - Verteilen Sie Updates direkt auf reine IPv4-Clients.

Ebenso kann ein reiner IPv4 Security Server keine Updates direkt von reinen benutzerdefinierten IPv6-Adressen erhalten und Updates an reine IPv6-Agents verteilen.

In diesen Situationen muss ein Dual-Stack-Proxy-Server, der IP-Adressen wie DeleGate konvertieren kann, ermöglichen, dass der Security Server Updates erhalten und verteilen kann.

- Wenn die Verbindung zum Internet über einen Proxy-Server hergestellt wird, legen Sie auf der Registerkarte **Administration** > **Allgemeine Einstellungen** > **Proxy** die korrekten Proxy-Einstellungen fest, um die Updates herunterzuladen.

Komponentenduplizierung

Damit der Virenschutz immer aktuell ist, veröffentlicht Trend Micro regelmäßig neue Pattern-Dateien. Da Pattern-Datei-Updates regelmäßig verfügbar sind, verwendet Security Server den Mechanismus der **Komponentenduplizierung**, der schnellere Downloads von Pattern-Dateien ermöglicht.

Zusammen mit der neuesten Version einer vollständigen Pattern-Datei werden auf dem Trend Micro ActiveUpdate Server auch inkrementelle Pattern-Dateien zum Download zur Verfügung gestellt. Inkrementelle Pattern sind kleinere Versionen der vollständigen Pattern-Datei und umfassen den Unterschied zwischen der neuesten und vorhergehenden vollständigen Versionen der Pattern-Datei. Wenn beispielsweise 175 die neueste Version ist, umfasst das inkrementelle Pattern v_173.175 Signaturen aus Version 175, die es in Version 173 nicht gibt (Version 173 ist die vorhergehende vollständige Pattern-Version, da der Unterschied zwischen den Pattern-Dateinummern immer zwei beträgt). Das inkrementelle Pattern v_171.175 umfasst Signaturen aus Version 175, die es in Version 171 nicht gibt.

Zur Vermeidung von Netzwerkverkehr, der durch den Download des neuesten Patterns erzeugt wird, dupliziert der Security Server Komponenten. Bei dieser Methode des Komponenten-Updates lädt der Server nur inkrementelle Pattern herunter. Stellen Sie sicher, dass der Security Server regelmäßig aktualisiert wird, um von den Vorteilen der

Komponentenduplizierung zu profitieren. Anderenfalls wird der Server gezwungen, die vollständige Pattern-Datei herunterzuladen.

Komponentenduplizierung betrifft folgende Komponenten:

- Viren-Pattern
- Agent-Pattern von Smart Scan
- Damage Cleanup Template
- IntelliTrap Ausnahme-Pattern
- Spyware-Pattern

Die Update-Adresse des Security Servers konfigurieren

Vorbereitungen

Standardmäßig empfängt der Security Server Updates über den Trend Micro ActiveUpdate Server. Legen Sie eine andere benutzerdefinierte Update-Adresse fest, wenn der Security Server den ActiveUpdate Server nicht direkt erreichen kann.

- Wenn der **Trend Micro ActiveUpdate Server** die Adresse ist, stellen Sie sicher, dass der Security Server eine Verbindung zum Internet hat. Wenn Sie einen Proxy-Server benutzen, überprüfen Sie, ob eine Internetverbindung mit den Proxy-Einstellungen hergestellt werden kann. Weitere Informationen finden Sie unter *Internet-Proxy-Einstellungen konfigurieren auf Seite 11-3*.
- Falls die Adresse eine benutzerdefinierte Update-Adresse ist (**Intranet-Site, die eine Kopie der aktuellen Datei enthält** oder **Alternative Update-Adresse**), konfigurieren Sie die entsprechende Umgebung und die Update-Ressourcen diese Update-Adresse. Stellen Sie auch sicher, dass der Security Server mit dieser Update-Adresse verbunden ist. Sollten Sie beim Einrichten einer Update-Adresse Hilfe benötigen, wenden Sie sich an Ihren Support-Anbieter.
- Ein reiner IPv6-Security Server kann Updates nicht direkt vom Trend Micro ActiveUpdate Server oder einer reinen, benutzerdefinierten IPv4-

Update-Adresse herunterladen. Ebenso kann ein reiner IPv4 Security Server keine Updates direkt von reinen benutzerdefinierten IPv6-Adressen erhalten. Ein Dual-Stack-Proxy-Server, der IP-Adressen wie DeleGate konvertieren kann, muss ermöglichen, dass der Security Server eine Verbindung zu den Update-Adressen herstellen kann.

Prozedur

1. Navigieren Sie zu **Updates** > **Adresse**.
2. Wählen Sie auf der Registerkarte **Server** eine Update-Adresse aus.
   - **Trend Micro ActiveUpdate Server**
   - **Intranet-Site, die eine Kopie der aktuellen Datei enthält**: Geben Sie den UNC-Pfad (Universal Naming Convention) zur Adresse ein, z. B. `\\Web\ActiveUpdate`. Geben Sie zudem die Anmeldedaten an (Benutzername und Kennwort), die der Security Server verwenden wird, um sich mit dieser Adresse zu verbinden.
   - **Alternative Update-Adresse**: Geben Sie die URL der Adresse ein. Stellen Sie sicher, dass das virtuelle HTTP-Verzeichnis (Webfreigabe) dem Security Server zur Verfügung steht.
3. Klicken Sie auf **Speichern**.

Den Security Server manuell aktualisieren

Aktualisieren Sie die Komponenten des Security Servers nach der Installation oder einem Upgrade des Servers sowie bei einem Ausbruch manuell.

Prozedur

1. Sie haben zwei Möglichkeiten, um ein manuelles Update zu starten:
   - Gehen Sie zu **Updates** > **Manuell**.

- Gehen Sie zu **Live-Status** und klicken Sie im Agent-Status-Widget auf **Komponentenstatus überprüfen**.

Das Fenster **Manuelles Update** wird angezeigt.

2. Wählen Sie die zu aktualisierenden Komponenten aus.

   Weitere Informationen zu Komponenten finden Sie unter *Update-Komponenten auf Seite 8-4*.

3. Klicken Sie auf **Jetzt aktualisieren**.

   Ein neues Fenster mit dem Update-Status wird angezeigt. Nach einem erfolgreichen Update verteilt der Security Server die aktualisierten Komponenten automatisch an die Agents.

Zeitgesteuerte Updates für den Security Server konfigurieren

Konfigurieren Sie den Security Server für die regelmäßige Überprüfung der Update-Adresse und für den automatischen Download verfügbarer Updates. Durch das zeitgesteuerte Update können Sie einfach und wirksam sicherstellen, dass Ihr Schutz vor Bedrohungen immer auf dem neuesten Stand ist.

Bei einem Viren-/Malware-Ausbruch stellt Trend Micro sofort aktuelle Pattern-Dateien zur Verfügung (Updates gibt es möglicherweise mehrmals pro Woche). Die Scan Engine und andere Komponenten werden ebenfalls regelmäßig aktualisiert. Trend Micro empfiehlt, die Komponenten täglich – und bei einem Viren-/Malware-Angriff häufiger – zu aktualisieren, damit dem Agent stets die aktuellen Komponenten zur Verfügung stehen.

Wichtig

Vermeiden Sie, dass eine zeitgesteuerte Suche und ein Update gleichzeitig ausgeführt werden. Die zeitgesteuerte Suche könnte unerwartet beendet werden.

Prozedur

1. Navigieren Sie zu **Updates** > **Zeitgesteuert**.
2. Wählen Sie die zu aktualisierenden Komponenten aus.

   Weitere Informationen zu Komponenten finden Sie unter *Update-Komponenten auf Seite 8-4*.
3. Klicken Sie auf die Registerkarte **Zeitplan**, und legen Sie den Zeitplan für die Updates fest.
   - **Updates der herkömmlichen Suche** umfassen alle Komponenten außer das Smart-Scan-Pattern und das Agent-Pattern von Smart Scan. Wählen Sie zwischen täglichen, wöchentlichen und monatlichen Updates und geben Sie unter **Update im Zeitraum von** das Zeitintervall an, in dem das Update durchgeführt werden soll. Der Security Server führt das Update zu einem beliebigen Zeitpunkt innerhalb dieses Zeitraums aus.

     Hinweis

     Wenn Sie bei monatlichen Updates (nicht empfohlen) 31, 30 oder 29 Tage wählen und ein Monat weniger Tage hat, wird in diesem Monat kein Update durchgeführt.
   - **Smart-Scan-Updates** betreffen nur das Smart-Scan-Pattern und das Agent-Pattern von Smart Scan. Wenn kein Agent Smart Scans durchführt, können Sie diesen Punkt ignorieren.
4. Klicken Sie auf **Speichern**.

Rollback für Komponenten durchführen

Ein Rollback ist eine Rückabwicklung zur vorherigen Version des Viren-Patterns, des Agent-Pattern von Smart Scan und der Viren-Scan-Engine. Wenn diese Komponenten nicht ordnungsgemäß funktionieren, sollten Sie ein Rollback auf die vorherige Version durchführen. Der Security Server behält die aktuelle und die vorherige Version der Viren-Scan-Engine sowie

die letzten drei Versionen des Viren-Patterns und des Agent-Pattern von Smart Scan bei.

Hinweis

Es kann nur für die oben genannten Komponenten ein Rollback durchgeführt werden.

Worry-Free Business Security verwendet unterschiedliche Scan Engines für Agents auf 32-Bit- und 64-Bit-Plattformen. Für diese Scan-Engines müssen separate Rollbacks durchgeführt werden. Das Rollback wird bei allen Versionen der Scan-Engine auf dieselbe Weise durchgeführt.

Prozedur

1. Navigieren Sie zu **Updates** > **Rollback**.
2. Klicken Sie für eine spezifische Komponente auf **Synchronisieren**, um Agents aufzufordern, ihre Komponenten mit der Version auf dem Server zu synchronisieren.
3. Klicken Sie für eine spezifische Komponente auf **Rollback**, um für diese Komponente sowohl auf dem Security Server als auch in den Agents ein Rollback durchzuführen.

Updates für Security Agent und Messaging Security Agent

Automatische Updates

Security Agents und Messaging Security Agents (nur Advanced) führen automatisch folgende Updates durch:

- Direkt nach der Installation werden die Agents über den Security Server aktualisiert.

- Wenn der Security Server ein Update abschließt, werden die Updates automatisch auf die Agents übertragen.
- Wenn der Update-Agent ein Update abschließt, werden die Updates automatisch auf die jeweiligen Security Agents übertragen.
- Standardmäßig werden zeitgesteuerte Updates wie folgt durchgeführt:
  - Alle 8 Stunden für Security Agents im Büro
  - Alle 2 Stunden für Security Agents, die sich nicht im Büro befinden.
- Messaging Security Agents führen standardmäßig im Abstand von 24 Stunden jeweils um 0.00 Uhr ein zeitgesteuertes Update durch.

Manuelles Update ausführen

Der Security Agent empfängt Updates automatisch vom Security Server.

Wenn Sie zeitweise vom Büronetzwerk getrennt sind oder dringend den neuesten Schutz vor Sicherheitsbedrohungen benötigen (z. B. nach einem Ausbruch), können Sie manuell aktualisieren.

Wenn die Verbindung zum Internet über einen Proxy-Server hergestellt wird, stellen Sie sicher, dass Sie die korrekten Proxy-Einstellungen verwenden.

Prozedur

1. Öffnen Sie die Hauptkonsole und klicken Sie auf **Aktualisieren**.

   Hinweis

   Sie können auch ein manuelles Aktualisieren ausführen, indem Sie in der Windows Task-Leiste mit der rechten Maustaste auf das Symbol Security Agent klicken und anschließend **Jetzt aktualisieren** auswählen.

2. Klicken Sie auf **Schließen**, wenn der Update-Vorgang abgeschlossen wurde.

Hinweise und Empfehlungen zu Agent-Updates

- Security Agents werden über den Security Server, Update-Agents oder den Trend Micro ActiveUpdate Server aktualisiert.

  Messaging Security Agents werden nur über den Security Server aktualisiert.

  Informationen zum Update-Vorgang finden Sie unter *Update-Übersicht auf Seite 8-2*.

- Ein reiner IPv6-Agent kann keine direkten Updates von einem reinen IPv4 Security Server/Update-Agent und vom Trend Micro ActiveUpdate Server erhalten.

  Ein reiner IPv4-Agent kann wiederum keine direkten Updates von einem reinen IPv6 Security Server/Update-Agent erhalten.

  In diesen Situationen ist ein Dual-Stack-Proxy-Server erforderlich, der IP-Adressen konvertieren kann, wie DeleGate, damit der Agent Updates erhalten kann.

- Informationen zu den Komponenten, die Agents aktualisieren, finden Sie unter *Update-Komponenten auf Seite 8-4*.

- Neben den Komponenten erhalten Agents außerdem aktualisierte Konfigurationsdateien, wenn sie über den Security Server aktualisiert werden. Agents benötigen diese Konfigurationsdateien, um neue Einstellungen zu übernehmen. Bei jeder Änderung der Agent-Einstellungen über die Webkonsole ändern sich auch die Konfigurationsdateien.

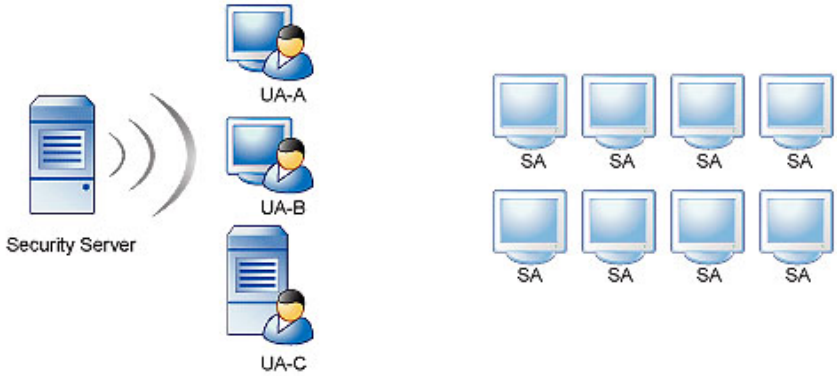
Update Agents

Update Agents sind Security Agents, die aktualisierte Komponenten vom Security Server oder ActiveUpdate Server erhalten und an andere verteilen können.

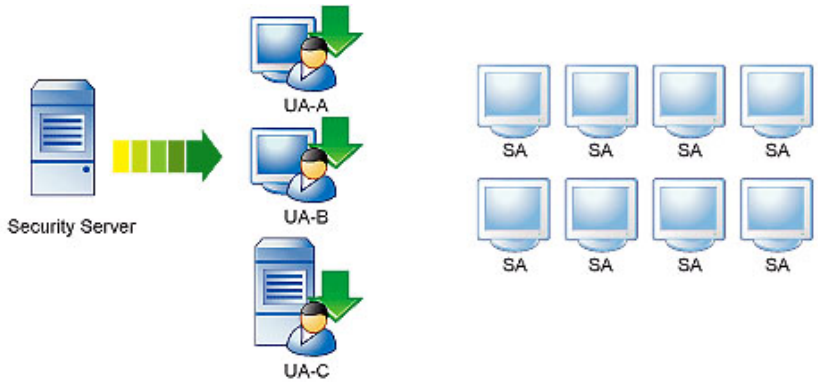
Wenn in Ihrem Netzwerk zwischen den Clients und dem Trend Micro Security Server Bereiche mit geringer Bandbreite oder einem hohen Datenaufkommen vorhanden sind, können Sie Security Agents als Update Agents festlegen. Update Agents reduzieren die Netzwerkbandbreitenauslastung, da für Komponenten-Updates nicht mehr alle Security Agents auf den Security Server zugreifen müssen. Wenn Ihr Netzwerk beispielsweise nach Standorten segmentiert ist und das Datenaufkommen über die Netzwerkverbindung häufig besonders hoch ist, sollten Sie mindestens einen Security Agent pro Segment als Update-Agent einrichten.

Der Aktualisierungsvorgang des Update-Agents kann wie folgt beschrieben werden:

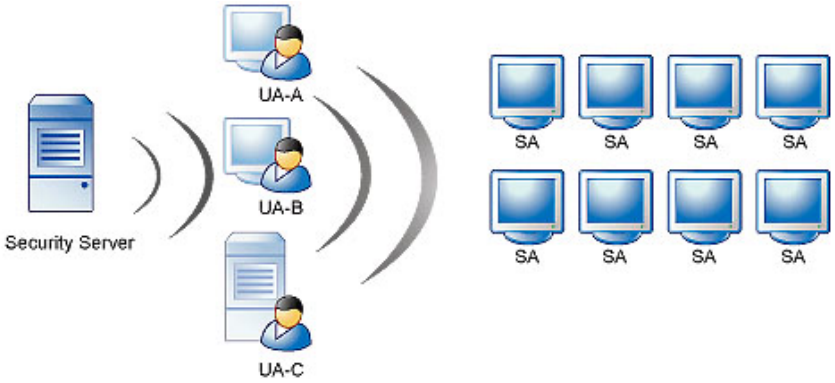
1. Der Security Server informiert die Update-Agents über neue verfügbare Updates.



2. Die Update Agents laden die aktualisierten Komponenten vom Security Server herunter.

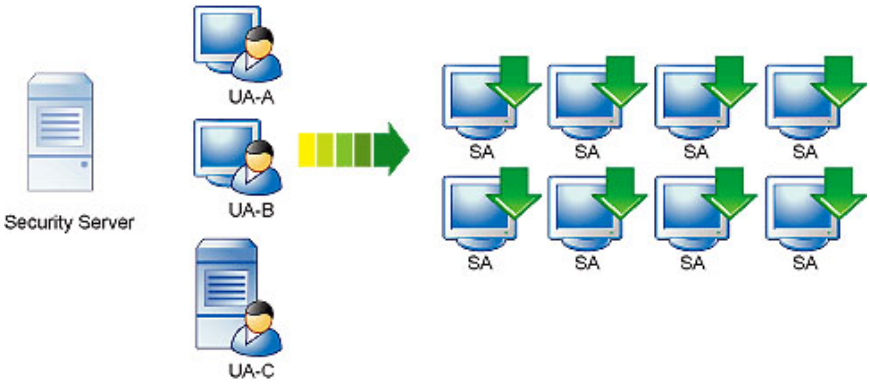


3. Anschließend informiert der Security Server die Security Agents, dass aktualisierte Komponenten verfügbar sind.



4. Jeder Security Agent lädt eine Kopie der Reihenfolgentabelle der Update-Agents herunter, um die geeignete Update-Adresse zu bestimmen. Die Reihenfolge der Update-Agents in der Reihenfolgentabelle der Update-Agents wird zunächst durch die Reihenfolge bestimmt, in der sie auf der Webkonsole als alternative Update-Adressen hinzugefügt wurden. Jeder Security Agent durchsucht die Tabelle beginnend beim ersten Eintrag Schritt für Schritt, bis die Update-Adresse gefunden wird.

5. Die Security Agents laden dann die aktualisierten Komponenten von dem zugewiesenen Update-Agent herunter. Falls der zugewiesene Update-Agent aus bestimmten Gründen nicht verfügbar ist, versucht der Security Agent, die aktualisierten Komponenten vom Security Server herunterzuladen.



Update Agents konfigurieren

Prozedur

1. Navigieren Sie zu **Updates** > **Adresse**.
2. Klicken Sie auf die Registerkarte **Update-Agents**.
3. Führen Sie folgende Aufgaben durch:

Task	Schritte
Security Agents als Update Agents zuweisen	a. Klicken Sie im Bereich **Update-Agent(s) zuweisen** auf **Hinzufügen**. Es öffnet sich ein neues Fenster. b. Wählen Sie aus dem Listenfeld einen oder mehrere Agents als Update Agent aus. c. Klicken Sie auf **Speichern**. Das Fenster wird geschlossen. d. Wählen Sie zurück im Bereich **Update-Agent(s) zuweisen** **Update-Agents immer direkt über Security Server aktualisieren** aus, wenn Sie möchten, dass die Update-Agents aktualisierte Komponenten immer vom Security Server herunterladen statt von einem anderen Update-Agent.
Security Agents für die Aktualisierung über Update Agents konfigurieren	a. Wählen Sie im Bereich **Alternative Update-Adressen** **Alternative Update-Adressen für Security Agents und Update Agents aktivieren** aus. **Hinweis** Wenn diese Option deaktiviert ist, können die Security Agents nicht über die Update Agents aktualisieren, so dass die Update-Adresse wieder auf den Security Server eingestellt wird. b. Klicken Sie auf **Hinzufügen**. Es öffnet sich ein neues Fenster. c. Geben Sie die IP-Adresse der Security Agents ein, die über einen Update-Agent aktualisieren. • Geben Sie einen IPv4-Adressbereich ein. Um einen einzelnen Security Agent anzugeben, geben Sie jeweils die IP-Adresse des Security Agents in die Felder **von** und **bis** ein. • Geben Sie ein IP-Präfix und eine Länge für IPv6 ein. d. Wählen Sie einen Update-Agent aus dem Listenfeld aus.

Task	Schritte
	Ist ein Zugriff auf das Listenfeld nicht möglich, wurden keine Update Agents konfiguriert. e. Klicken Sie auf **Speichern**. Das Fenster wird geschlossen. f. Legen Sie mehr IP-Bereiche fest, als erforderlich. Wenn Sie mehrere IP-Bereiche angegeben haben, können Sie die Option **Neu ordnen** verwenden, um die Priorität des IP-Bereichs festzulegen. Wenn der Security Server die Security Agents über verfügbare Updates informiert, suchen diese in der IP-Bereichsliste nach der richtigen Update-Adresse. Der Security Agent durchsucht den ersten Eintrag in der Liste und arbeitet die Liste dann nach unten ab, bis er die richtige Update-Adresse findet. **Tipp** Legen Sie als Ausfallsicherung mehrere Update Agents für den gleichen IP-Bereich fest. Können Security Agents nicht über einen Update-Agent aktualisiert werden, versuchen Sie es über andere Update-Agents. Erstellen Sie hierfür mindestens (2) Einträge mit identischem IP-Bereich und weisen Sie jedem Eintrag einen anderen Update-Agent zu.
Update Agents entfernen	Wenn Sie einen Update-Agent und alle zugewiesenen Security Agents entfernen möchten, navigieren Sie zum Bereich **Update-Agent(s) zuweisen** und aktivieren Sie das entsprechende Kontrollkästchen mit dem Computernamen des Update-Agents und klicken Sie auf **Entfernen**. Dadurch wechseln die 'verwaisten' Security Agents nur ihre Update-Adresse zurück zum Security Server und die IP-Adresse des Security Agents wird nicht aus dem Bereich **Alternative Update-Adressen** entfernt. Wenn Sie einen anderen Update-Agent besitzen, können Sie diesen den verwaisten Security Agents zuweisen.
Zuweisung der Security Agents zu Update Agents entfernen	Wenn Sie nicht mehr möchten, dass Security Agents eines IP-Adressenbereichs von einem Update-Agent aktualisieren, navigieren Sie zum Bereich **Alternative Update-Adressen** und

Task	Schritte
	aktivieren Sie das entsprechende Kontrollkästchen mit dem IP-Adressenbereich des Security Agents und klicken Sie auf **Entfernen**.

4. Klicken Sie auf **Speichern**.

Kapitel 9

Live-Status verwenden

Live-Status

Worry-Free Business Security bietet Widgets, die als schnelle visuelle Referenzen zur Verwaltung des Security Agents dienen.

Das Fenster **Live-Status** wird angezeigt, wenn Sie die Worry-Free Business Security-Webkonsole öffnen oder im Hauptmenü auf **Live-Status** klicken.

TABELLE 9-1. Live-Status-Widgets

WIDGET	BESCHREIBUNG
Aktionszentrum	Dieses Widget zeigt die Ereignisse an, bei denen Administratoren Maßnahmen zur Problembehebung ergreifen müssen.
Erkennung von Sicherheitsrisiken im Zeitverlauf	Dieses Widget enthält einen Überblick über die Endpunkte im Netzwerk mit entdeckten Bedrohungen und die Bedrohungstypen, von denen Ihr Netzwerk in einem bestimmten Zeitraum betroffen war.
Ransomware-Übersicht	Dieses Widget enthält einen Überblick über alle versuchten Ransomware-Angriffe für einen bestimmten Zeitraum.
Lizenzstatus	Dieses Widget enthält einen Überblick über die Anzahl der genutzten Lizenzen und den Ablaufstatus Ihrer Lizenz.
Übersicht zu Exchange Server	Dieses Widget stellt eine Übersicht zum Verbindungsstatus der Messaging Security Agents und eine Verteilung der Erkennung von Bedrohungen auf Ihren Exchange Servern bereit.
Agent-Status	Dieses Widget enthält einen Überblick über die Verbindung und den Update-Status der Security Agents in Ihrem Netzwerk.

Die im Fenster **Live-Status** angezeigten Informationen werden in verschiedenen Intervallen aktualisiert. Die Aktualisierungsrate liegt im Allgemeinen zwischen 1 und 10 Minuten. Um die angezeigten Informationen manuell zu aktualisieren, klicken Sie in Ihrem Browser auf die Schaltfläche zum **Aktualisieren**.

Aktionszentrum

Dieses Widget zeigt die Ereignisse an, bei denen Administratoren Maßnahmen zur Problembehebung ergreifen müssen.

Einige Ereignisse enthalten empfohlene Aktionsschaltflächen. Klicken Sie auf die entsprechende Schaltfläche, um die Probleme zu lösen, oder klicken Sie auf die Ereignisse, um weitere Einzelheiten anzuzeigen.

TABELLE 9-2. Ereignisse des Aktionszentrums

EREIGNIS	EMPFEHLUNG
Virenschutz – Nicht behobene Bedrohungen	Führen Sie eine Suche mit dem Trend Micro HouseCall Tool durch.
Virenschutz: Echtzeitsuche auf Endpunkten deaktiviert	Aktivieren Sie Echtzeitsuche auf allen Geräten, um geschützt zu bleiben.
Virenschutz: Echtzeitsuche auf Exchange Server(n) deaktiviert	Aktivieren Sie Echtzeitsuche auf allen Exchange Servern, damit Ihr Computer geschützt bleibt.
Anti-Spyware: Funde machen Geräteneustart erforderlich	Starten Sie zur vollständigen Entfernung erkannter Bedrohungen die Geräte neu.
Lizenzereignisse	Navigieren Sie zu **Administration** > **Produktlizenz**, um den Status der Produktlizenz zu überprüfen.
Mangel an Ressourcen: verbleibender Speicherplatz unter %threshold%	Führen Sie das Disk Cleaner Tool aus, um nicht verwendete Sicherungs-, Protokoll- und Pattern-Dateien zu löschen. Weitere Informationen finden Sie unter *Festplattenspeicher sparen auf Seite 14-15*.
Smart Protection Services: Dienst nicht verfügbar	Überprüfen Sie den Smart Scan Server-Status in der Konsole Worry-Free Business Security und stellen Sie sicher, dass der Server ordnungsgemäß funktioniert.
Update: mindestens ein nicht aktueller Messaging Security Agent nach einer Stunde der Pattern-Veröffentlichung	Stellen Sie sicher, dass zeitgesteuerte Updates für die Messaging Security Agents auf dem Security Server aktiviert sind und die Messaging Security Agents eine Verbindung mit dem Internet herstellen können.

Ereignis	Empfehlung
Update: Verteilungsrate weniger als %threshold% nach einer Stunde der Pattern-Veröffentlichung	Prüfen Sie die Internetverbindung des Security Agent, und aktualisieren Sie die Security Agents erneut.
Update: Komponenten des Security Servers nicht aktualisiert seit mehr als %threshold% Tagen	Stellen Sie sicher, dass zeitgesteuerte Updates für die Komponenten auf dem Security Server aktiviert sind und dass der Security Server eine Verbindung mit dem Internet herstellen kann.
Update: Smart-Scan-Pattern nicht aktualisiert seit mehr als %threshold% Stunden	Stellen Sie sicher, dass zeitgesteuerte Updates für das Smart-Scan-Pattern auf dem Security Server aktiviert sind und dass der Security Server eine Verbindung mit dem Internet herstellen kann.

Virenschutz: nicht behobene Bedrohungen

Sie können diese Informationen anzeigen, indem Sie im Aktionszentrum auf das Ereignis **Virenschutz – nicht behobene Bedrohungen: %N%** klicken. Worry-Free Business Security erstellt oder aktualisiert diese Protokollinformationen bei jeder Echtzeit-, manuellen oder zeitgesteuerten Suche.

- Klicken Sie auf **Download-Tool**, um das Trend Micro HouseCall-Tool herunterzuladen und damit eine Suche auf dem betroffenen Gerät auszuführen.
- Klicken Sie auf **Über Aktionszentrum schließen**, um zum Bildschirm **Live-Status** zu gelangen und das Benachrichtigungsereignis aus dem Aktionszentrum zu entfernen. Protokolle, die mit diesen Ereignissen in Zusammenhang stehen, sind über die Protokollabfrage nach wie vor verfügbar.
- Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit des letzten fehlgeschlagenen Versuchs, Virus oder Malware zu säubern oder zu entfernen.
Gerätename	Name des betroffenen Gerätes
Viren-/Malware-Name	Name des entdeckten Virus oder der entdeckten Malware Klicken Sie auf diesen Link, um zur Trend Micro Bedrohungsenzyklopädie zu gelangen, die eine ausführliche Beschreibung der Bedrohung sowie Hinweise zum manuellen Säubern enthält.
Dateiname	Name der vom Virus oder von Malware betroffenen Datei
Pfad	Speicherort der infizierten Datei
Suchtyp	Der zum Entdecken vom Virus oder von Malware verwendete Suchtyp
Durchgeführte Aktion	Aktion, mit der Worry-Free Business Security auf die Erkennung von Viren oder Malware reagiert.

Virenschutz: Echtzeitsuche auf Endpunkten deaktiviert

Sie können diese Informationen anzeigen, indem Sie im Aktionszentrum auf das Ereignis **Virenschutz: Echtzeitsuche auf Endpunkten deaktiviert: %N %** klicken.

- Klicken Sie auf **Echtzeitsuche aktivieren**, um die Suche auf allen Geräten zu aktivieren.
- Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Gerätename	Name des Geräts mit deaktivierter Echtzeitsuche
Gruppenname	Name der Gruppe, zu der das Gerät gehört

Virenschutz: Echtzeitsuche auf Exchange Server(n) deaktiviert

Sie können diese Informationen anzeigen, indem Sie im Aktionszentrum auf das Ereignis **Virenschutz: Echtzeitsuche auf Exchange Server(n) deaktiviert: %N %** klicken.

- Klicken Sie auf **Echtzeitsuche aktivieren**, um die Suche auf allen Exchange Servern zu aktivieren.
- Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Exchange Server-Name	Name des Exchange Servers mit deaktivierter Echtzeitsuche

Anti-Spyware: Erkennungen, die einen Geräteneustart erforderlich machen

Sie können diese Protokollinformationen anzeigen, indem Sie im Aktionszentrum auf das Ereignis **Anti-Spyware: Funde machen Geräteneustart erforderlich: %N%** klicken.

- Klicken Sie auf **Über Aktionszentrum schließen**, um zum Bildschirm **Live-Status** zu gelangen und das Benachrichtigungsereignis aus dem Aktionszentrum zu entfernen. Protokolle, die mit diesen Ereignissen in Zusammenhang stehen, sind über die Protokollabfrage nach wie vor verfügbar.
- Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, an dem bzw. zu der der Security Agent Informationen zur Erkennung von Spyware oder Grayware an Worry-Free Business Security gemeldet hat.
Gerätename	Name des betroffenen Gerätes

Spalte	Beschreibung
Spyware-/Grayware-Name	Name der entdeckten Spyware oder Grayware Klicken Sie auf diesen Link, um zur Trend Micro Bedrohungsenzyklopädie zu gelangen, die eine ausführliche Beschreibung der Bedrohung sowie Hinweise zum manuellen Säubern enthält.
Suchtyp	Der zum Entdecken der Spyware oder Grayware verwendete Suchtyp

Mangel an Ressourcen: verbleibender Speicherplatz

Sie können diese Informationen anzeigen, indem Sie auf das Ereignis **Mangel an Ressourcen: verbleibender Speicherplatz unter %threshold%** im Aktionszentrum klicken.

Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Servername	Name des Servers mit wenig Speicherplatz
Gruppenname	Name der Gruppe, zu der der Server gehört

Update: nicht aktuelle Agents

Sie können diese Informationen anzeigen, indem Sie auf das Ereignis **Update-Verteilungsrate weniger als %threshold% nach einer Stunde der Pattern-Veröffentlichung** im Aktionszentrum klicken. Für die in diesem Fenster aufgeführten Security Agents sind Engine- oder Pattern-Updates erforderlich.

- Klicken Sie auf **Jetzt aktualisieren**, um eine Benachrichtigung zum Update auf die neuesten Komponenten an die nicht aktuellen Security Agents zu übermitteln.

- Klicken Sie auf **Komponentenstatus überprüfen**, um das Fenster **Manuelles Update** zu öffnen.
- Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Gerätename	Name des Geräts, für das Komponenten-Updates erforderlich sind
Gruppenname	Name der Gruppe, zu der das Gerät gehört
Suchmethode	• Smart Scan • Herkömmliche Suche

Update: nicht aktuelle Messaging Security Agents

Sie können diese Informationen anzeigen, indem Sie im Aktionszentrum auf das Ereignis **Update: mindestens ein nicht aktueller Messaging Security Agent nach einer Stunde der Pattern-Veröffentlichung** klicken.

- Klicken Sie auf **Jetzt aktualisieren**, um eine Benachrichtigung zum Update auf die neuesten Komponenten an die nicht aktuellen Messaging Security Agents zu übermitteln.
- Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Exchange Server-Name	Name des Exchange Servers, für den Komponenten-Updates erforderlich sind

Erkennung von Sicherheitsrisiken im Zeitverlauf

Dieses Widget enthält einen Überblick über die Endpunkte im Netzwerk mit entdeckten Bedrohungen und die Bedrohungstypen, von denen Ihr Netzwerk in einem bestimmten Zeitraum betroffen war.

- Klicken Sie auf oder , um zwischen verschiedenen Ansichten zu wechseln.
- Klicken Sie auf die Registerkarte **Bekannte Bedrohungen**, **Unbekannte Bedrohungen** oder **Richtlinienverstöße**, um die Erkennungsinformationen für die jeweiligen Bedrohungen anzuzeigen.

Anzeigen	Beschreibung
Diagramm ( )	• Klicken Sie unten im Diagramm auf die Namen der Bedrohungstypen, um Erkennungsinformationen im Diagramm ein-/auszublenden. • Zeigen Sie mit der Maus auf die Knoten für einen Tag, um die Gesamtzahl der Funde für die angezeigten Bedrohungstypen anzuzeigen. Klicken Sie auf einen Knoten, um zum Protokollbildschirm für den in der Liste markierten Bedrohungstyp zu gelangen.
Tabelle ( )	• Klicken Sie auf die Anzahl der Funde, um das Protokollfenster mit den Erkennungsdetails zu öffnen.

Erkennung von Sicherheitsrisiken: Virus/Malware

Sie können diese Informationen anzeigen, indem Sie auf einen der folgenden Links auf der Registerkarte **Bekannte Bedrohungen** im Widget **Erkennung von Sicherheitsrisiken im Zeitverlauf** klicken:

- Die Anzahl der Funde von **Virus/Malware** in der Tabellenansicht
- Beliebiger Knoten **Virus/Malware** in der Diagrammansicht

Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, an dem/zu der der Security Agent Informationen zu Funden von Viren oder Malware an Worry-Free Business Security gemeldet hat

Spalte	Beschreibung
Gerätename	Name des betroffenen Gerätes
Viren-/Malware-Name	Name des entdeckten Virus oder der entdeckten Malware Klicken Sie auf diesen Link, um zur Trend Micro Bedrohungsenzyklopädie zu gelangen, die eine ausführliche Beschreibung der Bedrohung sowie Hinweise zum manuellen Säubern enthält.
Dateiname	Name der vom Virus oder von Malware betroffenen Datei
Pfad	Speicherort der infizierten Datei
Suchtyp	Der zum Entdecken vom Virus oder von Malware verwendete Suchtyp
Durchgeführte Aktion	Aktion, mit der Worry-Free Business Security auf die Erkennung von Viren oder Malware reagiert.

Erkennung von Sicherheitsrisiken: Spyware/Grayware

Sie können diese Informationen anzeigen, indem Sie auf einen der folgenden Links auf der Registerkarte **Bekannte Bedrohungen** im Widget **Erkennung von Sicherheitsrisiken im Zeitverlauf** klicken:

- Die Anzahl der Funde von **Spyware/Grayware** in der Tabellenansicht
- Beliebiger Knoten **Spyware/Grayware** in der Diagrammansicht

Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, an dem bzw. zu der der Security Agent Informationen zur Erkennung von Spyware oder Grayware an Worry-Free Business Security gemeldet hat.

Spalte	Beschreibung
Gerätename	Name des betroffenen Gerätes Klicken Sie auf den Namen, um eine Liste einzelner Spyware- oder Grayware-Software anzuzeigen, die auf diesem Gerät erkannt wurde.
Spyware-/Grayware-Name	Name der entdeckten Spyware oder Grayware
Suchtyp	Der zum Entdecken der Spyware oder Grayware verwendete Suchtyp
Durchgeführte Aktion	Aktion, mit der Worry-Free Business Security auf die Erkennung von Spyware oder Grayware reagiert.

Erkennung von Sicherheitsrisiken: Web Reputation

Sie können diese Informationen anzeigen, indem Sie auf einen der folgenden Links auf der Registerkarte **Bekannte Bedrohungen** im Widget **Erkennung von Sicherheitsrisiken im Zeitverlauf** klicken:

- Die Anzahl der Funde von **Web Reputation** in der Tabellenansicht
- Beliebiger Knoten **Web Reputation** in der Diagrammansicht

Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, an dem bzw. zu der der Security Agent Informationen zum URL-Verstoß an Worry-Free Business Security gemeldet hat.
Gerätename	Name des Gerätes, das versucht, auf eine unzulässige URL zuzugreifen
URL	Unzulässige URL
Risikostufe	Eine von TrendLabs ermittelte Bewertung des Risikos einer Infektion und möglicher Schäden.

Erkennung von Sicherheitsrisiken: Netzwerkvirus

Sie können diese Informationen anzeigen, indem Sie auf einen der folgenden Links auf der Registerkarte **Bekannte Bedrohungen** im Widget **Erkennung von Sicherheitsrisiken im Zeitverlauf** klicken:

- Die Anzahl der Funde von **Netzwerkvirus** in der Tabellenansicht
- Beliebiger Knoten **Netzwerkvirus** in der Diagrammansicht

Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, an dem/zu der der Security Agent Daten zu Netzwerkvirenfunden an Worry-Free Business Security gemeldet hat
Gerätename	Name des betroffenen Gerätes
Angriffs-IP	IP-Adresse des Angreifers
Opfer-IP	IP-Adresse des Opfers
Paketrichtung	Richtung des Pakets
Name des Netzwerkvirus	Name des entdeckten Netzwerkvirus
Anzahl	Jeder Netzwerkvirus wird jedes Mal gezählt, wenn er erkannt wird.

Erkennung von Sicherheitsrisiken: Verhaltensüberwachung

Sie können diese Informationen anzeigen, indem Sie auf einen der folgenden Links auf der Registerkarte **Unbekannte Bedrohungen** im Widget **Erkennung von Sicherheitsrisiken im Zeitverlauf** klicken:

- Die Anzahl der Funde von **Verhaltensüberwachung** in der Tabellenansicht
- Beliebiger Knoten **Verhaltensüberwachung** in der Diagrammansicht

Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, an dem bzw. zu der der Security Agent Informationen zum Verstoß gegen die Verhaltensüberwachung an Worry-Free Business Security gemeldet hat.
Gerätename	Name des Gerätes, das einen Richtlinienverstoß ausgelöst hat
Sicherheitsbedrohung	Typ der Sicherheitsbedrohung
Betreff	Betreff des Vorgangs
Ereignistyp	Zugehöriges Systemereignis
Ziel	Ziel des Vorgangs
Aktion	Vom Benutzer ausgeführte Aktion, die den Verstoß ausgelöst hat
Ergebnis	Aktion, mit der Worry-Free Business Security auf Verstöße gegen die Verhaltensüberwachung reagiert.

Erkennung von Sicherheitsrisiken: Vorausschauendes Maschinenlernen

Sie können diese Informationen anzeigen, indem Sie auf einen der folgenden Links auf der Registerkarte **Unbekannte Bedrohungen** im Widget **Erkennung von Sicherheitsrisiken im Zeitverlauf** klicken:

- Die Anzahl der Funde von **Vorausschauendes Maschinenlernen** in der Tabellenansicht
- Beliebiger Knoten **Vorausschauendes Maschinenlernen** in der Diagrammansicht

Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
⊞ / ⊟	Klicken Sie auf das Symbol, um die Protokolldetails unterhalb der Tabellenzeile zu erweitern oder zu schließen.
Datum/Uhrzeit	Datum und Uhrzeit, an dem/zu der der Security Agent Informationen zu Funden an Worry-Free Business Security gemeldet hat
Gerätename	Name des betroffenen Gerätes
Gruppenname	Name der Gruppe, zu der das Gerät gehört
Unbekannte Bedrohung	Name der möglichen Bedrohung
Bedrohungsprobabilität	Gibt an, wie genau die Datei/der Prozess mit dem Malware-Modell übereinstimmt
Dateiname	Name des Dateiobjekts oder des Programms, das den Prozess ausführt **Wichtig** Der erkannte Dateiname für diesen Fund stimmt möglicherweise nicht mit dem Dateinamen überein, der auf anderen Endpunkten erkannt wurde. Vorausschauendes Maschinenlernen assoziiert Funde nach Datei-Hashwerten, nicht nach bestimmten Dateinamen.
Pfad	Pfad des Dateiobjekts oder Pfad des Programms, das den Prozess ausführt
Infektionskanal	Kanal, aus dem die Bedrohung stammt
Durchgeführte Aktion	Von Worry-Free Business Security durchgeführte Aktion als Reaktion auf die Erkennung

Erkennung von Sicherheitsrisiken: Details zu Vorausschauendes Maschinenlernen

Sie können diese Informationen anzeigen, indem Sie auf alle

-Symbole in der ersten Spalte des Protokollfensters **Erkennung von Sicherheitsrisiken: Details zu Vorausschauendes Maschinenlernen** klicken.

Der Abschnitt mit den Protokolldetails besteht aus zwei Registerkarten:

- **Unbekannte Bedrohung**: stellt die Ergebnisse der Analyse von Vorausschauendes Maschinenlernen bereit
- **Dateiname**: stellt allgemeine Details im Zusammenhang mit Dateieigenschaften und Zertifikatsinformationen für dieses bestimmte Erkennungsprotokoll bereit

> **Tipp**
>
> Klicken Sie auf **Zur Ausnahmeliste hinzufügen**, um den Datei-Hashwert der betroffenen Datei schnell zur globalen Ausnahmeliste für Vorausschauendes Maschinenlernen hinzuzufügen. Zeigen Sie die gesamte Ausnahmeliste im Fenster **Allgemeine Einstellungen** an.
>
> Weitere Informationen finden Sie unter *Einstellungen für die Ausnahmeliste konfigurieren auf Seite 11-14*.

In der folgenden Tabelle werden die auf der Registerkarte **Unbekannte Bedrohung** bereitgestellten Informationen dargestellt.

TABELLE 9-3. Details zur Registerkarte 'Unbekannte Bedrohung'

ELEMENT	BESCHREIBUNG
Bedrohungsprobabilität	Gibt an, wie genau die Datei/der Prozess mit dem Malware-Modell übereinstimmt

Element	Beschreibung
Wahrscheinliche Bedrohungsart	Gibt die wahrscheinlichste Art der Bedrohung an, die in der Datei enthalten ist, nachdem Vorausschauendes Maschinenlernen die Analyse mit anderen bekannten Bedrohungen verglichen hat
Bedrohungsidentifikation	Stellt eine Liste mit API-Funktionen bereit, die von der Datei/dem Prozess verwendet werden und die möglicherweise auf die erkannte Bedrohungsart hinweisen **Wichtig** Die API-Funktionsidentifikation ist nur ein Faktor bei der Bestimmung der Bedrohungsart. Vorausschauendes Maschinenlernen verwendet viele andere Dateifunktionen und Analysemethoden zum Berechnen der Bedrohungswahrscheinlichkeit und der wahrscheinlichen Bedrohungsart.
Erkennungstyp	Objekttyp, der die Erkennung ausgelöst hat ('Datum' oder 'Prozess')
Ähnliche bekannte Bedrohungen	Enthält eine Liste der bekannten Bedrohungsarten, die ähnliche Datei-/Prozessfunktionen für die Erkennung aufweisen

Erkennung von Sicherheitsrisiken: URL-Filter

Sie können diese Informationen anzeigen, indem Sie auf einen der folgenden Links auf der Registerkarte **Richtlinienverstöße** im Widget **Erkennung von Sicherheitsrisiken im Zeitverlauf** klicken:

- Anzahl der Funde von **URL-Filter** in der Tabellenansicht
- Beliebiger Knoten **URL-Filter** in der Diagrammansicht

Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, an dem bzw. zu der der Security Agent Informationen zum URL-Verstoß an Worry-Free Business Security gemeldet hat.
Gerätename	Name des Gerätes, das versucht, auf eine unzulässige URL zuzugreifen
URL	Unzulässige URL

Erkennung von Sicherheitsrisiken: Gerätesteuerung

Sie können diese Informationen anzeigen, indem Sie auf einen der folgenden Links auf der Registerkarte **Richtlinienverstöße** im Widget **Erkennung von Sicherheitsrisiken im Zeitverlauf** klicken:

- Die Anzahl der Funde von **Gerätesteuerung** in der Tabellenansicht
- Beliebiger Knoten **Gerätesteuerung** in der Diagrammansicht

Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, an dem/zu der der Security Agent die Daten der Verstöße gegen die Gerätesteuerung an Worry-Free Business Security gemeldet hat
Gerätename	Name des Gerätes, das einen Richtlinienverstoß ausgelöst hat
Typ	Art des Speichergeräts
Berechtigung	Berechtigung für das Speichergerät festgelegt
Betreff	Betreff des Vorgangs
Objekt	Objekt des Vorgangs
Aktion	Vorgang fertig

Ransomware-Übersicht

Dieses Widget enthält einen Überblick über alle versuchten Ransomware-Angriffe für einen bestimmten Zeitraum.

Die Standardansicht zeigt eine Übersicht über alle Ransomware-Funde und kategorisiert weiterhin die Versuche basierend auf dem Angriffskanal.

- Klicken Sie in der Standardansicht auf die Anzahl der Ransomware-Funde, um den Protokollbildschirm **Ransomware-Übersicht** zu gelangen, in dem die Ransomware-Funddetails aufgeführt sind.
- Verwenden Sie die Listenfelder, um zwischen verschiedenen Ansichten zu wechseln.

Klicken Sie auf , um die Erkennungsinformationen in einem Diagramm anzuzeigen.

- Zeigen Sie mit der Maus auf die Knoten für einen Tag, um die Gesamtzahl der Funde für die angezeigte Erkennungskategorie anzuzeigen. Klicken Sie auf einen Knoten, um zum Protokollbildschirm **Ransomware-Übersicht** zu gelangen, in dem die Ransomware-Funddetails für diesen Tag aufgeführt sind.

Protokolle zur Ransomware-Übersicht

Sie können diese Informationen anzeigen, indem Sie auf einen Knoten im Diagramm oder eine Erkennungsanzahl im Widget **Ransomware-Übersicht** klicken.

- Verwenden Sie die Listen **Infektionskanal** und **Zeitraum**, um die Ansicht anzupassen.
- Klicken Sie auf **Exportieren**, um die Protokollereignisse in einer CSV-Datei zu speichern.

Spalte	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, an dem bzw. zu der der Security Agent Informationen zur Erkennung von Ransomware an Worry-Free Business Security gemeldet hat.
Sicherheitsbedrohung	Art der Ransomware • Viren-/Malware-Name: zeigt den Erkennungsnamen einer bekannten Ransomware-Datei an • Nicht autorisierte Dateiverschlüsselung: zeigt an, wenn Worry-Free Business Security ein verdächtiges Programm entdeckt, das eine Datei verschlüsselt • <URL>: zeigt an, wenn Worry-Free Business Security eine URL im Zusammenhang mit einer bekannten Ransomware erkennt
Quelle	Typ der Suche, die die Bedrohung erkannt hat
Pfad/URL	• Dateipfad der Ransomware • Mit Ransomware infizierte ULR
Durchgeführte Aktion	Aktion, mit der Worry-Free Business Security auf die Erkennung von Ransomware reagiert.
Gerätename	Name des betroffenen Gerätes
Infektionskanal	Kanal der Ransomware-Erkennung
Details	Klicken Sie auf **Anzeigen**, um die Protokollinformationen anzuzeigen.

Ransomware: Details zu Verhaltensüberwachungsprotokollen

Sie können diese Informationen anzeigen, indem Sie auf dem Protokollbildschirm zur Ransomware-Übersicht in der Spalte **Details** auf den Link **Anzeigen** klicken.

Zeile	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, an dem bzw. zu der der Security Agent Informationen zum Verstoß gegen die Verhaltensüberwachung an Worry-Free Business Security gemeldet hat.
Gerätename	Name des Gerätes, das einen Richtlinienverstoß ausgelöst hat
Sicherheitsbedrohung	Typ der Sicherheitsbedrohung
Betreff	Betreff des Vorgangs
Ereignistyp	Zugehöriges Systemereignis
Ziel	Ziel des Vorgangs
Aktion	Vom Benutzer ausgeführte Aktion, die den Verstoß ausgelöst hat
Ergebnis	Aktion, mit der Worry-Free Business Security auf Verstöße gegen die Verhaltensüberwachung reagiert.

Ransomware: Details zum URL-Filterprotokoll

Sie können diese Informationen anzeigen, indem Sie auf dem Protokollbildschirm zur Ransomware-Übersicht in der Spalte **Details** auf den Link **Anzeigen** klicken.

Zeile	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, an dem bzw. zu der der Security Agent Informationen zum URL-Verstoß an Worry-Free Business Security gemeldet hat.
Gerätename	Name des Gerätes, das versucht, auf eine unzulässige URL zuzugreifen
URL	Unzulässige URL
URL-Kategorie	Kategorie der unzulässigen URL

Zeile	Beschreibung
Durchgeführte Aktion	Aktion, mit der Worry-Free Business Security auf einen URL-Verstoß reagiert.

Ransomware: Details zum Virusprotokoll

Sie können diese Informationen anzeigen, indem Sie auf dem Protokollbildschirm zur Ransomware-Übersicht in der Spalte **Details** auf den Link **Anzeigen** klicken.

Zeile	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, an dem bzw. zu der der Security Agent Informationen zur Erkennung von Ransomware an Worry-Free Business Security gemeldet hat.
Gerätename	Name des betroffenen Gerätes
Viren-/Malware-Name	Name der entdeckten Ransomware Klicken Sie auf diesen Link, um zur Trend Micro Bedrohungsenzyklopädie zu gelangen, die eine ausführliche Beschreibung der Bedrohung sowie Hinweise zum manuellen Säubern enthält.
Dateiname	Name der von Ransomware betroffenen Datei
Pfad	Speicherort der infizierten Datei
Angriffskanal	Medium, durch das Ransomware Zugriff auf den Endpunkt erlangt
Suchtyp	Der zum Entdecken der Ransomware verwendete Suchtyp
Durchgeführte Aktion	Aktion, mit der Worry-Free Business Security auf die Erkennung von Ransomware reagiert.

Ransomware: Details zum Web Reputation-Protokoll

Sie können diese Informationen anzeigen, indem Sie auf dem Protokollbildschirm zur Ransomware-Übersicht in der Spalte **Details** auf den Link **Anzeigen** klicken.

Zeile	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, an dem bzw. zu der der Security Agent Informationen zum URL-Verstoß an Worry-Free Business Security gemeldet hat.
Gerätename	Name des Gerätes, das versucht, auf eine unzulässige URL zuzugreifen
URL	Unzulässige URL
Risikostufe	Eine von TrendLabs ermittelte Bewertung des Risikos einer Infektion und möglicher Schäden.
Durchgeführte Aktion	Aktion, mit der Worry-Free Business Security auf einen URL-Verstoß reagiert.

Lizenzstatus

Dieses Widget enthält einen Überblick über die Anzahl der genutzten Lizenzen und den Ablaufstatus Ihrer Lizenz.

Übersicht zu Exchange Server

Dieses Widget stellt eine Übersicht zum Verbindungsstatus der Messaging Security Agents und eine Verteilung der Erkennung von Bedrohungen auf Ihren Exchange Servern bereit.

Klicken Sie auf die Sicherheitsebene, um die Spam-Erkennungsebene für den Messaging Security Agent zu konfigurieren.

Spalte	Description
Server	Name des Exchange Servers
Ereignis	Art der Spam-E-Mails
Rate	Ist gleich der Anzahl der Funde geteilt durch die Anzahl der durchsuchten Nachrichten

Agent-Status

Dieses Widget enthält einen Überblick über die Verbindung und den Update-Status der Security Agents in Ihrem Netzwerk.

- Klicken Sie auf die Anzahl neben dem Status, um zum Fenster **Geräte** weitergeleitet zu werden. In diesem Fenster sind die Geräteinformationen für diesen bestimmten Status aufgeführt.
- Klicken Sie auf **Geräte hinzufügen**, um zum Fenster **Geräte hinzufügen** weitergeleitet zu werden. In diesem Fenster können Sie den Security Agent auf weiteren Geräten installieren.

  Weitere Informationen finden Sie unter *Agents installieren auf Seite 3-1*.
- Klicken Sie auf **Komponentenstatus überprüfen**, um zum Fenster **Manuelles Update** weitergeleitet zu werden. In diesem Fenster können Sie die neuesten Komponenteninformationen anzeigen.

  Weitere Informationen finden Sie unter *Update-Komponenten auf Seite 8-4*.

Kapitel 10

Benachrichtigungen verwalten

Dieses Kapitel erläutert die Verwendung verschiedener Benachrichtigungsoptionen.

Benachrichtigungen verwenden

Um den Zeitaufwand für Administratoren für die Überwachung von Worry-Free Business Security zu minimieren und sicherzustellen, dass Administratoren Frühwarnungen per E-Mail über drohende Ausbruchssituationen erhalten, stellen Sie den Server so ein, dass er bei abnormalen Ereignissen im Netzwerk Benachrichtigungen sendet.

Standardmäßig sind alle Ereignisse im Fenster **Benachrichtigungen** ausgewählt, sodass der Server eine Benachrichtigung an Administratoren sendet.

TABELLE 10-1. Benachrichtigungen zu erforderlichen Aktionen

EREIGNISTYP	BESCHREIBUNG
Bedrohungen	
Virenschutz – Nicht behobene Bedrohungen	Gegen Viren-/Malware-Bedrohungen durchgeführte Aktionen sind fehlgeschlagen. Die Anzahl der Funde beinhaltet nicht die folgende Suchaktion: Ein potenzielles Sicherheitsrisiko wurde übergangen
Virenschutz: Echtzeitsuche auf Endpunkten deaktiviert	Echtzeitsuche ist auf Endpunkten deaktiviert.
Virenschutz: Echtzeitsuche auf Exchange Server(n) deaktiviert	Echtzeitsuche ist auf Exchange Servern deaktiviert.
Anti-Spyware: Funde machen Geräteneustart erforderlich	Endpunkte mit Spyware-/Grayware-Funden müssen neu gestartet werden, um die Bedrohungen vollständig zu entfernen.
Systemereignisse	
Update: nicht aktuelle Agents	Für veraltete Security Agents sind Komponenten-Updates erforderlich.
Update: nicht aktuelle Messaging Security Agents	Für veraltete Messaging Security Agents sind Komponenten-Updates erforderlich.

Ereignistyp	Beschreibung
Update: nicht aktuelle Smart-Scan-Pattern	Für veraltete Smart-Scan-Pattern sind Pattern-Updates erforderlich.
Update: nicht aktuelle Security Server-Komponenten	Für veralteten Security Server sind Komponenten-Updates erforderlich.
Smart Protection Services: Dienst nicht verfügbar	Security Agents, die für Smart Scan konfiguriert sind, können keine Verbindung zu Smart Protection Services herstellen, oder der Service ist nicht verfügbar.
Mangel an Ressourcen: verbleibender Speicherplatz	Der verbleibende Festplattenspeicher auf bestimmten Servern unterschreitet den angegebenen Prozentsatz.
Lizenzereignisse	
Lizenz: abgelaufen	Lizenz ist abgelaufen.
Lizenz: wird in weniger als 60 Tagen ablaufen	Lizenz läuft in Kürze ab.
Lizenz: Lizenznutzung liegt bei mehr als 110%	Anzahl der genutzten Arbeitsplätze beträgt über 110%.
Lizenz: Lizenznutzung liegt bei mehr als 100%	Anzahl der genutzten Arbeitsplätze beträgt über 100%.

Tabelle 10-2. Benachrichtigungen zu Warnungen

Ereignistyp	Beschreibung
Bedrohungen	
Virenschutz: Virenfunde auf Endpunkten haben folgende Werte überschritten:	Auf Endpunkten erkannte Viren-/Malware-Bedrohungen haben die festgelegte Anzahl innerhalb des angegebenen Zeitraums überschritten.
Virenschutz: Virenfunde auf Exchange Servern haben folgende Werte überschritten:	Auf Exchange Servern entdeckte Viren-/Malware-Bedrohungen haben die festgelegte Anzahl innerhalb des angegebenen Zeitraums überschritten.
Anti-Spyware: Spyware-/Grayware-Funde haben folgende Werte überschritten:	Auf Endpunkten erkannte Spyware-/Grayware-Bedrohungen haben die festgelegte Anzahl innerhalb des angegebenen Zeitraums überschritten.

Ereignistyp	Beschreibung
Anti-Spam: Spam-Funde in empfangenen Nachrichten insgesamt haben folgende Werte überschritten:	Spam-Funde in empfangenen Nachrichten insgesamt haben den angegebenen Prozentsatz überschritten.
Web Reputation: URL-Verstöße haben folgende Werte überschritten:	URL-Verstöße haben die festgelegte Anzahl innerhalb des angegebenen Zeitraums überschritten.
URL-Filter: URL-Verstöße haben folgende Werte überschritten:	URL-Verstöße haben die festgelegte Anzahl innerhalb des angegebenen Zeitraums überschritten.
Vorausschauendes Maschinenlernen: Erkennung unbekannter Bedrohungen hat folgende Werte überschritten:	Erkennung unbekannter Bedrohungen hat die festgelegte Anzahl innerhalb des angegebenen Zeitraums überschritten.
Verhaltensüberwachung: Verstöße gegen die Verhaltensüberwachung haben folgende Werte überschritten:	Verstöße gegen die Verhaltensüberwachung haben die festgelegte Anzahl innerhalb des angegebenen Zeitraums überschritten.
Netzwerkvirus: Erkennung von Netzwerkvirus hat folgende Werte überschritten:	Erkennung von Netzwerkviren hat die festgelegte Anzahl innerhalb des angegebenen Zeitraums überschritten.
Gerätesteuerung: Verstöße gegen die Gerätesteuerung haben folgende Werte überschritten:	Verstöße gegen die Gerätesteuerung haben die festgelegte Anzahl innerhalb des angegebenen Zeitraums überschritten.

Ereignisse für Benachrichtigungen konfigurieren

Worry-Free Business Security bietet drei Methoden, um Benachrichtigungen zu übermitteln:

- SNMP-Benachrichtigung
- Windows Ereignisprotokoll

- E-Mail-Benachrichtigung

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen**.
2. Um SNMP-Benachrichtigungen zu erhalten, konfigurieren Sie den Abschnitt **Empfänger der SNMP-Benachrichtigung**.

   Simple Network Management Protocol (SNMP) ist ein Protokoll für die Netzwerkverwaltung. Verwenden Sie einen MIB-Browser (Management Information Base), um Daten aus dem SNMP-Trap anzuzeigen.

   a. Wählen Sie **SNMP-Benachrichtigungen aktivieren** aus.

   b. Geben Sie die IP-Adresse für den SNMP-Trap ein.

   c. Geben Sie die Zeichenfolge der SNMP-Community ein.
3. Um Windows-Ereignisprotokollbenachrichtigungen zu erhalten, wählen Sie **Eintrag im Windows Ereignisprotokoll erstellen** unter **Protokollierung** aus.
4. Um E-Mail-Benachrichtigungen zu erhalten, geben Sie Absender und Empfänger an.

   Tipp

   Trennen Sie mehrere Einträge mit einem Strichpunkt.
5. Klicken Sie auf die Registerkarte **Aktion erforderlich** oder **Warnungen**.
6. Aktivieren Sie in der Spalte **E-Mail-Benachrichtigungen** die Kontrollkästchen, die den Ereignistypen entsprechen, über die Sie Benachrichtigungen erhalten möchten.
7. Wenn die Option in der Spalte **Alarmschwellenwert** verfügbar ist, geben Sie die Anzahl der Funde oder Verstöße innerhalb jedes Zeitraums an, die eine Benachrichtigung auslösen.

8. Um die Betreffzeile und den Nachrichtentext der einzelnen Ereignisbenachrichtigungen anzupassen, klicken Sie auf den Benachrichtigungslink in der Spalte **Typ**.

   Weitere Informationen zum Anpassen von Benachrichtigungen finden Sie unter *Token-Variablen auf Seite 10-6*.

9. Klicken Sie auf **Speichern**.

Token-Variablen

Die Betreffzeile und der Nachrichtentext von Ereignisbenachrichtigungen können mit Token-Variablen angepasst werden.

Um zu vermeiden, dass alle E-Mail-Nachrichten von Adressen mit externen Domänen als Spam gekennzeichnet werden, fügen Sie die externen E-Mail-Adressen zu den Listen der zulässigen Absender für Anti-Spam hinzu.

Die folgenden Token stehen für Bedrohungsereignisse, die auf Desktops/Servern und Microsoft Exchange Servern entdeckt wurden.

Token	Description	Alarmstufe
%COUNT	Fügt die Anzahl der Funde ein	Warnungsereignisse: Alle
$CSM_SERVERNAME	Fügt den Namen des Security Servers ein	Alle
%DATE	Fügt die Anzahl der Tage ein, die für die Lizenz verbleiben	Lizenz: abgelaufen Lizenz: wird in weniger als 60 Tagen ablaufen

Token	Description	Alarmstufe
%DATE_TIME	Fügt das Datum und die Uhrzeit des Ereignisses ein	Virenschutz – Nicht behobene Bedrohungen Virenschutz: Echtzeitsuche auf Endpunkten deaktiviert Virenschutz: Echtzeitsuche auf Exchange Server(n) deaktiviert Anti-Spyware: Funde machen Geräteneustart erforderlich Update: nicht aktuelle Agents Update: nicht aktuelle Messaging Security Agents Update: nicht aktuelle Security Server-Komponenten Smart Protection Services: Dienst nicht verfügbar Mangel an Ressourcen: verbleibender Speicherplatz

Token	Description	Alarmstufe
%DEVICE_COUNT	Fügt die Anzahl der betroffenen Geräte ein	Virenschutz – Nicht behobene Bedrohungen Virenschutz: Echtzeitsuche auf Endpunkten deaktiviert Virenschutz: Echtzeitsuche auf Exchange Server(n) deaktiviert Anti-Spyware: Funde machen Geräteneustart erforderlich Update: nicht aktuelle Agents Update: nicht aktuelle Messaging Security Agents Mangel an Ressourcen: verbleibender Speicherplatz Alle Warnungsereignisse außer den folgenden: Anti-Spam: Spam-Funde in empfangenen Nachrichten insgesamt haben folgende Werte überschritten:
%FROM	Fügt Startzeit und Startdatum des Ereignisses ein	Alle Warnungsereignisse außer den folgenden: Anti-Spam: Spam-Funde in empfangenen Nachrichten insgesamt haben folgende Werte überschritten:

Token	Description	Alarmstufe
%NUMBER	Zeigt die Anzahl der Ereignisse auf	Virenschutz – Nicht behobene Bedrohungen Virenschutz: Echtzeitsuche auf Endpunkten deaktiviert Virenschutz: Echtzeitsuche auf Exchange Server(n) deaktiviert Anti-Spyware: Funde machen Geräteneustart erforderlich Alle Warnungsereignisse außer den folgenden: Anti-Spam: Spam-Funde in empfangenen Nachrichten insgesamt haben folgende Werte überschritten:
%SEAT_IN_USE_COUNT	Fügt die Anzahl der verwendeten Desktop/Server-Arbeitsplätze ein	Lizenz: Genutzte Arbeitsplätze überschreiten 110% Lizenz: Genutzte Arbeitsplätze überschreiten 100 %
%SEAT_PURCHASED_COUNT	Fügt die Anzahl der Desktop/Server-Arbeitsplätze ein, die in Ihrer Lizenz verfügbar sind	Lizenz: Genutzte Arbeitsplätze überschreiten 110% Lizenz: Genutzte Arbeitsplätze überschreiten 100 %

Token	Description	Alarmstufe
%THRESHOLD%	Stellt den Schwellenwert eines Ereignisses bereit	Update: nicht aktuelle Agents Update: nicht aktuelle Smart-Scan-Pattern Update: nicht aktuelle Security Server-Komponenten Smart Protection Services: Dienst nicht verfügbar Mangel an Ressourcen: verbleibender Speicherplatz Lizenz: Lizenznutzung liegt bei mehr als 110% Lizenz: Lizenznutzung liegt bei mehr als 100% Warnungsereignisse: Alle
%TO	Fügt Endzeit und Enddatum des Ereignisses ein	Alle Warnungsereignisse außer den folgenden: Anti-Spam: Spam-Funde in empfangenen Nachrichten insgesamt haben folgende Werte überschritten:

```
Betreff: [Security Server - <$CSM_SERVERNAME>] [Aktion
erforderlich] Virenschutz: nicht behobene Bedrohungen: %NUMBER
Nachricht: Benachrichtigung von Trend Micro Worry-Free Business Security
* Virenschutz: nicht behobene Bedrohungen: %NUMBER
* Berichtszeit: %DATE_TIME
* Betroffene Geräte: %DEVICE_COUNT
* Vorschlag:
  Führen Sie eine Suche mit dem Trend Micro HouseCall Tool durch.
```

```
Betreff: [Security Server - Server A] [Aktion erforderlich]
Virenschutz: nicht behobene Bedrohungen: 5
Nachricht: Benachrichtigung von Trend Micro Worry-Free Business Security
* Virenschutz: nicht behobene Bedrohungen: 5
```

```
* Berichtszeit: 14. Februar 2018
* Betroffene Geräte: 2
* Vorschlag:
  Führen Sie eine Suche mit dem Trend Micro HouseCall Tool durch.
```

Kapitel 11

Allgemeine Einstellungen verwalten

In diesem Kapitel werden die allgemeinen Einstellungen für Agents und die Systemeinstellungen für den Security Server beschrieben.

Allgemeine Einstellungen

Sie können die allgemeinen Einstellungen für den Security Server und die Security Agents über die Webkonsole konfigurieren.

Registerkarten	Description
Proxy	Wenn das Netzwerk über einen Proxy-Server mit dem Internet verbunden ist, geben Sie die Proxy-Servereinstellungen für folgende Services an: • Komponenten-Updates und Lizenz-Benachrichtigungen • Web Reputation, Verhaltensüberwachung und Smart Scan Weitere Informationen finden Sie unter *Internet-Proxy-Einstellungen konfigurieren auf Seite 11-3*.
SMTP	Die Einstellungen des SMTP-Servers gelten für alle vom Security Server erstellten Benachrichtigungen und Berichte. Weitere Informationen finden Sie unter *Einstellungen des SMTP-Servers konfigurieren auf Seite 11-4*.
Desktop/Server	Die Sicherheitseinstellungen gelten für alle Security Agents. Weitere Informationen finden Sie unter *Desktop-/Server-Einstellungen konfigurieren auf Seite 11-5*.
System	Mit den Systemeinstellungen können Sie automatisch inaktive Agents entfernen, die Verbindung von Agents überprüfen und den Quarantäne-Ordner verwalten. Weitere Informationen finden Sie unter *Systemeinstellungen konfigurieren auf Seite 11-10*.
Ausnahmen	Mit den Ausnahmelisten können Sie die in Web Reputation, URL-Filter und Vorausschauendes Maschinenlernen definierten Richtlinieneinstellungen außer Kraft setzen. Weitere Informationen finden Sie unter *Einstellungen für die Ausnahmeliste konfigurieren auf Seite 11-14*.

Internet-Proxy-Einstellungen konfigurieren

Wenn der Security Server und die Agents über einen Proxy-Server mit dem Internet verbunden sind, geben Sie die Proxy-Servereinstellungen an, um folgende Funktionen und Trend Micro Dienste nutzen zu können:

- **Security Server**: Komponenten-Updates und Lizenzwartung
- **Security Agents**: Web Reputation, URL-Filter, Verhaltensüberwachung, Smart Feedback und Smart Scan
- **Messaging Security Agents** (nur Advanced): Web Reputation und Anti-Spam

---

Prozedur

1. Gehen Sie zu **Administration** > **Allgemeine Einstellungen**.
2. Aktualisieren Sie auf der Registerkarte **Proxy** folgende Optionen bei Bedarf:
   - Security Server Proxy

     Hinweis

     Messaging Security Agents verwenden auch Security Server Proxy-Einstellungen.

     - Für Updates und Lizenz-Benachrichtigungen Proxy-Server verwenden
     - SOCKS 4/5 Proxy-Protokoll verwenden
     - Adresse: IPv4/IPv6-Adresse oder Host-Name
     - Port
     - Proxy-Server-Authentifizierung
       - Benutzername

        - Kennwort
    - Security Agent Proxy
        - Für den Update-Proxy festgelegte Anmeldedaten verwenden

Hinweis

Security Agents verwenden den Internet Explorer Proxy-Server und Port für die Internetverbindung. Wählen Sie diese Option nur aus, wenn sich der Internet Explorer auf den Clients und der Security Server die gleichen Authentifizierungsdaten teilen.

        - Benutzername
        - Kennwort

3. Klicken Sie auf **Speichern**.

Einstellungen des SMTP-Servers konfigurieren

Die Einstellungen des SMTP-Servers gelten für alle von Worry-Free Business Security erstellten Benachrichtigungen und Berichte.

Prozedur

1. Gehen Sie zu **Administration** > **Allgemeine Einstellungen**.
2. Klicken Sie auf die Registerkarte **SMTP**, und aktualisieren Sie folgende Einstellungen bei Bedarf:
    - **SMTP-Server**: die IPv4/IPv6-Adresse oder der Name des SMTP-Servers.
    - **Port**
    - **SMTP-Server-Authentifizierung aktivieren**
        - Benutzername

- Kennwort

3. Klicken Sie auf **Test-E-Mail versenden**, um die Richtigkeit der Einstellungen zu überprüfen. Schlägt der Versand fehl, ändern Sie die Einstellungen oder überprüfen Sie den Status des SMTP-Servers.

4. Klicken Sie auf **Speichern**.

Desktop-/Server-Einstellungen konfigurieren

Die Desktop- und Serveroptionen gehören zu den allgemeinen Einstellungen von Worry-Free Business Security. Einstellungen für einzelne Gruppen überschreiben diese Einstellungen. Wenn Sie keine bestimmte Option für eine Gruppe konfiguriert haben, werden die Desktop- und Serveroptionen verwendet. Sind zum Beispiel für eine bestimmte Gruppe keine Links zulässig, gelten alle in diesem Fenster zugelassenen Links für die Gruppe.

Prozedur

1. Gehen Sie zu **Administration** > **Allgemeine Einstellungen**.

2. Klicken Sie auf die Registerkarte **Desktop/Server** und aktualisieren Sie die folgenden Elemente bei Bedarf:

Einstellungen	Beschreibung
Location Awareness	Mit Location Awareness können Administratoren Sicherheitseinstellungen gemäß der Art der Verbindung des Clients mit dem Netzwerk steuern. Location Awareness steuert die Verbindungseinstellungen für "Im Büro" und "Nicht im Büro". Der Security Agent erkennt anhand der Gateway-Informationen, die auf der Webkonsole konfiguriert wurden, den Standort eines Clients automatisch und kontrolliert, auf welche Websites die Benutzer zugreifen dürfen. Die Einschränkungen gelten je nach Standort:

Einstellungen	Beschreibung

	• **Location Awareness aktivieren**: Diese Einstellungen haben Auswirkungen auf die Verbindungseinstellungen für Im Büro/ Nicht im Büro von Firewall, Web Reputation und die Häufigkeit zeitgesteuerter Updates.
	• **Gateway-Informationen**: Clients und Verbindungen in dieser Liste verwenden bei einer Remote-Verbindung mit dem Netzwerk (über VPN) die Einstellungen für Interne Verbindung. Die Option Location Awareness ist dabei aktiviert.
	  • Gateway-IP-Adresse
	  • MAC-Adresse: Durch Hinzufügen der MAC-Adresse wird die Sicherheit deutlich verstärkt, da sich nur das konfigurierte Gerät verbinden darf.
	Klicken Sie auf das entsprechende Symbol zum Löschen (x), um einen Eintrag zu löschen.

Helpdesk - Hinweis	Der Helpdesk-Hinweis platziert eine Benachrichtigung auf dem Security Agent, der den Benutzer darüber informiert, an wen er sich wenden kann, wenn er Hilfe benötigt. Aktualisieren Sie auf Anforderung folgende Einstellungen: • **Helpdesk – Kennzeichnung** • **Helpdesk – E-Mail-Adresse** • **Zusätzliche Informationen**: Diese werden angezeigt, wenn der Benutzer die Maus über die Kennzeichnung zieht.
Allgemeine Sucheinstellungen	• **Smart Scan Service deaktivieren**: Schaltet alle Security Agents in den Modus für die herkömmliche Suche um. Die Smart Scan ist erst wieder verfügbar, wenn sie hier erneut aktiviert wird. Navigieren Sie zu **Geräte** > **{Gruppe}** > **Richtlinie konfigurieren** > **Suchmethode**, um eine oder mehrere Security Agent-Gruppen umzuschalten. **Hinweis** Richtlinien zum Umschalten der Suchmethoden für Security Agents finden Sie unter *Suchmethoden konfigurieren auf Seite 5-5*.

Einstellungen	Beschreibung
	• **Verzögerte Suche für Dateivorgänge aktivieren**: Wählen Sie diese Option, um die Leistungsfähigkeit des Systems zu optimieren. **Warnung!** Die Aktivierung der verzögerten Suche kann zu Sicherheitsrisiken führen. • **Schattenkopiebereiche ausschließen**: Schattenkopien (Volume Snapshot Services) erzeugen manuelle oder automatische Backups oder Sicherungsabbilder einer Datei oder eines Ordners auf einem bestimmten Laufwerk. • **Den Datenbankordner des Security Servers ausschließen**: Verhindert, dass auf dem Security Server installierte Agents während der Echtzeitsuche ihre eigenen Datenbanken durchsuchen. Standardmäßig durchsucht WFBS seine eigene Datenbank nicht. Trend Micro empfiehlt, diese Einstellung beizubehalten, um mögliche Probleme mit der Datenbank während der Suche auszuschließen. • **Ordner von Microsoft Exchange Server ausschließen (bei Installation auf Microsoft Exchange Server)**: Verhindert, dass auf dem Microsoft Exchange Server installierte Agents Microsoft Exchange Ordner durchsuchen. • **Ordner des Microsoft Domänencontrollers ausschließen**: Verhindert, dass auf dem Domänencontroller installierte Agents Domänencontroller-Ordner durchsuchen. In diesen Ordnern sind Benutzerdaten, Benutzernamen, Kennwörter und andere wichtige Informationen gespeichert.
Einstellungen der Virensuche	• **Sucheinstellungen für große, komprimierte Dateien konfigurieren**: Geben Sie die maximale Größe der extrahierten Datei und die Anzahl der Dateien in der komprimierten Datei an, die der Agent durchsuchen soll. • **Komprimierte Dateien säubern**: Die Agents säubern infizierte Dateien innerhalb einer komprimierten Datei. • **Suche in bis zu { } OLE-Schichten**: Die Agents durchsuchen die festgelegte Anzahl von Object Linking and Embedding-

Einstellungen	Beschreibung
	Schichten (OLE). Mit OLE können Objekte mit einer Anwendung erstellt, in eine andere Anwendung eingebettet oder mit dieser verknüpft werden (z. B. eine in einer .doc-Datei eingebettete .xls-Datei). • **Manuelle Suche zum Windows Kontextmenü auf Clients hinzufügen**: Fügt die Verknüpfung **Mit Security Agent suchen** zum Kontextmenü hinzu. Der Benutzer kann dann mit der rechten Maustaste auf eine Datei oder einen Ordner auf dem Desktop oder im Windows Explorer klicken und die Datei oder den Ordner manuell durchsuchen.
Einstellungen der Suche nach Spyware/Grayware	• **Nach Cookies suchen**: Der Security Agent sucht nach Cookies. • **Cookie-Funde zum Spyware-Protokoll hinzufügen**: Fügt jedes entdeckte Spyware-Cookie zum Spyware-Protokoll hinzu.
Firewall-Einstellungen	Wählen Sie das Kontrollkästchen **Firewall deaktivieren und Treiber deinstallieren**, um die Worry-Free Business Security Client-Firewall zu deinstallieren und die zugehörigen Treiber zu entfernen. **Hinweis** Wenn Sie die Firewall deaktivieren, sind die entsprechenden Einstellungen erst dann verfügbar, wenn Sie die Firewall erneut aktivieren.
Schutz vor Internet-Bedrohungen für HTTPS	Aktivieren Sie diese Funktion, um HTTPS-URLs anhand von Web Reputation- und URL-Filter-Einstellungen auf Chrome, Firefox und Microsoft Edge zu überprüfen. **Hinweis** Für diese Funktion ist kein zusätzliches Browser-Add-On erforderlich. Standardmäßig überprüft Worry-Free Business Security HTTPS-URLs in Internet Explorer unter Verwendung von Browser-Add-Ons.

Einstellungen	Beschreibung
Warneinstellungen	**Warnsymbol in der Windows Task-Leiste anzeigen, wenn die Viren-Pattern-Datei nach {} Tagen nicht aktualisiert wurde**: Wenn die Pattern-Datei nach einer bestimmten Anzahl von Tagen nicht aktualisiert wurde, wird auf den Clients ein Warnsymbol angezeigt.
Security Agent Deinstallationskennwort	• **Den Client zur Deinstallation des Security Agents ohne ein Kennwort berechtigen.** • **Client-Benutzer zur Eingabe eines Kennworts bei der Deinstallation des Security Agents auffordern.**
Kennwort zum Beenden und Entsperren des Security Agent Programms	• **Client-Benutzer zum Beenden und Entsperren des Security Agents auf ihrem Computer ohne Eingabe eines Kennworts berechtigen.** • **Client-Benutzer zur Eingabe eines Kennworts beim Beenden und zum Entsperren des Security Agents auffordern.** **Hinweis** Wenn Benutzer den Security Agent entsperren, können sie alle Einstellungen außer Kraft setzen, die unter **Geräte** > **{Gruppe}** > **Richtlinie konfigurieren** > **Agent-Berechtigungen** konfiguriert wurden.
Bevorzugte IP-Adresse	Diese Einstellung ist nur auf Dual-Stack-Security Servern verfügbar und wird nur von Dual-Stack-Agents angewendet. Nach der Installation oder dem Upgrade von Agents, registrieren sich die Agents über eine IP-Adresse am Security Server. Wählen Sie dazu eine der folgenden Optionen aus: • **Zuerst IPv4, dann IPv6**: Agents verwenden zuerst ihre IPv4-Adresse. Wenn sich der Agent nicht mit seiner IPv4-Adresse registrieren kann, verwendet er seine IPv6-Adresse. Wenn die Registrierung mit beiden IP-Adressen fehlschlägt, wiederholt der Agent den Versuch mit Hilfe der IP-Adressen-Priorität für diese Auswahl. • **Zuerst IPv6, dann IPv4**: Agents verwenden zuerst ihre IPv6-Adresse. Wenn sich der Agent nicht mit seiner IPv6-Adresse

Einstellungen	Beschreibung
	registrieren kann, verwendet er seine IPv4-Adresse. Wenn die Registrierung mit beiden IP-Adressen fehlschlägt, wiederholt der Agent den Versuch mit Hilfe der IP-Adressen-Priorität für diese Auswahl.

3. Klicken Sie auf **Speichern**.

Systemeinstellungen konfigurieren

Der Bereich **System** im Fenster **Allgemeine Einstellungen** enthält Optionen zum automatischen Entfernen inaktiver Agents, zum Überprüfen der Verbindung von Agents und zur Verwaltung des Quarantäne-Ordners.

Prozedur

1. Gehen Sie zu **Administration** > **Allgemeine Einstellungen**.
2. Klicken Sie auf die Registerkarte **System**, und aktualisieren Sie folgende Einstellungen bei Bedarf:

Einstellungen	Beschreibung
Inaktive Security Agents entfernen	Wenn Sie die Agents mit dem Security Agent Deinstallationsprogramm von einem Client entfernen, wird der Security Server automatisch benachrichtigt. Daraufhin wird das Client-Symbol aus der Sicherheitsgruppenansicht des Security Servers entfernt. Wird der Security Agent jedoch auf andere Art entfernt, zum Beispiel durch das Formatieren der Festplatte oder das manuelle Löschen der Client-Dateien, erfolgt keine Benachrichtigung an den Security Server, und der Security Agent wird als inaktiv angezeigt. Deaktiviert der Benutzer den Agent über einen längeren Zeitraum, zeigt der Security Server den Security Agent ebenfalls als inaktiv an. Damit in der Sicherheitsgruppenansicht nur aktive Clients angezeigt werden, können Sie den Security Server so konfigurieren, dass inaktive Security Agents automatisch aus dieser Ansicht gelöscht werden. • **Automatisches Entfernen inaktiver Security Agents aktivieren**: Aktiviert das automatische Entfernen der Clients, die im festgelegten Zeitraum keine Verbindung zum Security Server aufgenommen haben. • **Inaktiven Security Agent automatisch entfernen nach {} Tagen**: Die Anzahl der Tage, die ein Client inaktiv sein darf, bevor er aus der Webkonsole entfernt wird.

Einstellungen	Beschreibung

Agentenverbindung süberprüfung	Worry-Free Business Security stellt den Verbindungsstatus der Clients in der Sicherheitsgruppenansicht durch Symbole dar. Bestimmte Umstände können dazu führen, dass der Agent-Verbindungsstatus in der Sicherheitsgruppenansicht nicht richtig angezeigt wird. Wenn das Netzwerkkabel eines Clients beispielsweise versehentlich entfernt wird, kann der Agent den Trend Micro Security Server nicht darüber informieren, dass er offline ist. Er wird somit in der Sicherheitsgruppenansicht weiterhin als online angezeigt.
	
	Die Agent/Server-Kommunikation kann über die Webkonsole manuell oder zeitgesteuert überprüft werden.
	
	Hinweis
	Bei der Überprüfung der Verbindung können keine bestimmten Gruppen oder Clients ausgewählt werden. Es wird die Verbindung aller mit dem Security Server registrierten Clients überprüft.
	
	• **Zeitgesteuerte Überprüfung aktivieren**: Aktiviert die zeitgesteuerte Überprüfung der Agent/Server-Verbindung.
	  • **Stündlich**
	  • **Täglich**
	  • **Wöchentlich, jeden**
	  • **Startzeit**: Zeitpunkt, zu dem die Überprüfung gestartet werden soll.
	• **Jetzt überprüfen**: Überprüft die Verbindung sofort.

Einstellungen	Beschreibung
Quarantäne-Wartung	Security Agents verschieben infizierte Dateien standardmäßig in Quarantäne in das folgende Verzeichnis im Security Server: `<Security Server-Installationsordner>\PCCSRV\Virus` Wenn Sie das Verzeichnis ändern müssen (z. B. aufgrund unzureichenden Speicherplatzes), geben Sie im Feld **Quarantäne-Ordner** einen absoluten Pfad wie `D:\Dateien in Quarantäne` ein. Stellen Sie in diesem Fall sicher, dass Sie dieselben Änderungen auch in **Geräte** > **{Gruppe}** > **Richtlinie konfigurieren** > **Quarantäne** vornehmen. Andernfalls senden Agents Dateien weiterhin an `<Security Server-Installationsordner>\PCCSRV\Virus`. Konfigurieren Sie außerdem die folgenden Wartungseinstellungen: • **Speicherumfang des Quarantäne-Ordners**: Die Größe des Quarantäne-Ordners in MB. • **Maximale Größe einer Datei**: Maximale Größe einzelner Dateien im Quarantäne-Ordner (in MB). • **Alle Dateien in Quarantäne löschen**: Löscht alle Dateien im Quarantäne-Ordner. Wenn der Ordner voll ist, werden neu hochgeladene Dateien nicht gespeichert. Wenn Agents keine Dateien in Quarantäne an den Security Server senden sollen, konfigurieren Sie das neue Verzeichnis unter **Geräte** > **{Gruppe}** > **Richtlinie konfigurieren** > **Quarantäne** und ignorieren Sie alle Wartungseinstellungen. Weitere Informationen finden Sie unter *Quarantäne-Ordner auf Seite 5-18*.

Einstellungen	Beschreibung
Security Agent-Installation	**Security Agent-Installationsverzeichnis**: Sie werden bei der Installation aufgefordert, das Security Agent Installationsverzeichnis einzugeben, in dem die einzelnen Security Agents installiert werden. Ändern Sie das Verzeichnis bei Bedarf, indem Sie einen absoluten Pfad eingeben. Es werden nur künftige Agents in diesem Verzeichnis installiert. Bestehende Agents bleiben in ihrem aktuellen Verzeichnis. Verwenden Sie eine der folgenden Variablen, um den Installationspfad festzulegen: • `$BOOTDISK`: Laufwerksbuchstabe der Startfestplatte • `$WINDIR`: Windows-Installationsordner • `$ProgramFiles`: Die Programmordner

3. Klicken Sie auf **Speichern**.

Einstellungen für die Ausnahmeliste konfigurieren

Prozedur

1. Gehen Sie zu **Administration** > **Allgemeine Einstellungen**.
2. Klicken Sie auf die Registerkarte **Ausnahmen** und konfigurieren Sie folgende Optionen bei Bedarf:

Abschnitt	Beschreibung
Web Reputation und URL-Filter	• **Liste der zulässigen URLs**: Websites (und deren untergeordnete Domänen), die von den Überprüfungen durch Web Reputation und URL-Filter ausgeschlossen sind.

Abschnitt	Beschreibung
	Hinweis Die Liste der genehmigten URLs hat Vorrang vor der Liste der gesperrten URLs. Wenn ein URL einem Eintrag in der Liste der genehmigten URLs entspricht, erlauben die Agents stets den Zugriff darauf, selbst wenn er sich auf der Liste der gesperrten URLs befindet. Benutzerdefinierte zulässige/gesperrte URLs für eine bestimmte Gruppe überschreiben die Einstellungen für die allgemeinen Ausnahmen. • **Liste der gesperrten URLs**: Websites (und deren untergeordnete Domänen), die durch den URL-Filter immer gesperrt sind. • **Prozess-Ausnahmeliste**:Prozesse, die von den Überprüfungen durch Web Reputation und URL-Filter ausgeschlossen sind. Geben Sie kritische Prozesse ein, die Ihr Unternehmen als vertrauenswürdig erachtet. **Tipp** Wenn Sie die Prozess-Ausnahmeliste aktualisieren und der Server die aktualisierte Liste an die Agents verteilt, werden alle aktiven HTTP-Verbindungen auf dem Client-Computer (durch Port 80, 81 oder 8080) für einige Sekunden unterbrochen. Aktualisieren Sie die Prozess-Ausnahmeliste an Zeiten mit geringem Arbeitsaufkommen. • **IP-Ausnahmeliste**:IP-Adressen (z. B. 192.168.0.1) sind von den Überprüfungen durch Web Reputation und URL-Filter ausgeschlossen. Geben Sie kritische IP-Adressen ein, die Ihr Unternehmen für vertrauenswürdig hält. • **Web Reputation- und URL-Filter-Protokolle an den Security Server senden**

Abschnitt	Beschreibung
Ausnahmeliste zu 'Vorausschauendes Maschinenlernen'	Konfigurieren Sie die globalen Ausnahmen für Vorausschauendes Maschinenlernen-Dateien, um zu verhindern, dass alle Security Agents eine Datei als bösartig erkennen. Geben Sie den SHA-1-Hashwert der Datei ein, der von der Suche ausgeschlossen werden soll. Geben Sie optional einen Hinweis zum Grund für die Ausnahme an oder beschreiben Sie den mit dem Hashwert verknüpften Dateinamen.

3. Klicken Sie auf **Speichern**.

Kapitel 12

Protokolle und Berichte verwenden

Dieses Kapitel beschreibt die Verwendung von Protokollen und Berichten zur Systemüberwachung und Analyse des Systemschutzes.

Protokolle

Worry-Free Business Security führt umfangreiche Protokolle über Viren-/Malware-Vorfälle, Spyware-/Grayware-Vorfälle und Updates und andere wichtige Ereignisse. Mit Hilfe dieser Protokolle können Sie die Unternehmensrichtlinien zum Schutz vor Bedrohungen bewerten, Clients ermitteln, die einem höheren Infektionsrisiko ausgesetzt sind, und sicherstellen, dass Updates erfolgreich verteilt wurden.

Hinweis

Protokolldateien im CSV-Format werden mit Tabellenkalkulationsanwendungen, wie beispielsweise Microsoft Excel, angezeigt.

Worry-Free Business Security verwaltet Protokolle unter den folgenden Kategorien:

- Ereignisprotokolle der Webkonsole
- Desktop-/Server-Protokolle
- Protokolle von Microsoft Exchange Server (nur Advanced)

Tabelle 12-1. Protokolltyp und Inhalt

Typ (Element, das den Protokolleintrag erstellt hat)	Inhalt (Protokolltyp, aus dem Inhalte angezeigt werden)
Ereignisse auf der Management-Konsole	• Manuelle Suche (über die Webkonsole gestartet) • Update (Updates des Security Servers) • Konsolenereignisse

Typ (Element, das den Protokolleintrag erstellt hat)	Inhalt (Protokolltyp, aus dem Inhalte angezeigt werden)

Desktop/Server	• Virenprotokolle
	  • Manuelle Suche
	  • Echtzeitsuche
	  • Zeitgesteuerte Suche
	• Spyware-/Grayware-Protokolle
	  • Manuelle Suche
	  • Echtzeitsuche
	  • Zeitgesteuerte Suche
	• Protokolle zu 'Vorausschauendes Maschinenlernen'
	• Web Reputation-Protokolle
	• URL-Filterprotokolle
	• Verhaltensüberwachungsprotokolle
	• Update-Protokolle
	• Netzwerkviren-Protokolle
	• Ereignisprotokolle
	• Protokolle der Gerätesteuerung
	• Hotfix-Anwendungsprotokolle aktualisieren
	• Ransomware-Protokolle
	  • Virenschutz
	  • Verhaltensüberwachung
	  • Web Reputation
	  • URL-Filter
	  • Vorausschauendes Maschinenlernen

Typ (Element, das den Protokolleintrag erstellt hat)	Inhalt (Protokolltyp, aus dem Inhalte angezeigt werden)
Exchange Server (nur Advanced)	• Virenprotokolle • Protokolle zu gesperrten Anhängen • Content-Filter / Prävention vor Datenverlust - Protokolle • Update-Protokolle • Backup-Protokolle • Archivprotokolle • Suchereignisprotokolle • Protokolle für nicht durchsuchbare Nachrichtenteile • Web Reputation-Protokolle • Mobile Ereignisprotokolle

Protokollabfrage verwenden

Führen Sie Protokollabfragen durch, um Informationen aus der Protokolldatenbank zu sammeln. Sie können Abfragen im Fenster **Protokollabfrage** einrichten und durchführen. Die Ergebnisse lassen sich dann als CSV-Datei exportieren oder ausdrucken.

Ein Messaging Security Agent (nur Advanced) versendet alle fünf Minuten die erstellten Protokolle an den Security Server (unabhängig vom Zeitpunkt der Protokollerstellung).

Prozedur

1. Navigieren Sie zu **Berichte** > **Protokollabfrage**.
2. Aktualisieren Sie folgende Optionen bei Bedarf:
   - **Zeitraum**
     - **Vorkonfigurierter Zeitraum**

    - **Ausgewählter Zeitraum**: Beschränkt den Bericht auf ein bestimmtes Datum.

  - **Typ**: Informationen über das Anzeigen des Inhalts der jeweiligen Protokolltypen finden Sie unter *Protokolle auf Seite 12-2*.

    - **Ereignisse auf der Management-Konsole**
    - **Desktop/Server**
    - **Exchange Server** (nur Advanced)

  - **Inhalt**: Je nach **Protokolltyp** sind unterschiedliche Optionen verfügbar.

3. Klicken Sie auf **Protokolle anzeigen**.
4. Wenn Sie das Protokoll als komma-separierte Datei im CSV-Format speichern möchten, klicken Sie auf **Exportieren**. Verwenden Sie zur Anzeige von Protokolldateien im CSV-Format ein Tabellenkalkulationsprogramm.

Berichte

Sie können Einzelberichte manuell erstellen oder den Security Server für die Erstellung zeitgesteuerter Berichte konfigurieren.

Ebenso können Sie Berichte drucken oder per E-Mail an einen Administrator oder andere Personen versenden.

Die im Bericht aufgeführten Daten hängen von der Anzahl der Protokolle ab, die zum Zeitpunkt der Berichtserstellung auf dem Security Server verfügbar waren. Die Anzahl der Protokolle ändert sich, da neue Protokolle hinzugefügt und bestehende gelöscht werden. Unter **Berichte** > **Wartung** können Sie Protokolle manuell löschen oder einen Zeitplan zum Löschen von Protokollen erstellen.

Mit Einzelberichten arbeiten

Prozedur

1. Navigieren Sie zu **Berichte** > **Einzelberichte**.
2. Führen Sie folgende Aufgaben durch:

Task	Schritte

Einen Bericht erstellen	a. Klicken Sie auf **Hinzufügen**.
	Ein neues Fenster wird angezeigt.
	b. Konfigurieren Sie das Folgende:
	• **Name des Berichts**
	• **Zeitraum**: Beschränkt den Bericht auf ein bestimmtes Datum.
	• **Inhalt**: Aktivieren Sie das Kontrollkästchen **Alle auswählen**, um alle Bedrohungen auszuwählen. Um nur bestimmte Bedrohungen auszuwählen, aktivieren Sie das jeweilige Kontrollkästchen. Klicken Sie auf das Plussymbol (+), um die Auswahl zu erweitern.
	• **Bericht senden an**
	  • **Empfänger**: Geben Sie die E-Mail-Adressen der Empfänger ein, und trennen Sie sie jeweils durch einen Strichpunkt (;).
	  • **Format**: Wählen Sie PDF oder einen Link zu einem HTML-Bericht. Wenn Sie PDF auswählen, wird die PDF-Datei an die E-Mail angehängt.
	c. Klicken Sie auf **Hinzufügen**.

Task	Schritte
Den Bericht anzeigen	Klicken Sie in der Spalte Name des Berichts auf die Links zu einem Bericht. Der erste Link öffnet einen Bericht im PDF-Format, der zweite Link öffnet einen Bericht im HTML-Format. Die im Bericht aufgeführten Daten hängen von der Anzahl der Protokolle ab, die zum Zeitpunkt der Berichtserstellung auf dem Security Server verfügbar waren. Die Anzahl der Protokolle ändert sich, da neue Protokolle hinzugefügt und bestehende gelöscht werden. Unter **Berichte** > **Wartung** können Sie Protokolle manuell löschen oder einen Zeitplan zum Löschen von Protokollen erstellen. Weitere Informationen zum Inhalt des Berichts finden Sie unter *Berichte interpretieren auf Seite 12-11*.
Berichte löschen	a. Wählen Sie die Zeile mit den Berichtslinks aus. b. Klicken Sie auf **Löschen**. **Hinweis** Um Berichte automatisch zu löschen, navigieren Sie zu **Berichte** > **Wartung** > **Berichte**, und legen Sie die maximale Anzahl an Einzelberichten fest, die Worry-Free Business Security beibehält. Der Standardwert ist 10 Einzelberichte. Wenn die Anzahl überschritten wird, löscht der Security Server diese überzähligen Berichte, beginnend mit dem Bericht, der am längsten aufbewahrt wurde.

Mit zeitgesteuerten Berichten arbeiten

Prozedur

1. Navigieren Sie zu **Berichte** > **Zeitgesteuerte Berichte**.
2. Führen Sie folgende Aufgaben durch:

Task	Schritte

Vorlagen für einen zeitgesteuerten Bericht erstellen	a. Klicken Sie auf **Hinzufügen**.
	
	Ein neues Fenster wird angezeigt.
	
	b. Konfigurieren Sie das Folgende:
	
	• **Name der Berichtvorlage**
	
	• **Zeitplan**: Täglich, wöchentlich oder monatlich und die Zeit zum Erstellen des Berichts
	
	Wenn Sie bei monatlichen Berichten 31, 30 oder 29 Tage auswählen und ein Monat weniger Tage hat, erstellt WFBS in diesem Monat keinen Bericht.
	
	• **Inhalt**: Aktivieren Sie das Kontrollkästchen **Alle auswählen**, um alle Bedrohungen auszuwählen. Um nur bestimmte Bedrohungen auszuwählen, aktivieren Sie das jeweilige Kontrollkästchen. Klicken Sie auf das Plussymbol (+), um die Auswahl zu erweitern.
	
	• **Bericht senden an**
	
	  • **Empfänger**: Geben Sie die E-Mail-Adressen der Empfänger ein, und trennen Sie sie jeweils durch einen Strichpunkt (;).
	
	  • **Format**: Wählen Sie PDF oder einen Link zu einem HTML-Bericht. Wenn Sie PDF auswählen, wird die PDF-Datei an die E-Mail angehängt.
	
	c. Klicken Sie auf **Hinzufügen**.

Task	Schritte
Zeitgesteuerte Berichte anzeigen	a. Klicken Sie in der Zeile mit der Vorlage, von der die zeitgesteuerten Berichte erstellt werden, auf **Berichtverlauf**. Es öffnet sich ein neues Fenster. b. Klicken Sie in der Spalte Ansicht auf die Links zu einem Bericht. Der erste Link öffnet einen Bericht im PDF-Format, der zweite Link öffnet einen Bericht im HTML-Format. Die im Bericht aufgeführten Daten hängen von der Anzahl der Protokolle ab, die zum Zeitpunkt der Berichtserstellung auf dem Security Server verfügbar waren. Die Anzahl der Protokolle ändert sich, da neue Protokolle hinzugefügt und bestehende gelöscht werden. Unter **Berichte** > **Wartung** können Sie Protokolle manuell löschen oder einen Zeitplan zum Löschen von Protokollen erstellen. Weitere Informationen zum Inhalt des Berichts finden Sie unter *Berichte interpretieren auf Seite 12-11*.
Aufgaben zu Vorlagenwartung	
Vorlageneinstellungen bearbeiten	Klicken Sie auf die Vorlage, und bearbeiten Sie anschließend die Einstellungen im anschließend angezeigten neuen Fenster. Die Berichte, die nach dem Speichern Ihrer Änderungen erstellt werden, verwenden die neuen Einstellungen.
Eine Vorlage aktivieren/ deaktivieren	Klicken Sie auf das Symbol unter der Spalte Aktiviert. Deaktivieren Sie eine Vorlage, wenn Sie das Erstellen von zeitgesteuerten Berichten vorübergehend anhalten möchten, und aktivieren Sie sie, wenn Sie die Berichte erneut benötigen.

Task	Schritte
Eine Vorlage löschen	Wählen Sie die Vorlage aus, und klicken Sie auf **Löschen**. Wenn Sie eine Vorlage löschen, werden die zeitgesteuerten Berichte, die über diese Vorlage erstellt wurden, nicht gelöscht. Jedoch stehen die Links zu diesen Berichten in der Webkonsole nicht mehr zur Verfügung. Sie können vom Security Server-Computer direkt auf diese Berichte zugreifen. Berichte werden nur gelöscht, wenn Sie sie manuell vom Computer löschen oder der Security Server die Berichte entsprechend der Einstellung zum automatischen Löschen unter **Berichte** > **Wartung** > **Berichte** automatisch löscht. Um Vorlagen automatisch zu löschen, navigieren Sie zu **Berichte** > **Wartung** > **Berichte**, und legen Sie die maximale Anzahl an Vorlagen fest, die Worry-Free Business Security beibehält. Der Standardwert ist 10 Vorlagen. Wenn die Anzahl überschritten wird, löscht der Security Server diese überzähligen Vorlagen, beginnend mit der Vorlage, die am längsten aufbewahrt wurde.
Aufgaben zur Berichtwartung	
Link zu zeitgesteuerten Berichten senden	Senden Sie per E-Mail einen Link zu den zeitgesteuerten Berichten (im PDF-Format). Die Empfänger klicken auf den Link in der E-Mail-Benachrichtigung, um auf die PDF-Datei zuzugreifen. Stellen Sie sicher, dass die Empfänger auf den Security Server-Computer zugreifen können, damit die Datei angezeigt werden kann. **Hinweis** In der E-Mail wird nur ein Link zur PDF-Datei bereitgestellt. Die eigentliche PDF-Datei ist nicht angehängt. a. Klicken Sie in der Zeile mit der Vorlage, von der die zeitgesteuerten Berichte erstellt werden, auf **Berichtverlauf**. Es öffnet sich ein neues Fenster. b. Wählen Sie die Berichte aus, und klicken Sie anschließend auf **Senden**. Ihr Standard-Mail-Client wird geöffnet und zeigt eine neue E-Mail mit dem Link zum Bericht an.

Task	Schritte
Zeitgesteuerte Berichte löschen	a. Klicken Sie in der Zeile mit der Vorlage, von der die zeitgesteuerten Berichte erstellt werden, auf **Berichtverlauf**. Es öffnet sich ein neues Fenster. b. Wählen Sie die Berichte aus, und klicken Sie auf **Löschen**. **Hinweis** Um Berichte automatisch zu löschen, navigieren Sie zu **Berichte** > **Wartung** > **Berichte**, und legen Sie die maximale Anzahl an zeitgesteuerten Berichten fest, die Worry-Free Business Security beibehält. Der Standardwert ist 10 zeitgesteuerte Berichte. Wenn die Anzahl überschritten wird, löscht der Security Server diese überzähligen Berichte, beginnend mit dem Bericht, der am längsten aufbewahrt wurde.

Berichte interpretieren

Worry-Free Business Security verwendet die folgenden Informationen: Welche Informationen angezeigt werden, hängt von den ausgewählten Optionen ab.

Tabelle 12-2. Inhalte eines Berichts

Berichtelement	Beschreibung
Virenschutz	**Virenübersicht für Desktops und Server** Virenberichte enthalten detaillierte Informationen über Anzahl und Art der von der Scan Engine entdeckten Viren und Malware sowie den jeweils durchgeführten Aktionen. Der Bericht enthält außerdem die Namen der am häufigsten gefundenen Viren und Malware. Klicken Sie auf den Namen des Virus/der Malware, um eine neue Seite Ihres Webbrowsers zu öffnen und zur Trend Micro Virenenzyklopädie weitergeleitet zu werden. Dort erhalten Sie weiterführende Informationen.
	Die 5 Desktops/Server mit den meisten Virenfunden Hier werden die fünf Desktops oder Server mit den häufigsten Viren-/Malware-Funden angezeigt. Regelmäßige Viren- oder Malware-Vorfälle auf einem Client können bedeuten, dass dieser Client ein hohes Sicherheitsrisiko darstellt und genauer untersucht werden sollte.
Anti-spyware	**Spyware-/Grayware-Übersicht für Desktops und Server** Der Spyware-/Grayware-Bericht enthält ausführliche Informationen über die auf Clients entdeckten Spyware- und Grayware-Bedrohungen, einschließlich der Anzahl entdeckter Vorfälle und der von WFBS durchgeführten Aktionen. Der Bericht enthält ein Tortendiagramm mit den Prozentsätzen jeder durchgeführten Anti-Spyware-Suchaktion.
	Die 5 Desktops/Server mit den meisten Spyware-/Grayware-Funden Der Bericht zeigt außerdem die fünf häufigsten Spyware- und Grayware-Bedrohungen und die fünf Desktops/Server mit den meisten entdeckten Spyware-/Grayware-Vorfällen. Weitere Informationen über die entdeckten Spyware- und Grayware-Bedrohungen erhalten Sie durch Klicken auf die Spyware-/Grayware-Namen. Auf einer neuen Seite des Webbrowsers wird die Trend Micro Website geöffnet, auf der zugehörige Informationen über die Spyware/Grayware angezeigt werden.

Berichtelement	Beschreibung
Anti-Spam-Übersicht (nur Advanced)	**Spam-Übersicht** Anti-Spam-Berichte geben an, wie viele Spam- und Phishing-Mails in allen durchsuchten Nachrichten entdeckt wurden, und listen außerdem alle gemeldeten Fehlalarme auf.
Vorausschauendes Maschinenlernen	**5 Programme, die am häufigsten gegen die Richtlinien für Vorausschauendes Maschinenlernen verstoßen**
	10 Computer, die am häufigsten gegen die Richtlinien für Vorausschauendes Maschinenlernen verstoßen
Web Reputation	**Die 10 Computer mit den häufigsten Verstößen gegen Web Reputation-Richtlinien**
URL-Kategorie	**Die 5 URL-Kategorierichtlinien, gegen die am häufigsten verstoßen wurde** Eine Liste der Website-Kategorien, die gegen die Richtlinie verstoßen und auf die am häufigsten zugegriffen wird.
	Die 10 Computer mit den häufigsten Verstößen gegen URL-Kategorierichtlinien
Verhaltensüberwachung	**Die 5 Programme mit den häufigsten Verstößen gegen Verhaltensüberwachungsrichtlinien**
	Die 10 Computer mit den häufigsten Verstößen gegen Verhaltensüberwachungsrichtlinien
Gerätesteuerung	**Die 10 Computer mit den häufigsten Verstößen gegen die Gerätesteuerungsrichtlinie**
Content-Filter-Übersicht (nur Advanced)	**Content-Filter-Übersicht** Content-Filter-Berichte enthalten die Gesamtzahl der vom Messaging Security Agent gefilterten Nachrichten.
	Die 10 häufigsten Verstöße gegen Content-Filter-Regeln Eine Liste der zehn häufigsten Verstöße gegen Content-Filter-Regeln. Optimieren Sie anhand dieser Liste die Einstellungen Ihrer Filter-Regeln.

Berichtelement	Beschreibung
Netzwerkvirus	**Die 10 häufigsten Netzwerkviren** Eine Liste der zehn Netzwerkviren, die der allgemeine Firewall-Treiber am häufigsten entdeckt. Klicken Sie auf den Namen des Virus, um eine neue Seite Ihres Webbrowsers zu öffnen und zur Trend Micro Virenenzyklopädie weitergeleitet zu werden. Dort erhalten Sie weiterführende Informationen.
	Die 10 am häufigsten angegriffenen Computer Eine Liste der Computer in Ihrem Netzwerk, die die meisten Virenvorfälle melden.

Wartungsaufgaben für Berichte und Protokolle durchführen

Prozedur

1. Navigieren Sie zu **Berichte** > **Wartung**.
2. Führen Sie folgende Aufgaben durch:

Task	Schritte
Maximale Anzahl für Berichte und Vorlagen festlegen	Sie können die Anzahl der Einzelberichte, der zeitgesteuerten Berichte (pro Vorlage) sowie die Anzahl der auf dem Security Server verfügbaren Vorlagen beschränken. Wenn die Anzahl überschritten wird, löscht der Security Server diese überzähligen Berichte/Vorlagen, beginnend mit dem Bericht/der Vorlage, der/die am längsten aufbewahrt wurde. a. Klicken Sie auf die Registerkarte **Berichte**. b. Geben Sie maximale Anzahl für Einzelberichte, zeitgesteuerte Berichte und Berichtvorlagen ein, die aufbewahrt werden soll.

Task	Schritte
Automatischen Löschvorgang für Protokolle konfigurieren	a. Klicken Sie auf die Registerkarte **Automatische Protokolllöschung**. b. Wählen Sie die Protokolltypen und geben Sie das Höchstalter für die Protokolle ein. Protokolle, die älter sind als dieser Wert, werden gelöscht.
Protokolle manuell löschen	a. Klicken Sie auf die Registerkarte **Manuelle Protokolllöschung**. b. Geben Sie für jeden Protokolltyp das Höchstalter für die Protokolle ein. Protokolle, die älter sind als dieser Wert, werden gelöscht. Geben Sie `0` ein, um alle Protokolle zu löschen. c. Klicken Sie auf **Löschen**.

3. Klicken Sie auf **Speichern**.

Kapitel 13

Administrative Aufgaben durchführen

In diesem Kapitel wird die Durchführung zusätzlicher administrativer Aufgaben wie das Anzeigen der Produktlizenz, das Arbeiten mit dem Plug-in Manager und die Deinstallation des Security Servers erläutert.

Das Kennwort der Web-Konsole ändern

Trend Micro empfiehlt die Verwendung sicherer Kennwörter für die Webkonsole. Ein sicheres Kennwort besteht aus mindestens acht Zeichen, die sich aus jeweils mindestens einem Großbuchstaben (A - Z), einem Kleinbuchstaben (a - z), einer Zahl (0 - 9) und einem Sonder- oder Interpunktionszeichen (!@#$%^&,.:;?) zusammensetzen. Sichere Kennwörter dürfen nicht mit dem Benutzernamen identisch sein und diesen auch nicht enthalten. Außerdem dürfen sie nicht aus Vornamen, Nachnamen, Geburtsdatum oder sonstigen leicht zu ermittelnden Daten des Benutzers bestehen.

Prozedur

1. Navigieren Sie zu **Administration** > **Kennwort**.
2. Aktualisieren Sie folgende Optionen bei Bedarf:
   - **Altes Kennwort**
   - **Neues Kennwort**
   - **Kennwort bestätigen**: Geben Sie das neue Kennwort zur Bestätigung erneut ein.
3. Klicken Sie auf **Speichern**.

Mit dem Plug-in Manager arbeiten

Der Plug-in Manager zeigt die Programme für den Security Server und die Agents in der Webkonsole an, sobald diese verfügbar sind. Sie können die Programme dann über die Webkonsole installieren und verwalten und die Plug-ins auf die Agents verteilen. Laden Sie den Plug-in Manager unter **Administration** > **Plug-Ins** herunter und installieren Sie ihn. Nach der Installation können Sie nach verfügbaren Plug-ins suchen. Weitere

Informationen finden Sie in der Dokumentation des Plug-in Managers und der Plug-in-Programme.

Produktlizenz verwalten

Über das Fenster Produktlizenz können Sie Ihre Lizenz verlängern oder aktualisieren oder Details zu Ihrer Produktlizenz anzeigen.

Das Fenster Produktlizenz enthält Einzelheiten zu Ihrer Lizenz. Je nach den während der Installation gewählten Optionen verfügen Sie über eine lizenzierte Vollversion oder eine Testversion. In jedem Fall haben Sie unter der Lizenz Anspruch auf einen Wartungsvertrag. Nach Ablauf des Wartungsvertrags ist der Schutz der Clients im Netzwerk stark eingeschränkt. Im Fenster Produktlizenz können Sie sehen, wann die Lizenz abläuft, und sie vor dem Ablaufdatum verlängern.

Hinweis

Die Lizenzen für die unterschiedlichen Komponenten der Trend Micro Produkte können regional unterschiedlich sein. Nach der Installation erscheint eine Übersicht der Komponenten, die Sie mit Ihrem Registrierungsschlüssel/Aktivierungscode verwenden dürfen. Bei weiteren Fragen zu den Komponenten, für die Sie Lizenzen erworben haben, wenden Sie sich bitte an Ihren zuständigen Vertriebspartner.

Lizenzverlängerung

Sie können eine Verlängerung einer oder ein Upgrade auf eine lizenzierte Vollversion von Worry-Free Business Security vornehmen, indem Sie erneut einen Wartungsvertrag abschließen. Für die lizenzierte Vollversion ist ein Aktivierungscode erforderlich.

Sie haben zwei Möglichkeiten, um die Produktlizenz zu verlängern:

- Navigieren Sie auf der Webkonsole zum Fenster Live-Status und befolgen Sie die Anweisungen im Fenster. Die Anweisungen werden 60 Tage vor und 30 Tage nach Ablauf der Lizenz angezeigt.

- Wenden Sie sich an einen Trend Micro Vertriebspartner oder Reseller, um den Lizenzvertrag zu verlängern.

  Reseller können Ihre Kontaktdaten in einer Datei auf dem Security Server speichern. Überprüfen Sie die Datei unter:

  `{Installationsordner des Security Servers}\PCCSRV\Private\contact_info.ini`

  Hinweis

  `{Installationsordner des Security Servers}` ist normalerweise `C:\Programme\Trend Micro\Security Server`.

  Ein Trend Micro Mitarbeiter aktualisiert Ihre Registrierungsinformationen über die Trend Micro Produktregistrierung.

  Der Security Server fragt den Produktregistrierungsserver ab und erhält das neue Ablaufdatum direkt von diesem Server. Zur Verlängerung der Lizenz muss kein neuer Aktivierungscode eingegeben werden.

Eine neue Lizenz aktivieren

Der Worry-Free Business Security Aktivierungscode hängt von Ihrem Lizenztyp ab.

TABELLE 13-1. Aktivierungscode für die jeweilige Lizenzart

LIZENZART	AKTIVIERUNGSCODE
Lizenzierte Vollversion von Worry-Free Business Security Standard	CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx
Lizenzierte Vollversion von Worry-Free Business Security Advanced	CM-xxxx-xxxxx-xxxxx-xxxxx-xxxxx

Hinweis

Weitere Informationen zum Aktivierungscode finden Sie auf der Trend Micro Support-Website unter:

http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326

Im Fenster Produktlizenz können Sie die Lizenzart ändern, indem Sie einen neuen Aktivierungscode eingeben.

1. Navigieren Sie zu **Administration** > **Produktlizenz**.
2. Klicken Sie auf **Neuen Code eingeben**.
3. Geben Sie den neuen Aktivierungscode in das entsprechende Feld ein.
4. Klicken Sie auf **Aktivieren**.

Einstellungen zu Produkt-Updates konfigurieren

Konfigurieren Sie Worry-Free Business Security, um Produkt-Updates zu automatisieren.

Prozedur

1. Navigieren Sie zu **Administration** > **Produkt-Update**.

Die Registerkarte **Einstellungen** wird angezeigt.

2. Wählen Sie unter **Einstellungen für Updates**, **Downloads von Produkt-Update aktivieren** aus.

3. Geben Sie die Aktion an, die ausgeführt werden soll, wenn ein neues Update-Paket verfügbar ist.

- **Herunterladen**: lädt das Update-Paket automatisch basierend auf dem konfigurierten Zeitplan in den Download-Ordner herunter.
- **Herunterladen und installieren** : lädt das Update-Paket automatisch basierend auf dem konfigurierten Zeitplan herunter und installiert es.

4. Geben Sie an, wann die Aktion ausgeführt werden soll.

Hinweis

Es kann einige Zeit dauern, bis der Installationsvorgang abgeschlossen ist und der Security Server neu gestartet wird. Wählen Sie einen Zeitpunkt, der minimale Auswirkungen auf die Installation des Update-Pakets hat.

5. Klicken Sie auf **Speichern**.

Konfigurieren von Benachrichtigungen über Produkt-Updates

Worry-Free Business Security kann Benutzer über Produkt-Updates informieren, sobald neue Versionen, Service Packs oder Patches zur Verfügung stehen. Sie können die folgenden Typen von Benachrichtigungen über Produkt-Updates einrichten:

- Security Agent: Zeigt eine Benachrichtigung in der Nähe des Benachrichtigungsbereichs auf dem Endpunkt an.
- E-Mail

Prozedur

1. Navigieren Sie zu **Administration** > **Produkt-Update**.
2. Klicken Sie auf **Benachrichtigungen**.
3. Konfigurieren Sie den Bereich **Security Agent-Benachrichtigung**, um Benachrichtigungen vom Security Agent zu erhalten.
   a. Klicken Sie auf **Hinzufügen**.
   b. Wählen Sie die Security Agents in der Liste aus.
   c. Klicken Sie auf **Speichern**.
4. Geben Sie die Empfänger im Bereich **E-Mail-Benachrichtigung** an, um E-Mail-Benachrichtigungen über Produkt-Updates zu erhalten.

Hinweis

Um E-Mail-Benachrichtigungen zu erhalten, müssen Sie die Registerkarte **SMTP** in **Administration** > **Allgemeine Einstellungen** konfigurieren.

5. Klicken Sie auf **Speichern**.

Am Smart Feedback Programm teilnehmen

Weitere Informationen über Smart Feedback finden Sie unter *Smart Feedback auf Seite 1-6*.

Prozedur

1. Navigieren Sie zu **Administration** > **Smart Protection Network**.
2. Klicken Sie auf **Trend Micro Smart Feedback aktivieren**.
3. Um Informationen über potenzielle Sicherheitsbedrohungen in den Dateien auf Ihren Client-Computern zu senden, aktivieren Sie das Kontrollkästchen **Feedback von verdächtigen Programmdateien aktivieren**.

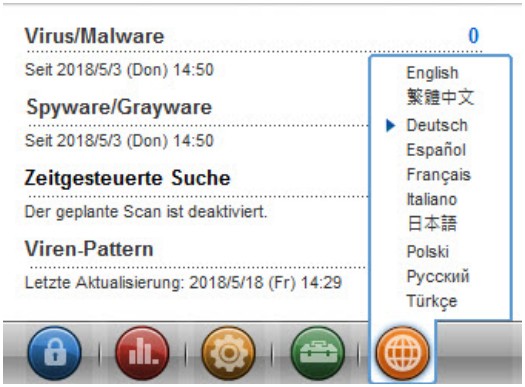
Hinweis

Die Dateien, die an Smart Feedback gesendet werden, enthalten keine Benutzerdaten und werden nur zur Bedrohungsanalyse übertragen.

4. Um Trend Micro beim Verständnis Ihre Unternehmens zu unterstützen, wählen Sie die **Branche**.
5. Klicken Sie auf **Speichern**.

Sprache der Benutzeroberfläche des Agents ändern

Die Sprache, die auf der Benutzeroberfläche des Agents verwendet wird, stimmt mit der Sprache überein, die im Betriebssystem des Clients konfiguriert ist. Benutzer können die Sprache über die Benutzeroberfläche des Agents ändern.



Programmeinstellungen speichern und wiederherstellen

Sie können eine Kopie der Datenbank des Security Servers und wichtige Konfigurationsdateien speichern, um ein Rollback des Security Servers durchzuführen. Diese Lösung bietet sich an, wenn Schwierigkeiten auftreten und Sie den Security Server neu installieren oder eine frühere Konfiguration verwenden möchten.

Prozedur

1. Beenden Sie den Trend Micro Security Server Master-Dienst.

2. Kopieren Sie folgende Dateien und Ordner manuell aus dem Verzeichnis an einen anderen Speicherort:

Warnung!

Verwenden Sie hierfür keine Tools oder Anwendungen für das Erstellen von Sicherungskopien.

`<Installationspfad des Security Server>\PCCSRV`

- `ofcscan.ini`: Diese Datei enthält allgemeine Einstellungen.
- `Ous.ini`:: Diese Datei enthält die Liste der Update-Adressen für die Verteilung von Antiviren-Komponenten.
- `Persönlicher` Ordner:Dieser Ordner enthält die Einstellungen der Firewall und der Update-Adressen.
- `Pccnt\Common\OfcPfw.dat`: Diese Datei enthält die Einstellungen der Firewall.
- `Download\OfcPfw.dat`: Diese Datei enthält die Einstellungen zur Verteilung der Firewall.
- `Protokoll`ordner: Dieser Ordner enthält Systemereignisse und das Verbindungsprotokoll.
- `Viren`ordner: Der Ordner, in den WFBS infizierte Dateien in Quarantäne verschiebt.
- `HTTDB`-Ordner: Enthält die WFBS-Datenbank.

3. Deinstallieren Sie den Security Server. Weitere Informationen finden Sie unter *Den Security Server deinstallieren auf Seite 13-10*.

4. Führen Sie eine Neuinstallation durch. Siehe Worry-Free Business Security *Installations- und Upgrade-Handbuch*.

5. Nach dem Installationsvorgang müssen Sie den Trend Micro Security Server Master-Dienst auf dem Zielcomputer beenden.

6. Aktualisieren Sie die Viren-Pattern-Version über die Sicherungsdatei:

a. Laden Sie die aktuelle Pattern-Version vom neuen Server herunter.

```
<Installationspfad des Security Server>\PCCSRV\Private
\component.ini. [6101]

ComponentName=Viren-Pattern

Version=xxxxxx 0 0
```

b. Aktualisieren Sie die Version der Viren-Pattern in der gesicherten Datei:

```
\Private\component.ini
```

Hinweis

Wenn Sie den Installationspfad des Security Servers ändern, müssen Sie diese Informationen in den Sicherungsdateien `ofscan.ini` und `\private\ofcserver.ini` aktualisieren.

7. Überschreiben Sie im Ordner `PCCSRV` die Worry-Free Business Security Datenbank sowie die betreffenden Dateien und Ordner auf dem Zielcomputer mit den erstellten Sicherungskopien.
8. Starten Sie den Trend Micro Security Server Master-Dienst neu.

Den Security Server deinstallieren

Beim Deinstallieren des Security Servers wird auch der Suchserver deinstalliert.

Worry-Free Business Security verwendet ein Deinstallationsprogramm, mit dem der Trend Micro Security Server sicher vom Computer entfernt werden kann. Entfernen Sie den Agent von allen Clients, bevor Sie den Security Server deinstallieren.

Beim Entfernen des Trend Micro Security Servers wird der Agent nicht deinstalliert. Vor der Deinstallation des Trend Micro Security Servers müssen alle Agents von einem Administrator deinstalliert oder auf einen

anderen Security Server verschoben werden. Weitere Informationen finden Sie unter *Agents entfernen auf Seite 3-40*.

Prozedur

1. Klicken Sie auf dem Computer, auf dem Sie den Server installiert haben, auf **Start** > **Systemsteuerung** > **Software**.
2. Wählen Sie **Trend Micro Security Server** aus, und klicken Sie anschließend auf **Ändern/Entfernen**.

   Ein Bestätigungsfenster wird angezeigt.
3. Klicken Sie auf **Weiter**.

   Der Master Uninstaller (das Programm zur Deinstallation des Servers) fordert Sie zur Eingabe des Administratorkennworts auf.
4. Geben Sie das Administratorkennwort in das Textfeld ein, und klicken Sie auf **OK**.

   Der Master Uninstaller beginnt mit dem Entfernen der Serverdateien. Nach der Deinstallation des Security Server wird eine Bestätigungsmeldung angezeigt.
5. Klicken Sie auf **OK**, um das Deinstallationsprogramm zu schließen.

Kapitel 14

Management-Tools verwenden

In diesem Kapitel wird die Verwendung der Administrations- und Client-Tools und Add-ins beschrieben.

Tool-Typen

Worry-Free Business Security enthält mehrere Tools, mit denen Sie z. B. den Server konfigurieren, die Clients verwalten und viele andere Aufgaben einfach und schnell durchführen können.

Hinweis

Administrative Tools und Client-Tools können nicht an der Webkonsole gestartet werden. Add-ins können von der Webkonsole heruntergeladen werden.

Hinweise zur Verwendung der Tools finden Sie in den folgenden Abschnitten.

Die Tools lassen sich in drei Kategorien unterteilen:

- **Administrator-Tools**
  - **Anmeldeskript-Setup** (`SetupUsr.exe`): Automatisiert die Installation des Security Agents. Weitere Informationen finden Sie unter *Mit dem Anmeldeskript-Setup installieren auf Seite 3-12*.
  - **Vulnerability Scanner** (`TMVS.exe`): Findet ungeschützte Computer im Netzwerk. Weitere Informationen finden Sie unter *Mit dem Vulnerability Scanner installieren auf Seite 3-22*.
  - **Remote Manager Agent**: Ermöglicht Resellern die Verwaltung von Worry-Free Business Security über eine zentralisierte Webkonsole. Weitere Informationen finden Sie unter *Den Trend Micro Remote Manager Agent installieren (Customer Licensing Portal Benutzer) auf Seite 14-4*.
  - **Trend Micro Disk Cleaner**: Löscht nicht benötigte Worry-Free Business Security-Sicherungsdateien, Protokolldateien und ungenutzte Pattern-Dateien. Weitere Informationen finden Sie unter *Festplattenspeicher sparen auf Seite 14-15*.
  - **Scan Server Database Mover**: Verschiebt die Scan Server Datenbank sicher auf eine andere Festplatte. Weitere Informationen finden Sie unter *Die Scan Server Datenbank verschieben auf Seite 14-18*.

- **Client-Tools**
  - **Client Packager** (`ClnPack.exe`): Erstellt eine selbstextrahierende Datei, die den Security Agent und die Komponenten enthält. Weitere Informationen finden Sie unter *Mit Client Packager installieren auf Seite 3-14*.
  - **Restore Encrypted Virus and Sypware** (`VSEncode.exe`): Öffnet infizierte Dateien, die von Worry-Free Business Security entschlüsselt wurden. Weitere Informationen finden Sie unter *Verschlüsselte Dateien wiederherstellen auf Seite 14-18*.
  - **Client Mover Tool** (`ipXfer.exe`): Überträgt Agents von einem Security Server auf einen anderen. Weitere Informationen finden Sie unter *Agents verschieben auf Seite 4-12*.
  - **Regenerate the Security Agent ClientID** (`WFBS_WIN_All_ReGenID.exe`): Erstellt die Security Agent ClientID neu. Dabei wird beachtet, ob es sich bei dem Agent um einen geklonten Computer oder eine virtuelle Maschine handelt. Weitere Informationen finden Sie unter *ReGenID Tool verwenden auf Seite 14-23*.
- **Add-ins**: Ermöglichen es Administratoren, Systemstatus- und Sicherheitsinformationen in Echtzeit auf unterstützten Windows Betriebssystemen anzuzeigen. Dabei handelt es sich um die gleichen ausführlichen Informationen, die im Fenster Live-Status angezeigt werden. Weitere Informationen finden Sie unter *SBS und EBS Add-ins verwalten auf Seite 14-24*.

Hinweis

Einige Tools aus den Vorgängerversionen sind in dieser Version von Worry-Free Business Security nicht enthalten. Wenn Sie diese Tools benötigen, wenden Sie sich bitte an den Technischen Support von Trend Micro.

Trend Micro Remote Manager Agent

Mit dem Trend Micro Remote Manager Agent können Reseller oder Partner Worry-Free Business Security mit dem Trend Micro Remote Manager verwalten. Sie können den Remote Manager Agent nach Abschluss der Security Manger Installation auf dem Security Server installieren oder den Remote Manager Agent zu einem späteren Zeitpunkt installieren.

Installationsvoraussetzungen:

- Remote Manager Agent GUID (Globally Unique Identifier)
- Eine aktive Internet-Verbindung
- 50MB freier Festplattenspeicher

Befolgen Sie die Anweisungen in einem der folgenden Abschnitte:

- *Den Trend Micro Remote Manager Agent installieren (Customer Licensing Portal Benutzer) auf Seite 14-4*
- *Den Trend Micro Remote Manager Agent installieren (Licensing Management Platform Benutzer) auf Seite 14-6*

Den Trend Micro Remote Manager Agent installieren (Customer Licensing Portal Benutzer)

Prozedur

1. Beziehen Sie die Remote Manager Agent GUID.
   a. Navigieren Sie in der Remote Manager Webkonsole zu **Kunden**.
   b. Klicken Sie in der Spalte **Unternehmen** auf den Kunden.
   c. Wählen Sie auf der Registerkarte **Produkte** das Produkt Worry-Free Business Security aus.
   d. Kopieren Sie die GUID.

2. Wechseln Sie zum Security Server und navigieren Sie zum Installationsordner:`PCCSRV\Admin\Utility\RmAgent`. Starten Sie die Anwendung `TMRMAgentforWFBS.exe`.

   Beispiel:`C:\Programme\Trend Micro\Security Server\PCCSRV\Admin\Utility\RmAgent\TMRMAgentforWFBS.exe`

   Hinweis

   Überspringen Sie diesen Schritt, wenn Sie die Installation über das Setup-Fenster des Security Servers starten.

3. Lesen Sie die Lizenzvereinbarung im Trend Micro Remote Manager Agent Setup Assistenten. Wenn Sie sich mit den Bedingungen einverstanden erklären, klicken Sie auf **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** und anschließend auf **Weiter**.

4. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie ein zertifizierter Partner sind.

5. Wählen Sie **Ich habe bereits ein Trend Micro Remote Manager Konto und möchte den Agent installieren** aus und klicken Sie auf **Weiter**.

6. Legen Sie Ihr Szenario fest.

Szenario	Schritte
Neuer Kunde	a. Wählen Sie **Mit einem neuen Kunden verbinden** aus. b. Klicken Sie auf **Weiter**. Geben Sie die Kundendaten ein. **Hinweis** Wenn der Kunde bereits in der TMRM Konsole vorhanden ist und Sie die oben aufgeführte Option für die Verbindung mit einem neuen Kunden verwenden, werden in der TMRM Netzwerkstruktur zwei Kunden mit demselben Namen angezeigt. Verwenden Sie die unten stehende Methode, um dies zu verhindern.
Bestehender Kunde	a. Wählen Sie **Dieses Produkt ist bereits im Remote Manager vorhanden**.

Szenario	Schritte
	Hinweis WFBS muss bereits zur TMRM Konsole hinzugefügt worden sein. Weitere Hinweise finden Sie in der TMRM Dokumentation. b. Geben Sie die GUID ein.

7. Klicken Sie auf **Weiter**.
8. Wählen Sie **Region** und **Protokoll** aus, und geben Sie die Proxy-Angaben ein, falls erforderlich.
9. Klicken Sie auf **Weiter**.

   Das Fenster "Installationsspeicherort" wird angezeigt.
10. Klicken Sie auf **Weiter**, um den Standardspeicherort zu verwenden.
11. Klicken Sie auf **Fertig stellen**.

    Bei erfolgreicher Installation und korrekten Einstellungen wird der Remote Manager Agent automatisch beim Trend Micro Remote Manager Server registriert. Der Remote Manager Agent sollte jetzt in der Remote Manager Webkonsole als 'online' angezeigt werden.

Den Trend Micro Remote Manager Agent installieren (Licensing Management Platform Benutzer)

Prozedur

1. Beziehen Sie den Worry-Free Business Security Aktivierungscode.
   a. Navigieren Sie in der Remote Manager Webkonsole zu **Kunden**.
   b. Klicken Sie in der Spalte **Unternehmen** auf den Kunden.
   c. Wählen Sie auf der Registerkarte **Produkte** das Produkt Worry-Free Business Security aus.

d. Kopieren Sie den Aktivierungscode.

2. Aktualisieren Sie die Lizenzinformationen für Worry-Free Business Security.

   a. Navigieren Sie in der Worry-Free Business Security Webkonsole zu **Administration** > **Produktlizenz**.

   b. Klicken Sie unter **Lizenzinformationen** auf **Neuen Code eingeben**.

   c. Fügen Sie den Aktivierungscode in das Feld **Neuer Aktivierungscode** ein.

   d. Klicken Sie auf **Aktivieren**.

   e. Klicken Sie auf **Lizenzinformationen aktualisieren**.

3. Wechseln Sie zum Security Server und navigieren Sie zum Installationsordner:`PCCSRV\Admin\Utility\RmAgent`. Starten Sie die Anwendung `TMRMAgentforWFBS.exe`.

   Beispiel:`C:\Programme\Trend Micro\Security Server\PCCSRV\Admin\Utility\RmAgent\TMRMAgentforWFBS.exe`

   Hinweis

   Überspringen Sie diesen Schritt, wenn Sie die Installation über das Setup-Fenster des Security Servers starten.

4. Wählen Sie **Ich habe bereits ein Trend Micro Remote Manager Konto und möchte den Agent installieren** aus und klicken Sie auf **Weiter**.

5. Wählen Sie **Mit vorhandener Licensing Management Platform Lizenz verknüpfen** aus und klicken Sie auf **Weiter**.

6. Geben Sie die Anmeldedaten für das Remote Manager Konto an und klicken Sie auf **Weiter**.

7. Geben Sie bei Bedarf die Angaben zum Proxy-Server an und klicken Sie auf **Weiter**.

8. Geben Sie bei Bedarf den Installationsordner an und klicken Sie auf **Weiter**.

9. Klicken Sie auf **Fertig stellen**.

   Bei erfolgreicher Installation und korrekten Einstellungen wird der Remote Manager Agent automatisch beim Trend Micro Remote Manager Server registriert. Der Remote Manager Agent sollte jetzt in der Remote Manager Webkonsole als 'online' angezeigt werden.

Agents über den verwalteten Server verwalten

Dieser Abschnitt enthält Informationen zum Verwalten von Agents über den verwalteten Server.

Agent-Statusmeldungen

Auf dem verwalteten Server zeigt der Agent eines der folgenden Task-Leistensymbole an:

TABELLE 14-1. Symbole der Task-Leiste

SYMBOL	BESCHREIBUNG
	Ein grünes Symbol gibt an, dass der Agent mit dem Remote Manager Kommunikationsserver verbunden ist. Der Agent wird ordnungsgemäß ausgeführt.
	Ein rotes Symbol gibt an, dass der Agent nicht mit dem Remote Manager Kommunikationsserver verbunden ist oder dass die Version des Agents nicht mit der Serverversion übereinstimmt und aktualisiert werden muss.
	Ein Symbol mit einem roten Pfeil gibt an, dass der Agent vom Remote Manager abgemeldet wurde.
	Ein Symbol mit einem roten "X" bedeutet, dass der Agent deaktiviert wurde.

Die Agent-GUID auf dem verwalteten Server ändern

Falls Sie bei der Remote Manager Agent Installation eine falsche GUID (Globally Unique Identifier) eingegeben haben, löschen Sie den Agent und

installieren Sie Ihn erneut mit der richtigen GUID. Wenn Sie diesen Vorgang nicht ausführen können, können Sie Folgendes tun:

Prozedur

1. Wechseln Sie zu `C:\Programme\Trend Micro\TMRMAgentForWFBS`.
2. Öffnen Sie die Datei `AgentSysConfig.xml` in einem Texteditor.
3. Suchen Sie die GUID zwischen den Parametern `<AgentGUID>` und `</AgentGUID>`.
4. Bearbeiten Sie die GUID, und speichern Sie die Datei.
5. Öffnen Sie die Datei `csmSysConfig.xml` im selben Ordner mit einem Texteditor.
6. Suchen Sie die GUID zwischen den Parametern `<ProductGUID>` und `</ProductGUID>`.
7. Bearbeiten Sie die GUID, und speichern Sie die Datei.
8. Klicken Sie in der Taskleiste mit der rechten Maustaste auf das Remote Manager Agent Symbol und klicken Sie dann auf **Dienst neu starten**.

Agent-Konfigurationstool verwenden

Mit dem Agent Konfigurationstool können Änderungen an den Konfigurationseinstellungen des Remote Manager Agent vorgenommen werden.

Navigieren Sie zu **Start** > **Programme** > **Trend Micro Remote Manager Agent** > **Agent Configuration Tool** oder klicken Sie mit der rechten Maustaste auf das Task-Leistensymbol und klicken Sie dann auf **Konfigurieren**.

Weitere Informationen finden Sie unter *Agent-Konfiguration auf Seite 14-10*.

Agent-Konfiguration

Agent-Konfigurationsmenü

Um den Agent zu konfigurieren, klicken Sie mit der rechten Maustaste auf das Task-Leistensymbol und öffnen Sie das folgende Menü:

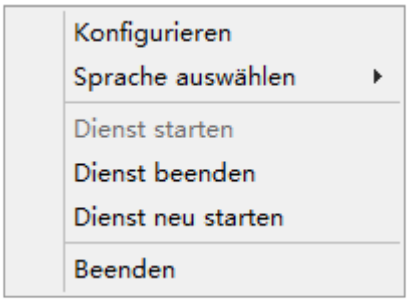


ABBILDUNG 14-1. Kontextmenü des Agent-Konfigurationstools

Die folgenden Elemente werden angezeigt:

- **Konfigurieren**: Öffnet das Agent-Konfigurationsfenster.
- **Sprache auswählen**: Zusätzlich zu anderen möglichen Sprachen ist "Englisch" immer verfügbar.
- **Dienst**: Starten, Beenden, Neu starten.
- **Beenden**: Durch das Beenden des Tools wird der Remote Manager Dienst nicht beendet. Es wird nur das Konfigurationstool geschlossen und das Symbol aus der Task-Leiste entfernt. Das Tool kann jederzeit erneut gestartet werden.

Hauptdialog des Konfigurationstools

Klicken Sie mit der rechten Maustaste auf das Task-Leistensymbol, und klicken Sie auf **Konfigurieren** im Agent-Konfigurationsmenü, um die Registerkarte **Allgemein** des Agent-Konfigurationstools zu öffnen.

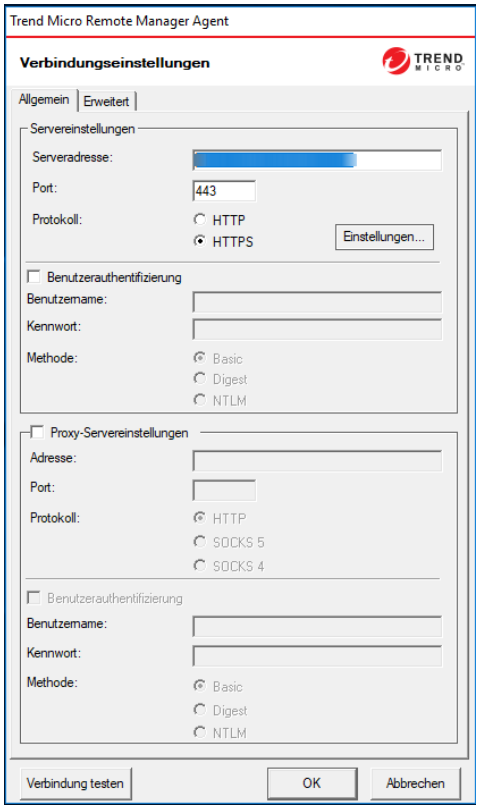


ABBILDUNG 14-2. Registerkarte "Allgemein" des Agent-Konfigurationstools

Die folgenden Bereiche des Agent-Konfigurationsfensters sind die einzigen zurzeit relevanten Bereiche dieses Tools.

- **Servereinstellungen**: Konfigurieren Sie die Serverkommunikation mit den folgenden Einstellungen:

- **Serveradresse**: Der vollqualifizierter Domänenname (FQDN) des Remote Manager Kommunikationsservers. Der FQDN ist je nach Region unterschiedlich. Wenden Sie sich an Ihren Support-Mitarbeiter, wenn Sie die Serveradresse ändern müssen.
- **Port**: Der Port, den der Remote Manager Server für die Kommunikation mit dem Agent verwendet. Dieser sollte 80 für HTTP und 443 für HTTPS sein.
- **Protokoll**: Das Protokoll, das für die Kommunikation zwischen Server und Agent verwendet wird.

Wichtig

Trend Micro empfiehlt, die **Serveradresse** oder den **Port** nicht zu ändern, es sei denn, Sie werden von Ihrem Support-Anbieter dazu aufgefordert.

- **Proxy-Server-Einstellungen**: Aktivieren Sie diesen Bereich, indem Sie das Kontrollkästchen **Proxy-Servereinstellungen** aktivieren, wenn das Netzwerk des Benutzers für die Kommunikation mit dem Remote Manager Server einen Proxy benötigt.
  - **Adresse**: Die IP-Adresse des Proxy-Servers.
  - **Port**: Der Port des Proxy-Servers.
  - **Protokoll**
- **Schaltfläche zum Testen der Verbindung**: Mit Hilfe der Schaltfläche **Verbindung testen** wird die Kommunikation zwischen dem Agent und dem Remote Manager Server getestet. Verwenden Sie diese Funktion, um die Verbindung zum Kommunikationsserver allgemein zu testen. Falls der Test fehlschlägt (wenn das Tool keine Verbindung mit dem Server herstellen kann, erscheint ein Popup-Dialogfeld), liegen möglicherweise allgemeine Probleme beispielsweise bei Adresse und Port des Kommunikationsservers oder des Proxy-Servers vor.

Agent-Einstellungen sichern und wiederherstellen

Falls Sie innerhalb von drei Tagen den Agent mit derselben GUID deinstallieren und dann erneut installieren müssen, behalten Sie die Agent-

Einstellungen bei, um Datenüberlappungen zu vermeiden. Sichern Sie zu diesem Zweck die Konfigurationsdateien manuell, und ersetzen Sie dann nach der Neuinstallation des Agents die Konfigurationsdateien durch die Sicherungskopien.

Einstellungen sichern

Prozedur

1. Klicken Sie auf dem verwalteten Server mit der rechten Maustaste auf das Agent-Symbol in der Task-Leiste, und klicken Sie auf **Dienst beenden**, um den Agent-Dienst zu stoppen.
2. Kopieren Sie alle Dateien des Typs `.xml`, `.dat` und `.ini` aus dem Installationsordner: `C:\Programme\Trend Micro\TMRMAgentForWFBS` oder `C:\Programme (x86)\Trend Micro\TMRMAgentForWFBS`.
   - `XML`-Dateien
     - `csmSysConfig.xml`
     - `csmLocalConfig.xml`
     - `csmLogDef.xml`
     - `AgentWorkConfig.xml`
     - `AgentSysConfig.xml`
     - `AgentStatus.xml`
     - `AgentLocalConfig.xml`
   - `DAT`-Dateien
     - `MSA.dat`
     - `logBuf.dat`
     - `group.dat`
     - `CSA.dat`

    - `CriticalVA.dat`
  - `INI`-Dateien
    - `csmStatusData.ini`

3. Kopieren Sie alle Dateien aus dem Ordner `\Cache`.
4. Starten Sie den Agent-Dienst neu.

Einstellungen wiederherstellen

Prozedur

1. Entfernen Sie den Agent lokal.

   Hinweis

   Wenn der Agent lokal entfernt wird, wird er beim Remote Manager abgemeldet. Dadurch werden automatisch alle mit dem Agent verknüpften Daten gelöscht. Wenn Sie verhindern möchten, dass sich der Agent abmeldet, ändern Sie vor der Deinstallation des Agents den Wert der Serveradresse in der Agent-Benutzeroberfläche.

2. Installieren Sie den Agent neu. Stellen Sie sicher, dass Sie dieselbe GUID wie in der Datei `agentSysConfig.xml` verwenden.
3. Klicken Sie auf dem verwalteten Server mit der rechten Maustaste auf das Agent-Symbol in der Task-Leiste, und klicken Sie auf **Dienst beenden**, um den Agent-Dienst zu stoppen.
4. Ersetzen Sie die Konfigurationsdateien durch die Sicherungsdateien.
5. Klicken Sie mit der rechten Maustaste auf das Agent-Symbol in der Task-Leiste, und klicken Sie auf **Dienst starten**, um den Agent-Dienst neu zu starten.

Festplattenspeicher sparen

Führen Sie das Tool Disk Cleaner aus, um Festplattenspeicher auf dem Security Server und auf Clients zu sparen.

Disk Cleaner auf dem Security Server ausführen

Vorbereitungen

Um Speicherplatz zu sparen, identifiziert und löscht das Tool 'Disk Cleaner' (`TMDiskCleaner.exe`) ungenutzte Sicherungs-, Protokoll- und Pattern-Dateien in den folgenden Verzeichnissen:

- `{Security Agent}\AU_Data\AU_Temp\*`
- `{Security Agent}\Reserve`
- `{Security Server}\PCCSRV\TEMP\* (außer verborgene Dateien)`
- `{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\* (löscht Dateien in der Quarantäne, die älter als zwei Wochen sind, außer NOTVIRUS)`
- `{Security Server}\PCCSRV\ssaptpn.xxx (behält nur die neueste Pattern-Datei bei))`
- `{Security Server}\PCCSRV\lpt$vpn.xxx (behält nur die drei neuesten Pattern-Dateien bei)`
- `{Security Server}\PCCSRV\icrc$oth.xxx (behält nur die drei neuesten Pattern-Dateien bei)`
- `{Security Server}\DBBackup\* (behält nur die zwei neuesten Unterordner bei)`

- `{Messaging Security Agent}\AU_Data\AU_Temp\*`
- `{Messaging Security Agent}\Debug\*`
- `{Messaging Security Agent}\engine\vsapi\latest\pattern\*`

Prozedur

1. Wechseln Sie auf dem Security Server in das folgende Verzeichnis:

   `{Installationsordner des Servers}\PCCSRV\Admin\Utility\`

2. Doppelklicken Sie auf **TMDiskCleaner.exe**.

   Der Trend Micro Worry-Free Business Security Disk Cleaner wird angezeigt.

   Hinweis

   Dateien können nicht wiederhergestellt werden.

3. Klicken Sie auf **Dateien löschen**, um nach ungenutzten Sicherungs-, Protokoll- und Pattern-Dateien zu suchen.

Disk Cleaner auf dem Security Server mit der Befehlszeilenschnittstelle ausführen

Prozedur

1. Öffnen Sie auf dem Security Server die Eingabeaufforderung.
2. Geben Sie in der Eingabeaufforderung folgenden Befehl ein:

   `TMDiskCleaner.exe [/hide] [/log] [/allowundo]`

   - `/hide`: Führt das Tool als Hintergrundprozess aus.
   - `/log`: Speichert ein Protokoll des Vorgangs unter DiskClean.log im aktuellen Ordner.

Hinweis

`/log` ist nur verfügbar, wenn `/hide` verwendet wird.

- `/allowundo`: Verschiebt die Dateien in den Papierkorb, anstatt sie dauerhaft zu löschen.

3. Um Disk Cleaner regelmäßig auszuführen, konfigurieren Sie mit Hilfe der Windows Funktion "Geplante Tasks" einen neuen Task. Weitere Informationen dazu finden Sie in der Windows Dokumentation.

Festplattenspeicher auf Clients sparen

Prozedur

- Auf Desktops/Servern mit Security Agents:
  - Löschen Sie Dateien in Quarantäne.
  - Löschen Sie Protokolldateien.
  - Führen Sie das Windows Disk Cleanup Utility aus.
- Auf Microsoft Exchange Servern mit Messaging Security Agents:
  - Löschen Sie Dateien in Quarantäne.
  - Löschen Sie Protokolldateien.
  - Führen Sie das Windows Disk Cleanup Utility aus.
  - Säubern Sie die Archiv-Protokolle.
  - Säubern Sie Sicherungsdateien.
  - Prüfen Sie die Größe der Microsoft Exchange Datenbank oder der Transaktionsprotokolle.

Die Scan Server Datenbank verschieben

Wenn der Speicherplatz auf der Festplatte, auf dem der Scan Server installiert ist, nicht ausreicht, können Sie die Scan Server Datenbank mit dem Scan Server Database Mover Tool auf eine andere Festplatte verschieben.

Achten Sie darauf, dass der Security Server Computer über mehrere Festplatten verfügt und auf der neuen Festplatte mindestens 3 GB Speicherplatz frei sind. Zugeordnete Laufwerke sind nicht zulässig. Verschieben Sie die Datenbank auf keinen Fall manuell oder mit Hilfe anderer Tools.

Prozedur

1. Navigieren Sie auf dem Security Server Computer zu `<Security Server-Installationsordner>\PCCSRV\Admin\Utility`.
2. Starten Sie die Datei `ScanServerDBMover.exe`.
3. Klicken Sie auf **Ändern**.
4. Klicken Sie auf **Durchsuchen** und navigieren Sie zum Zielverzeichnis auf der anderen Festplatte.
5. Klicken Sie nach dem Verschieben der Datenbank auf **OK** und **Abschließen**.

Verschlüsselte Dateien wiederherstellen

Um zu verhindern, dass eine infizierte Datei geöffnet wird, wird die betreffende Datei während der folgenden Aktionen von Worry-Free Business Security verschlüsselt:

- Bevor eine Datei in Quarantäne verschoben wird
- Wenn vor der Säuberung eine Sicherheitskopie der Datei angefertigt wird

Worry-Free Business Security enthält ein Tool zum Entschlüsseln und anschließendem Wiederherstellen der Datei, falls Sie Informationen von der Datei abrufen müssen. Worry-Free Business Security kann die folgenden Dateien entschlüsseln und wiederherstellen:

TABELLE 14-2. Dateien, die Worry-Free Business Security entschlüsseln und wiederherstellen kann

DATEI	BESCHREIBUNG
Dateien in Quarantäne auf dem Client	Diese Dateien befinden sich in den folgenden Verzeichnissen: • `<Security Agent-Installationsordner>\SUSPECT\Backup` oder `<Security Agent-Installationsordner>\quarantine` – je nach Verfügbarkeit. • `<Messaging Security Agent Installationsordner>\storage\quarantine` Diese Dateien werden in den vorgesehenen Quarantäne-Ordner hochgeladen, der normalerweise ein Ordner auf dem Security Server ist.
Dateien in der Quarantäne im vorgesehenen Quarantäne-Ordner	Standardmäßig befindet sich das Verzeichnis auf dem Security Server Computer (`<Security Server Installationsordner>>\PCCSRV\Virus`). Um das Verzeichnis zu ändern, navigieren Sie zur Registerkarte **Administration** > **Allgemeine Einstellungen** > **System** und wählen Sie den Bereich Quarantäne-Wartung aus.
Gesicherte verschlüsselte Dateien	Dabei handelt es sich um Sicherheitskopien der infizierten Dateien, die die Agents säubern konnte. Diese Dateien befinden sich in den folgenden Ordnern: • `<Security Agent Installationsordner>\Backup` • `<Messaging Security Agent Installationsordner>\storage\backup` Um diese Dateien wiederherzustellen, müssen Sie sie in den Quarantäne-Ordner auf dem Client verschieben.

Warnung!

Durch das Wiederherstellen einer infizierten Datei könnte sich der Virus bzw. die Malware auf andere Dateien und Clients übertragen. Bevor Sie die Datei wiederherstellen, isolieren Sie den infizierten Client, und erstellen Sie Sicherheitskopien wichtiger Dateien auf diesem Client.

Dateien entschlüsseln und auf dem Security Agent wiederherstellen

Prozedur

1. Öffnen Sie ein Befehlszeilenfenster, und navigieren Sie zum `<Security Agent-Installationsordner>`.
2. Führen Sie `VSEncode.exe` aus, indem Sie Folgendes eingeben:

   ```
   VSEncode.exe /u
   ```

   Dieser Parameter öffnet ein Fenster mit einer Liste der Dateien unter `<Security Agent-Installationsordner>\SUSPECT\Backup`.

   Administratoren können als Spyware/Grayware eingestufte Dateien über die Registerkarte 'Spyware/Grayware' wiederherstellen. Das Fenster zeigt eine Liste der Dateien im folgenden Ordner an: `<Security Agent-Installationsordner>\BackupAS`.
3. Wählen Sie die Datei, die wiederhergestellt werden soll, und klicken Sie auf **Wiederherstellen**.

   Hinweis

   Mit dem Tool können Sie jeweils nur eine Datei wiederherstellen.
4. Geben Sie im daraufhin angezeigten Fenster den Ordners an, in dem die Datei wiederhergestellt werden soll.
5. Klicken Sie auf **OK**.

Hinweis

Unter Umständen kann der Agent die Datei erneut durchsuchen und als infizierte Datei behandeln, sobald die Datei wiederhergestellt wurde. Um zu verhindern, dass die Datei erneut durchsucht wird, fügen Sie sie der Suchausschlussliste hinzu.

Weitere Informationen finden Sie unter *Suchziele und Aktionen für Security Agents auf Seite 7-10*.

Die Datei wird im angegebenen Ordner wiederhergestellt.

6. Klicken Sie auf **Schließen**.

Dateien auf dem Security Server, in einem benutzerdefinierten Quarantäne-Verzeichnis oder Messaging Security Agent entschlüsseln und wiederherstellen

Prozedur

1. Wenn sich die Datei auf dem Security Server-Computer befindet, öffnen Sie ein Befehlszeilenfenster, und navigieren Sie zu `<Server-Installationsordner>\PCCSRV\Admin\Utility\VSEncrypt`.

   Wenn sich die Datei auf einem Messaging Security Agent-Client oder in einem benutzerdefinierten Quarantäne-Verzeichnis befindet, navigieren Sie zu `<Server-Installationsordner>\PCCSRV\Admin\Utility`, und kopieren Sie den Ordner `VSEncrypt` auf den Computer, auf dem sich der Client oder das benutzerdefinierte Quarantäne-Verzeichnis befindet.

2. Erstellen Sie eine Textdatei. Geben Sie anschließend den vollständigen Pfad zu den Dateien ein, die Sie ver- oder entschlüsseln möchten.

   Um beispielsweise Dateien im Verzeichnis `C:\Eigene Dateien\Reports wiederherzustellen, geben Sie C:\Eigene Dateien\Reports\*.*` in die Textdatei ein.

   Dateien unter Quarantäne befinden sich auf dem Security Server-Computer unter `<Server-Installationsordner>\PCCSRV\Virus`.

3. Speichern Sie die Textdatei mit der Erweiterung `INI` oder `TXT`. Speichern Sie sie beispielsweise unter `ZurVerschluesselung.ini` auf Laufwerk `C:` Laufwerk C:.

4. Öffnen Sie ein Befehlszeilenfenster, und navigieren Sie zum Verzeichnis, in dem sich der Ordner `VSEncrypt` befindet.

5. Führen Sie `VSEncode.exe` aus, indem Sie Folgendes eingeben:

   ```
   VSEncode.exe /d /i <Speicherort der INI- oder TXT-Datei>
   ```

   Wobei gilt:

   `<Speicherort der INI- oder TXT-Date>` ist der Pfad der von Ihnen erstellten `INI`- oder `TXT`-Datei (z. B. `C:\ForEncryption.ini`).

6. Verwenden Sie die anderen Parameter, um verschiedene Befehle auszuführen.

Tabelle 14-3. Parameter für die Wiederherstellung

Parameter	Beschreibung
Keiner (kein Parameter)	Dateien verschlüsseln
`/d`	Dateien entschlüsseln
`/debug`	Erstellen Sie ein Debug-Protokoll, und speichern Sie es auf dem Computer. Auf dem Client wird das Debug-Protokoll `VSEncrypt.log` im `<Agent-Installationsordner>` erstellt.
`/o`	Überschreibt eine ver- bzw. entschlüsselte Datei, falls bereits vorhanden
`/f <Dateiname>`	Ver- oder entschlüsselt eine einzelne Datei
`/nr`	Ursprünglicher Dateiname wird nicht wiederhergestellt
`/v`	Informationen über das Tool werden angezeigt
`/u`	Startet die Benutzeroberfläche des Tools
`/r <Zielordner>`	Der Ordner, in dem eine Datei wiederhergestellt wird

Parameter	Beschreibung
`/s <Ursprünglicher Dateiname>>`	Der Dateiname der ursprünglich verschlüsselten Datei

Sie können beispielsweise `VSEncode [/d] [/debug]` eingeben, um Dateien im Ordner `Suspect` zu entschlüsseln und ein Debug-Protokoll zu erstellen. Wenn Sie eine Datei ent- oder verschlüsseln, erstellt Worry-Free Business Security die ent- oder verschlüsselte Datei im selben Ordner. Vergewissern Sie sich, bevor Sie eine Datei entschlüsseln oder verschlüsseln, dass diese nicht gesperrt ist.

TNEF-Nachrichten (Transport Neutral Encapsulation Format) wiederherstellen

TNEF ist ein Nachrichtenverkapselungsformat, das in Microsoft Exchange und Outlook verwendet wird. Normalerweise ist das Format als E-Mail-Anhang `Winmail.dat` gepackt und wird von Outlook Express automatisch ausgeblendet.

Weitere Informationen finden Sie unter https://support.microsoft.com/en-us/help/290809/.

Wenn der Messaging Security Agent diesen E-Mail-Typ archiviert und die Dateierweiterung in .EML geändert wird, zeigt Outlook Express nur den Text der E-Mail an.

ReGenID Tool verwenden

Für jede Security Agent Installation ist ein GUID (Globally Unique Identifier) erforderlich, damit der Security Server die Clients eindeutig identifizieren kann. Duplizierte GUIDs treten normalerweise im Zusammenhang mit geklonten Clients oder virtuellen Maschinen auf.

Führen Sie das ReGenID Tool aus, um einen eindeutigen GUID für jeden Client zu erstellen, falls zwei oder mehr Agents denselben GUID melden.

Prozedur

1. Wechseln Sie auf dem Security Server in das folgende Verzeichnis: `<Installationsordner des Servers>\PCCSRV\Admin\Utility`.
2. Kopieren Sie `WFBS_WIN_All_ReGenID.exe` in einen temporären Ordner auf dem Client, auf dem der Security Agent installiert ist.

   Beispiel: `C:\temp`
3. Doppelklicken Sie auf `WFBS_WIN_All_ReGenID.exe` und folgen Sie der auf dem Bildschirm angezeigten Anleitung.

   Das Tool hält den Security Agent an und entfernt den Client-GUID.
4. Starten Sie den Security Agent dann neu.

   Der Security Agent erstellt einen neuen Client-GUID.

SBS und EBS Add-ins verwalten

Worry-Free Business Security bietet Add-ins, mit denen Administratoren auf den Konsolen der folgenden Windows-Betriebssysteme Agentstatus- und Sicherheitsinformationen in Echtzeit anzeigen können:

- 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

SBS und EBS Add-ins manuell installieren

Das SBS oder EBS Add-in wird automatisch installiert, wenn Sie den Security Server auf einem Endpunkt, auf dem die unterstützten Betriebssysteme

ausgeführt werden, installieren. Um das Add-in auf einem anderen Endpunkt, auf dem diese unterstützten Betriebssysteme ausgeführt werden, zu verwenden, ist eine manuelle Installation des Add-ins erforderlich.

Prozedur

1. Melden Sie sich bei der Webkonsole des Security Servers an.
2. Navigieren Sie zu **Administration** > **Management-Tools**.
3. Klicken Sie auf **Add-ins**.
4. Klicken Sie auf den entsprechenden **Download**-Link, um das Installationsprogramm herunterzuladen.
5. Kopieren Sie das Installationsprogramm auf den Zielendpunkt und starten Sie es.

SBS oder EBS Add-ins verwenden

Prozedur

1. Öffnen Sie die SBS oder EBS Konsole.
2. Klicken Sie in der Registerkarte **Sicherheit** auf **Trend Micro Worry-Free Business Security**, um die Statusinformation anzuzeigen.

Anhang A

Symbole für Security Agent

In diesem Anhang werden die verschiedenen Symbole für den Security Agent erklärt, die auf Clients angezeigt werden.

Status des Security Agents prüfen

Die folgende Abbildung zeigt eine Security Agent Konsole, bei der alles aktualisiert ist und die ordnungsgemäß arbeitet:

Die folgende Tabelle besteht aus einer Liste der Symbole auf der Hauptbenutzeroberfläche der Security Agent Konsole sowie deren Bedeutung:

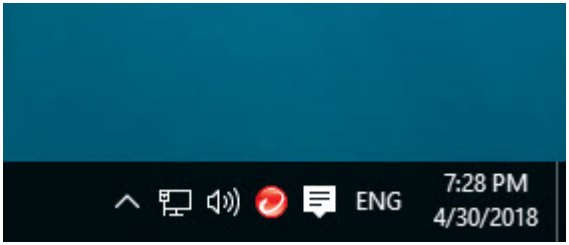
Tabelle A-1. Symbole auf der Hauptbenutzeroberfläche der Security Agent Konsole

Symbol	Status	Erklärung und Aktion
	Schutz aktiviert: Ihr Computer ist geschützt, und die Software ist auf dem neuesten Stand.	Die Software ist auf dem neuesten Stand und wird ordnungsgemäß ausgeführt. Keine Aktion erforderlich.
	Computer neu starten: Starten Sie den Computer neu, um die Behebung der Sicherheitsbedrohungen abzuschließen.	Der Security Agent hat Bedrohungen erkannt, die nicht sofort behoben werden konnten. Starten Sie den Computer neu, um die Behebung dieser Bedrohungen abzuschließen.
	Schutz gefährdet: Wenden Sie sich an den Administrator	Die Echtzeitsuche ist deaktiviert, oder Ihr Schutz ist aus einem anderen Grund gefährdet. Aktivieren Sie die Echtzeitsuche und wenden Sie sich an den Support, falls das Problem dadurch nicht behoben wird.
	Jetzt aktualisieren: Sie haben seit mehr als (Anzahl) Tagen kein Update erhalten.	Das Viren-Pattern ist älter als 3 Tage. Aktualisieren Sie den Security Agent umgehend.

Symbol	Status	Erklärung und Aktion
	Smart Scan ist nicht verfügbar: Überprüfen Sie Ihre Internet-Verbindung	Der Security Agent kann seit über 15 Minuten nicht auf den Suchserver zugreifen. Stellen Sie sicher, dass Sie mit dem Netzwerk verbunden sind, um die neuesten Pattern für die Suche verwenden zu können.
	Computer neu starten: Starten Sie den Computer neu, um die Installation des Updates abzuschließen	Starten Sie den Computer neu, um das Update fertig zu stellen.
	Programm wird aktualisiert: Ihre Sicherheits-Software wird aktualisiert	Ein Update wird durchgeführt. Trennen Sie die Netzwerkverbindung nicht, solange das Update läuft.

Security Agent-Symbole in der Windows Task-Leiste anzeigen

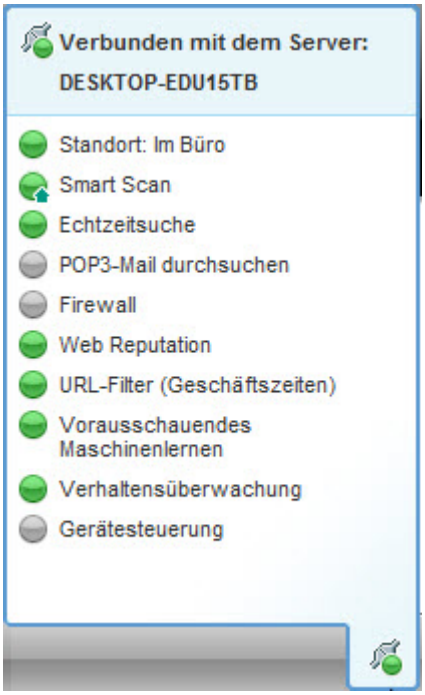
Die folgenden Security Agent-Symbole werden in der Windows Task-Leiste angezeigt:



Symbol	Bedeutung
	Status ist normal
	(Animiert) Eine manuelle oder zeitgesteuerte Suche wird ausgeführt. Der Security Agent verwendet die herkömmliche Suche oder die Smart Scan.
	Der Security Agent führt ein Update durch.
	Aktion ist erforderlich: • Echtzeitsuche ist deaktiviert • Neustart erforderlich, um die Malware vollständig vom System zu entfernen • Bedingt durch eine aktualisierte Engine ist ein Neustart erforderlich • Neustart erforderlich, um von Ransomware verschlüsselte Dateien wiederherzustellen • Update ist erforderlich **Hinweis** Öffnen Sie die Hauptkonsole des Security Agent, um festzustellen, welche Aktion erforderlich ist.

Auf den Flyover-Bereich der Konsole zugreifen

Das Security Agent-Konsolen-Flyover erscheint, wenn Sie mit Ihrem Mauszeiger über das kleine Symbol rechts unten in der Security Agent-Konsole fahren.



Die nachfolgende Tabelle enthält eine Liste der Symbole im Flyover-Bereich der Konsole sowie deren Bedeutung:

TABELLE A-2. Symbole im Flyover-Bereich der Konsole

FUNKTION	SYMBOL	BEDEUTUNG
Verbindung		Mit Security Server verbunden.
		Nicht mit Security Server verbunden, aber Echtzeitsuche wird noch ausgeführt. Möglicherweise ist die Pattern-Datei nicht mehr aktuell. Klicken Sie mit der rechten Maustaste auf das Agent-Symbol in der Windows Task-Leiste und klicken Sie auf **Jetzt aktualisieren**.

Funktion	Symbol	Bedeutung
Speicherort		Im Büro (internes Netzwerk)
		Nicht im Büro (externes Netzwerk)
Echtzeitsuche		Aktiviert
		Deaktiviert
POP3-Mail durchsuchen		Aktiviert
		Deaktiviert
Smart Scan		Verbunden mit dem Trend Micro Smart Protection Network
		Verbindung mit dem Smart Protection Network nicht möglich. Geringerer Schutz, da Security Agents keine Suchabfragen senden können. **Hinweis** Vergewissern Sie sich, dass der Smart Scan Service TMiCRCScanService ausgeführt wird und Security Agents mit dem Security Server verbunden sind.
		Die Smart Scan ist deaktiviert. Herkömmliche Suche verwenden

Funktion	Symbol	Bedeutung
• Firewall • Web Reputation • URL-Filter • Verhaltensüberwachung • Gerätesteuerung • Vorausschauendes Maschinenlernen		Aktiviert
		Deaktiviert

Anhang B

IPv6-Unterstützung in Worry-Free Business Security

Benutzer, die die Verteilung von Worry-Free Business Security in einer Umgebung planen, die IPv6-Adressierung unterstützt, sollten diesen Anhang unbedingt lesen. In diesem Anhang finden Sie Informationen zum Umfang der IPv6-Unterstützung in Worry-Free Business Security.

Trend Micro setzt voraus, dass der Leser mit IPv6-Konzepten und mit den Aufgaben vertraut ist, die mit dem Einrichten eines Netzwerks verbunden sind, das IPv6-Adressierung unterstützt.

IPv6-Unterstützung für Worry-Free Business Security und Security Agents

Die IPv6-Unterstützung für Worry-Free Business Security beginnt in Version 8.0. Frühere Worry-Free Business Security Versionen unterstützen die IPv6-Adressierung nicht. IPv6-Unterstützung wird automatisch nach der Installation oder dem Upgrade von Security Server, Security Agents und Messaging Security Agents aktiviert, wenn sie die IPv6-Voraussetzungen erfüllen.

IPv6-Voraussetzungen für den Security Server

Für den Security Server gelten folgende IPv6-Voraussetzungen:

- Wenn der Server IPv4- und IPv6-Agents verwaltet, muss er eine IPv4- wie auch eine IPv6-Adresse haben und über seinen Hostnamen identifiziert werden. Wenn der Server über seine IPv4-Adresse identifiziert wird, können reine IPv6-Agents keine Verbindung zum Server herstellen. Dasselbe Problem tritt auf, wenn reine IPv4-Clients eine Verbindung mit einem Server herstellen, der über seine IPv6-Adresse identifiziert wird.
- Wenn der Server nur IPv6-Agents verwaltet, ist mindestens eine IPv6-Adresse erforderlich. Der Server kann über seinen Hostnamen oder seine IPv6-Adresse identifiziert werden. Wenn der Server über seinen Hostnamen identifiziert wird, sollte vorzugsweise sein vollqualifizierter Domänenname (FQDN) verwendet werden. Der Grund hierfür ist, dass ein WINS Server in einer reinen IPv6-Umgebung einen Hostnamen nicht in seine entsprechende IPv6-Adresse übersetzen kann.
- Vergewissern Sie sich, dass die IPv6- oder IPv4-Adresse des Host-Computers abgerufen werden kann. Verwenden Sie dazu z. B. den Befehl "`ping`" oder "`nslookup`".
- Wenn Sie den Security Server auf einem reinen IPv6-Computer installieren, richten Sie einen Dual-Stack Proxy-Server ein, der zwischen IPv4- und IPv6-Adressen konvertieren kann (wie etwa DeleGate).

Platzieren Sie den Proxy-Server zwischen den Security Server und das Internet, damit der Server sich erfolgreich mit den von Trend Micro verwalteten Diensten verbinden kann, z. B. dem ActiveUpdate Server, der Online-Registrierungswebsite und dem Smart Protection Network.

Voraussetzungen für den Messaging Security Agent

Der Messaging Security Agent (nur Advanced) muss auf einem Dual-Stack- oder einem reinen IPv6-Microsoft Exchange Server installiert werden.

Ein Messaging Security Agent sollte vorzugsweise sowohl über IPv4- als auch IPv6-Adressen verfügen, da einige Elemente, zu denen er sich verbindet, nur IPv4-Adressierung unterstützen.

Einschränkungen bei reinen IPv6-Servern

Die folgende Tabelle enthält eine Liste mit Einschränkungen von Security Servern, die nur über eine IPv6-Adresse verfügen.

Tabelle B-1. Einschränkungen bei reinen IPv6-Servern

Element	Einschränkung
Agent-Verwaltung	Ein reiner IPv6-Server kann nicht: • Verteilt Agents an reine IPv4-Clients • Reine IPv4-Agents verwalten.
Updates und zentrale Verwaltung	Ein reiner IPv6-Server kann sich nicht über reine IPv4-Update-Quellen aktualisieren, wie etwa: • Trend Micro ActiveUpdate Server • Jede reine, benutzerdefinierte IPv4-Update-Quelle
Produktregistrierung, -aktivierung und -verlängerung	Ein reiner IPv6-Server kann sich nicht mit dem Trend Micro Online-Registrierungsserver verbinden, um das Produkt zu registrieren, eine Lizenz anzufordern und die Lizenz zu aktivieren/erneuern.
Proxy-Verbindung	Ein reiner IPv6-Server kann sich nicht über einen reinen IPv4-Proxy-Server verbinden.

Element	Einschränkung
Plug-in-Lösungen	Ein reiner IPv6-Server verfügt über Plug-in Manager, kann aber keine Plug-in-Lösung verteilen an: • Reine IPv4-Agents oder reine IPv4-Hosts (da keine direkte Verbindung besteht). • Reine IPv6-Agents oder reine IPv6-Hosts, weil keine der Plug-in-Lösungen IPv6 unterstützt.

Die meisten dieser Einschränkungen können überwunden werden, indem man einen Dual-Stack-Proxy-Server aufsetzt, der zwischen IPv4- und IPv6-Adressen konvertieren kann (wie etwa DeleGate). Positionieren Sie den Proxy-Server zwischen dem Security Server und den Elementen, zu denen er sich verbindet, oder den Elementen, die er bedient.

Einschränkungen bei reinen IPv6-Security Agents

Die folgende Tabelle enthält eine Liste von Einschränkungen, wenn der Security Agent nur über eine IPv6-Adresse verfügt.

Tabelle B-2. Einschränkungen bei reinen IPv6-Security Agents

Element	Einschränkung
Übergeordneter Security Server	Reine IPv6-Agents können nicht von einem reinen IPv4-Security Server verwaltet werden.
Updates	Ein reiner IPv6-Security Agent kann sich nicht über reine IPv4-Update-Quellen aktualisieren, wie etwa: • Trend Micro ActiveUpdate Server • Ein reiner IPv4-Security Server • Ein reiner IPv4-Update-Agent • Jede reine, benutzerdefinierte IPv4-Update-Quelle
Suchabfragen und Smart Feedback	Ein reiner IPv6-Security Agent kann keine Abfragen an das Trend Micro Smart Protection Network senden und Smart Feedback nicht verwenden.

Element	Einschränkung
Plug-in-Lösungen	Reine IPv6-Agents können keine Plug-in-Lösungen installieren, weil keine dieser Lösungen IPv6 unterstützt.
Proxy-Verbindung	Ein reiner IPv6-Security Agent kann sich nicht über einen reinen IPv4-Proxy-Server verbinden.

Die meisten dieser Einschränkungen können überwunden werden, indem man einen Dual-Stack-Proxy-Server aufsetzt, der zwischen IPv4- und IPv6-Adressen konvertieren kann (wie etwa DeleGate). Positionieren Sie den Proxy-Server zwischen den Security Agents und den Elementen, zu denen sie sich verbinden.

IPv6-Adressen konfigurieren

Auf der Webkonsole können Sie eine IPv6-Adresse oder einen IPv6-Adressbereich konfigurieren. Beachten Sie bitte die folgenden Richtlinien.

- Worry-Free Business Security akzeptiert Standarddarstellungen von IPv6-Adressen.

  Beispiel:

  `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`

- Worry-Free Business Security akzeptiert auch link-lokale IPv6-Adressen, wie etwa:

  `fe80::210:5aff:feaa:20a2`

Warnung!

Seien Sie vorsichtig, wenn Sie eine link-lokale IPv6-Adresse festlegen, da sie unter bestimmten Umständen möglicherweise nicht erwartungsgemäß funktioniert, obwohl Worry-Free Business Security diese Adresse akzeptieren kann. Zum Beispiel können Security Agents sich nicht über eine Update-Quelle aktualisieren, wenn sich die Quelle in einem anderen Netzwerksegment befindet und durch ihre link-lokale IPv6-Adresse identifiziert wird.

- Wenn die IPv6-Adresse Teil eines URL ist, setzen Sie die Adresse in eckige Klammern ([]).
- Bei IPv6-Adressbereichen sind normalerweise ein Präfix und eine Präfixlänge erforderlich. Bei Konfigurationen, bei denen der Server die IP-Adressen abfragen muss, helfen die Einschränkungen der Präfixlänge, um Leistungseinbußen zu vermeiden, die auftreten können, wenn der Server eine beträchtliche Anzahl von IP-Adressen abfragt. Zum Beispielor darf bei der Funktion der ausgelagerten Server-Verwaltung das Präfix nur zwischen 112 (65.536 IP-Adressen) und 128 (2 IP-Adressen) lang sein.
- Einige Einstellungen, bei denen IPv6-Adressen oder -Adressbereiche eine Rolle spielen, werden zwar an Security Agents verteilt, aber von Security Agents ignoriert. Wenn Sie zum Beispiel die Liste der Smart Protection Quellen konfiguriert haben und sich darin ein Smart Protection Server befindet, der an seiner IPv6-Adresse identifiziert wird, ignorieren reine IPv4-Security Agents den Server und verbinden sich mit den anderen Smart Protection Quellen.

Fenster, auf denen IP-Adressen angezeigt werden

In diesem Thema werden alle Stellen auf der Webkonsole genannt, an denen IP-Adressen angezeigt werden.

- Die Sicherheitsgruppenansicht

  Bei jedem Anzeigen der Sicherheitsgruppenansicht werden die IPv6-Adressen der reinen IPv6-Agents in der Spalte **IP-Adresse** angezeigt. Bei

Dual-Stack-Agents werden die IPv6-Adressen angezeigt, wenn sie sich mit ihrer IPv6-Adresse am Server registriert haben.

Hinweis

Sie können die IP-Adresse, die von Dual-Stack-Agents zur Registrierung beim Server verwendet wird, im Bereich **Bevorzugte IP-Adresse** auf der Registerkarte **Administration** > **Allgemeine Einstellungen** > **Desktop/Server** festlegen.

Wenn Sie die Einstellungen eines Agents in eine Datei exportieren, werden die IPv6-Adressen auch in der exportierten Datei angezeigt.

- Protokolle

  Die IPv6-Adressen von Dual-Stack- und reinen IPv6-Agents finden sich in den folgenden Protokollen:

Anhang C

Technischer Support

Erfahren Sie mehr über die folgenden Themen:

- *Ressourcen zur Fehlerbehebung auf Seite C-2*
- *Kontaktaufnahme mit Trend Micro auf Seite C-3*
- *Verdächtige Inhalte an Trend Micro senden auf Seite C-5*
- *Sonstige Ressourcen auf Seite C-6*

Ressourcen zur Fehlerbehebung

Vor der Kontaktaufnahme mit dem technischen Support sollten Sie die folgenden Online-Ressourcen zu Trend Micro heranziehen.

Support-Portal verwenden

Über das Trend Micro Support-Portal können Sie rund um die Uhr online auf die aktuellsten Informationen über allgemeine und ungewöhnliche Probleme zugreifen.

Prozedur

1. Gehen Sie zu https://success.trendmicro.com.
2. Wählen Sie unter den verfügbaren Produkten aus oder klicken Sie auf die entsprechende Schaltfläche, um nach Lösungen zu suchen.
3. Mit dem Feld **Support durchsuchen** können Sie nach verfügbaren Lösungen suchen.
4. Falls Sie keine Lösung finden, klicken Sie auf **Support kontaktieren** und wählen Sie den gewünschten Support aus.

   Tipp

   Um online eine Supportanfrage zu senden, besuchen Sie die folgende URL:

   https://success.trendmicro.com/smb-new-request

   Das Problem wird von einem Support-Mitarbeiter von Trend Micro untersucht, der innerhalb von 24 Stunden oder weniger auf Ihre Anfrage reagiert.

Bedrohungsenzyklopädie

Die meiste Malware besteht heutzutage aus komplexen Bedrohungen, bei denen zwei oder mehr Technologien miteinander kombiniert werden, um Computer-Sicherheitsprotokolle zu umgehen. Trend Micro bekämpft diese komplexe Malware mit Produkten, die eine benutzerdefinierte Verteidigungsstrategie verfolgen. Die Bedrohungsenzyklopädie enthält eine ausführliche Liste mit Namen und Symptomen von verschiedenen kombinierten Bedrohungen, wie etwa bekannte Malware, Spam, bösartige URLs und bekannte Schwachstellen.

Auf https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware finden Sie weitere Informationen zu folgenden Themen:

- Malware und bösartige mobile Codes, die zum jeweiligen Zeitpunkt aktiv und im Umlauf sind
- Seiten mit Bedrohungsinformationen, die eine umfassende Ressource für Internet-Angriffe darstellen
- Beratung zu Internet-Bedrohungen bezüglich gezielten Angriffen und Sicherheitsbedrohungen
- Informationen zu Internet-Angriffen und Online-Trends
- Wöchentliche Malware-Berichte

Kontaktaufnahme mit Trend Micro

Sie erreichen Ihre Trend Micro Ansprechpartner telefonisch oder per E-Mail:

Adresse	Trend Micro Deutschland GmbH Parkring 29 85748 Garching
Telefon	+49 (0)89 8393 29700
Website	https://www.trendmicro.com

E-Mail-Adresse	support@trendmicro.com

- Weltweite Support-Büros:

  https://www.trendmicro.com/us/about-us/contact/index.html

- Kontaktaufnahme mit Trend Micro:

  http://www.trendmicro.de/ueber-uns/kontakt/index.html

- Trend Micro Produktdokumentation:

  https://docs.trendmicro.com

Problemlösung beschleunigen

Sie sollten die folgenden Informationen zur Hand haben, um die Problemlösung zu beschleunigen:

- Schritte, um das Problem nachvollziehen zu können
- Informationen zur Appliance und zum Netzwerk
- Marke und Modell des Computers sowie zusätzlich angeschlossene Hardware oder Geräte
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Betriebssystem- und Service Pack-Version
- Version des installierten Agents
- Seriennummer oder Aktivierungscode
- Ausführliche Beschreibung der Installationsumgebung
- Genauer Wortlaut eventueller Fehlermeldungen

Verdächtige Inhalte an Trend Micro senden

Es gibt mehrere Optionen, um verdächtige Inhalte an Trend Micro zur weiteren Analyse zu senden.

Email Reputation Services

Fragen Sie die Reputation einer bestimmten IP-Adresse ab, und geben Sie einen Message Transfer Agent zum Hinzufügen zur Liste der allgemein zulässigen Adressen an:

https://servicecentral.trendmicro.com/en-us/ers/

Informationen zum Senden von Nachrichten an Trend Micro finden Sie im folgenden Knowledge Base-Artikel:

https://success.trendmicro.com/solution/1112106

File-Reputation-Dienste

Sammeln Sie Systeminformationen, und senden Sie verdächtige Dateiinhalte an Trend Micro:

https://success.trendmicro.com/solution/1059565

Notieren Sie sich die Anfragenummer für die weitere Bearbeitung Ihrer Anfrage.

Web Reputation-Dienste

Sie können die Sicherheitsbewertung und den Inhaltstyp einer URL abfragen, hinter der Sie eine Phishing-Website oder einen Infektionsüberträger vermuten, d. h. eine Quelle von Internet-Bedrohungen, wie z. B. Spyware und Viren:

https://global.sitesafety.trendmicro.com/

Falls die zugewiesene Bewertung nicht zutrifft, senden Sie eine Neuklassifizierungsanforderung an Trend Micro.

Sonstige Ressourcen

Neben Lösungen und Support sind online viele zusätzliche hilfreiche Ressourcen verfügbar, damit Sie immer auf dem neuesten Stand sind, Innovationen kennenlernen und mit den neuesten Sicherheitstrends vertraut sind.

Download Center

Trend Micro veröffentlicht in bestimmten Abständen Patches für gemeldete bekannte Probleme oder Upgrades zu bestimmten Produkten oder Diensten. Auf folgender Seite können Sie feststellen, ob Patches verfügbar sind:

https://www.trendmicro.com/download/

Falls ein Patch nicht angewendet wurde (Patches sind datiert), öffnen Sie die Readme-Datei, um festzustellen, ob er für Ihre Umgebung relevant ist. In der Readme-Datei finden Sie außerdem Installationsanweisungen.

Anregungen und Kritik

Das Trend Micro Team ist stets bemüht, die Dokumentationen zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder einem anderen Dokument von Trend Micro besuchen Sie diese Website:

https://docs.trendmicro.com/en-us/survey.aspx

Anhang D

Produktterminologie und Konzepte

Die Inhalte dieses Anhangs enthalten weitere Informationen über Produkte und Technologien von Trend Micro.

Kritischer Patch

Ein kritischer Patch ist auf sicherheitsrelevante Probleme ausgerichtet und kann an alle Kunden verteilt werden. Kritische Patches von Windows verfügen über ein Setup-Programm, während andere Patches in der Regel über ein Setup-Skript ausgeführt werden.

Hotfix

Ein Workaround bzw. eine Lösung zu einem bestimmten Problem, das Kunden an Trend Micro berichtet haben. Da sich Hotfixes auf ein bestimmtes Problem beziehen, werden sie nicht allen Kunden zur Verfügung gestellt. Im Gegensatz zu anderen Hotfixes umfassen Windows Hotfixes ein Setup-Programm (in der Regel müssen Sie die Programm-Daemons beenden, die installierte Datei überschreiben, und den Daemon neu starten).

IntelliScan

IntelliScan ist ein Verfahren, um festzustellen, welche Dateien durchsucht werden müssen. Bei ausführbaren Dateien, wie z. B. `*.EXE`), wird der ursprüngliche Dateityp (True File Type) über den Dateiinhalt bestimmt. Bei nicht ausführbaren Dateien, wie z. B. `.txt`, wird der ursprüngliche Dateityp über den Datei-Header bestimmt.

Die Verwendung von IntelliScan bietet die folgenden Vorteile:

- Leistungsoptimierung: IntelliScan beeinträchtigt keine Anwendungen auf dem Agent, da nur minimale Systemressourcen benötigt werden.
- Kürzere Virensuchzeiten: Da IntelliScan die True-File-Type-Erkennung verwendet, werden nur Dateien durchsucht, für die ein Infektionsrisiko besteht. Die Suchzeit verkürzt sich gegenüber der Suche in allen Dateien erheblich.

IntelliTrap

IntelliTrap ist eine heuristische Suchtechnologie von Trend Micro zur Erkennung von Bedrohungen, bei denen Echtzeitkomprimierung in Verbindung mit anderen Malware-Merkmalen, z. B. Packer, verwendet wird. Hierzu zählen Viren/Malware, Würmer, Trojaner, Backdoor-Programme und Bots. Virenschreiber versuchen oft, Viren- und Malware-Filter zu umgehen, indem sie unterschiedliche Methoden zur Komprimierung von Dateien anwenden. IntelliTrap ist eine regelbasierte Scan Engine Technologie zur Erkennung von Pattern in Echtzeit, die bekannte Viren/Malware in den 16 am häufigsten verwendeten Komprimierungsformaten mit bis zu 17 Komprimierungsebenen erkennt und entfernt.

Hinweis

IntelliTrap verwendet dieselbe Scan Engine wie die Virensuche. Demzufolge sind für IntelliTrap die Regeln über den Umgang mit Dateien und die Suche identisch mit denen, die der Administrator für die Virensuche definiert.

Der Agent erstellt Einträge über Bot- und Malware-Funde im IntelliTrap Protokoll. Sie können den Inhalt des Protokolls exportieren, um ihn in den Berichten zu verwenden.

Bei der Suche nach Bots und anderen schädlichen Programmen verwendet IntelliTrap folgende Komponenten:

- Viren Scan Engine
- IntelliTrap Pattern
- IntelliTrap Ausnahme-Pattern

Intrusion Detection System

Das Intrusion Detection System (IDS) kann bestimmte Muster in Netzwerkpaketen erkennen, die möglicherweise auf einen Angriff auf dem Endpunkt hindeuten.

Das Intrusion Detection System (IDS) kann dabei helfen, die folgenden bekannten Eindringversuche zu verhindern:

Intrusion	Beschreibung
Fragment zu groß	Ein Denial-of-Service-Angriff, bei dem ein Hacker ein übergroßes TCP/UDP-Paket an einen Zielendpunkt weiterleitet. Dies kann zu einem Pufferüberlauf führen, durch den der Endpunkt einfrieren oder neu gestartet werden kann.
Ping-of-Death	Ein Denial-of-Service-Angriff, bei dem ein Hacker ein übergroßes ICMP/ICMPv6-Paket an einen Zielendpunkt weiterleitet. Dies kann zu einem Pufferüberlauf führen, durch den der Endpunkt einfrieren oder neu starten kann.
ARP-Konflikt	Ein Angriff, bei dem ein Hacker eine ARP-Anforderung (Address Resolution Protocol) mit der gleichen Quell- und Ziel-IP-Adresse an ein Zielendpunkt sendet. Der Zielendpunkt sendet daraufhin ununterbrochen eine ARP-Antwort (seine MAC-Adresse) an sich selbst. Dies führt zum Einfrieren oder Systemabsturz des Endpunkts.
SYN-Flooding	Ein Denial-of-Service-Angriff, bei dem ein Programm mehrere TCP-SYN-Pakete (Synchronisierungspakete) an den Endpunkt sendet. Daraufhin sendet der Endpunkt ständig Synchronisierungsbestätigungen (SYN/ACK). Dies überlastet auf Dauer den Arbeitsspeicher des Endpunkts und kann zum Absturz des Endpunkts führen.
Überlappendes Fragment	Ähnlich einem Teardrop-Angriff sendet dieser Denial-of-Service-Angriff überlappende TCP-Fragmente an den Endpunkt. Dadurch werden die Header-Informationen im ersten TCP-Fragment überschrieben und können dann eine Firewall passieren. Daraufhin können weitere Fragmente mit bösartigem Code an den Zielendpunkt durchgelassen werden.
Teardrop	Ähnlich wie bei einem Angriff durch ein Überlappendes Fragment erfolgt der Angriff bei einem Denial-of-Service mit IP-Fragmenten. Ein falsch gesetzter Offset-Wert im zweiten (oder einem nachfolgenden) IP-Fragment kann zum Absturz des Betriebssystems auf dem empfangenden Endpunkt führen, wenn versucht wird, die Fragmente wieder zusammenzusetzen.
Tiny Fragment Attack	Eine Art Angriff, bei dem durch die geringe Größe des TCP-Fragments die Übernahme der Header-Informationen des ersten TCP-Pakets in das nächste Fragment erzwungen wird. Dadurch ignorieren die Router, die den Datenverkehr filtern, nachfolgende Fragmente, die möglicherweise bösartigen Code enthalten.

Intrusion	Beschreibung
Fragmentiertes IGMP	Ein Denial-of-Service-Angriff, bei dem fragmentierte IGMP-Pakete an den Zielendpunkt gesendet werden, der diese Pakete nicht ordnungsgemäß weiterverarbeiten kann. Dies schränkt die Leistung des Endpunkts stark ein oder kann zu einem Absturz führen.
LAND Attack	Bei diesem Angriff werden IP-SYN-Pakete (Synchronisierungspakete) mit der gleichen Quell- und Zieladresse an den Endpunkt gesendet. Daraufhin sendet der Endpunkt die Synchronisierungsbestätigung (SYN/ACK) laufend an sich selbst. Dies schränkt die Leistung des Endpunkts stark ein oder kann zu einem Absturz führen.

Schlüsselwörter

Worry-Free Business Security verwendet die folgenden Schlüsselwörter zum Filtern von Nachrichten:

- Wörter (Pistolen, Bomben, usw.)
- Zahlen (1, 2, 3, usw.)
- Sonderzeichen (&,#,+, etc.)
- Kurze Ausdrücke (blauer Fisch, rotes Telefon, großes Haus, usw.)
- Wörter oder Sätze, die durch logische Operatoren verbunden sind (Äpfel .AND. Orangen)
- Wörter oder Sätze, die reguläre Ausdrücke enthalten (.REG. l.*n findet ‘legen’, ‘lassen’ und ‘leisten’, aber nicht ‘leer’, ‘laut’ oder ‘Leistung’)

Worry-Free Business Security kann eine vorhandene Liste mit Schlüsselwörtern aus einer Textdatei (`.TXT`) importieren. Die importierten Schlüsselwörter werden in der Schlüsselwörterliste angezeigt.

Operatoren auf Schlüsselwörtern

Operatoren sind Befehle, die mehrere Schlüsselwörter verbinden. Operatoren können die Ergebnisse eines Kriteriums erweitern oder einschränken. Umschließen Sie Operatoren mit Punkten (.). Beispiel:

`Äpfel .AND. Orangen und Äpfel .NOT. Orangen`

Hinweis

Der Operator beginnt und endet mit einem Punkt. Zwischen dem letzten Punkt des Operators und dem nachfolgenden Schlüsselwort steht ein Leerzeichen.

TABELLE D-1. Operatoren verwenden

OPERATOR	FUNKTIONSWEISE	BEISPIEL
beliebiges Schlüsselwort	Der Messaging Security Agent sucht nach Inhalten, die mit dem Wort übereinstimmen.	Geben Sie das Wort ein, und fügen Sie es zur Schlüsselwörterliste zu.
OR	Der Messaging Security Agent sucht nach allen Schlüsselwörtern, die durch OR getrennt werden. Zum Beispiel: Apfel OR Orange. Der Agent sucht entweder nach Apfel oder nach Orange. Ist eines der beiden Schlüsselwörter enthalten, handelt es sich um eine Übereinstimmung.	Trennen Sie in der Liste alle Wörter, die Sie eingeben möchten, durch "`.OR.`" . Zum Beispiel: Apfel .OR. Orange
AND	Der Messaging Security Agent sucht nach allen Schlüsselwörtern, die durch AND getrennt werden. Zum Beispiel: Apfel AND Orange. Der Agent sucht nach Apfel und nach Orange. Sind nicht beide Wörter enthalten, liegt keine Übereinstimmung vor.	Tippen Sie "`.AND.`" zwischen alle Wörter, die Sie einbeziehen wollen. Zum Beispiel: Apfel .AND. Orange

Operator	Funktionsweise	Beispiel
NOT	Der Messaging Security Agent schließt Schlüsselwörter, die auf NOT folgen, von der Suche aus. Zum Beispiel: .NOT. Saft. Der Agent sucht nach Inhalten, die das Wort Saft nicht enthalten. Falls die Nachricht "Orangen-Limo" enthält, handelt es sich um eine Übereinstimmung. Geht es dagegen um "Orangen-Saft", ist dies nicht der Fall.	Geben Sie "`.NOT.`" vor ein Wort ein, das Sie ausschließen wollen. Zum Beispiel: '.NOT. Saft'
WILD	Das Platzhalter-Symbol ersetzt einen fehlenden Teil des Wortes. Sämtliche Wörter, die den restlichen Teil des Platzhalters enthalten, stellen Übereinstimmungen dar. **Hinweis** Der Messaging Security Agent erkennt kein '?' im Platzhalterbefehl '.WILD.'.	Geben Sie "`.WILD.`" vor dem Teil des Wortes ein, nach dem Sie suchen möchten. Wenn Sie zum Beispiel nach allen Wörtern suchen möchten, die "valu" beinhalten, geben Sie "`.WILD.geld`" ein. Die Wörter Geldgewinn, Geldwert und Geldschein entsprechen dann der Regel.
REG	Um einen regulären Ausdruck festzulegen, geben Sie einen .REG.-Operator vor solchen Zeichenketten ein (zum Beispiel .REG. l.*n). Weitere Informationen finden Sie unter *Reguläre Ausdrücke auf Seite D-10*.	Geben Sie vor die Zeichenketten, nach denen Sie suchen möchten, ein "`.REG.`" ein. Zum Beispiel: ".REG. l.*n" stimmt überein mit: "legen", "lassen" und "leisten", aber nicht mit "leer", "laut" oder "Leistung".

Schlüsselwörter wirksam einsetzen

Mit den einfach verwendbaren, leistungsstarken Funktionen des Messaging Security Agents können Sie sehr präzise Filter erstellen. Beim Erstellen Ihrer Content-Filter-Regeln sollten Sie Folgendes beachten:

- Der Messaging Security Agent sucht standardmäßig nach genauen Übereinstimmungen mit den Schlüsselwörtern. Verwenden Sie reguläre Ausdrücke, um nach teilweisen Übereinstimmungen mit den Schlüsselwörtern zu suchen. Weitere Informationen finden Sie unter *Reguläre Ausdrücke auf Seite D-10*.
- Der Messaging Security Agent unterscheidet zwischen mehreren Schlüsselwörtern in einer einzigen Zeile, mehreren Schlüsselwörtern, die in verschiedenen Zeilen stehen und mehreren Schlüsselwörtern, die mit Komma, Punkt, Bindestrich oder anderen Interpunktionszeichen getrennt sind. Weitere Informationen über die Verwendung von Schlüsselwörtern in verschiedenen Zeilen finden Sie in folgender Tabelle.
- Sie können den Messaging Security Agent auch für die Suche nach Synonymen der eigentlichen Schlüsselwörter konfigurieren.

Tabelle D-2. Schlüsselwörter verwenden

Konstellation	Beispiel	Übereinstimmung/keine Übereinstimmung
Zwei Wörter in derselben Zeile	Pistolen Bomben	Übereinstimmungen: "Klicken Sie hier, um Pistolen Bomben und andere Waffen zu kaufen." Keine Übereinstimmung: "Klicken Sie hier, um Pistolen und Bomben zu kaufen."
Zwei durch Komma getrennte Wörter	Pistolen, Bomben	Übereinstimmungen: "Klicken Sie hier, um Pistolen, Bomben und andere Waffen zu kaufen." Keine Übereinstimmung: "Klicken Sie hier, um gebrauchte Pistolen, neue Bomben und andere Waffen zu kaufen."

Konstellation	Beispiel	Übereinstimmung/keine Übereinstimmung
Mehrere Wörter in mehreren Zeilen	Pistolen Bomben Waffen und Munition	Wenn Sie **Beliebiges ausgewähltes Schlüsselwort** wählen: Übereinstimmungen: "Pistolen zu verkaufen" Weitere Übereinstimmungen: "Kaufen Sie Pistolen, Bomben und andere Waffen" Wenn Sie **Alle ausgewählten Schlüsselwörter** wählen: Übereinstimmungen: "Kaufen Sie Pistolen Bomben Waffen und Munition" Keine Übereinstimmung: "Kaufen Sie Pistolen Bomben Waffen Munition." Ebenfalls keine Übereinstimmung: "Kaufen Sie Pistolen, Bomben, Waffen und Munition"
Viele Schlüsselwörter in derselben Zeile	Pistolen Bomben Waffen Munition	Übereinstimmungen: "Kaufen Sie Pistolen Bomben Waffen Munition" Keine Übereinstimmung: "Kaufen Sie Munition für Ihre Pistolen und Waffen und neuen Bomben"

Patch

Ein Patch ist eine Gruppe von Hotfixes und Sicherheits-Patches, die zur Lösung verschiedener Programmprobleme dienen. Trend Micro stellt regelmäßig Patches zur Verfügung. Patches von Windows verfügen über ein Setup-Programm, während andere Patches in der Regel über ein Setup-Skript ausgeführt werden.

Reguläre Ausdrücke

Der Zeichenkettenvergleich erfolgt über reguläre Ausdrücke. Die folgende Tabelle enthält einige Beispiele für häufig verwendete reguläre Ausdrücke. Zur Kennzeichnung eines regulären Ausdrucks wird der Operator '.REG.' der Zeichenkette vorangestellt.

Zu diesem Thema stehen online mehrere Websites und Tutorials zur Verfügung, u. a. die Seite PerlDoc unter:

http://www.perl.com/doc/manual/html/pod/perlre.html

Warnung!

Reguläre Ausdrücke können den Zeichenkettenvergleich stark beeinflussen. Reguläre Ausdrücke sollten deshalb nur von Administratoren verwendet werden, die mit deren Syntax ausreichend vertraut sind. Fehlerhafte reguläre Ausdrücke können die Systemleistung stark einschränken. Zu Beginn empfehlen sich einfache reguläre Ausdrücke ohne komplexe Syntax. Bei der Einführung neuer Regeln sollte die Aktion zum Archivieren verwendet werden und das Verhalten des Messaging Security Agent bei der Bearbeitung von Nachrichten gemäß der neuen Regel beobachtet werden. Wird die Regel ohne unerwünschte Nebeneffekte ausgeführt, kann die Aktion entsprechend geändert werden.

Beispiel für reguläre Ausdrücke

Die folgende Tabelle enthält einige Beispiele für häufig verwendete reguläre Ausdrücke. Zur Kennzeichnung eines regulären Ausdrucks wird der Operator '.REG.' der Zeichenkette vorangestellt.

Tabelle D-3. Zählen und Gruppieren

Element	Bedeutung	Beispiel
.	Der Punkt steht für ein beliebiges Zeichen mit Ausnahme des Zeilenvorschubzeichens.	mi. steht zum Beispiel für mir oder mit etc. m.n steht für mein, man etc.

Element	Bedeutung	Beispiel
*	Das Sternchen (*) entspricht null oder mehreren Instanzen des davor stehenden Elements.	mi* steht zum Beispiel für m, mi, mii, usw.
+	Das Plus-Zeichen (+) entspricht einer oder mehreren Instanzen des davor stehenden Elements.	mi+ steht zum Beispiel für mi, mii, miii, aber nicht für m
?	Das Fragezeichen steht für null oder eine Instanz des davor stehenden Elements.	mi?r entspricht also mr oder mir, aber nicht miir, miiir usw.
( )	Runde Klammern fassen alles, was sich zwischen ihnen befindet, zu einer Einheit zusammen.	m(ein)+ entspricht mein oder meinein oder meineinein usw. Das Plus-Zeichen (+) bezieht sich hier also auf die Zeichenfolge innerhalb der runden Klammern. Der reguläre Ausdruck beginnt mit einem m, gefolgt von mindestens einer ein-Gruppe.
[ ]	Eckige Klammern stehen für eine Reihe oder einen Bereich von Zeichen.	m[aeiou]+ entspricht ma, me, mi, mo, mu, maa, mae, mai usw. Das Plus-Zeichen bezieht sich auf die Zeichenfolge innerhalb der eckigen Klammern. Der reguläre Ausdruck beginnt mit einem m, gefolgt von einer beliebigen Kombination aus einem oder mehreren der Zeichen aeiou. m[A-Z] findet mA, mB, mC bis mZ. Die Zeichen in eckigen Klammern entsprechen allen groß geschriebenen Buchstaben zwischen A und Z.

Element	Bedeutung	Beispiel
[^]	Der Zirkumflex (^) innerhalb eckiger Klammern schließt die eingegebene Zeichenfolge oder den Zeichenbereich aus. Der reguläre Ausdruck enthält keines der Zeichen in diesem Bereich/dieser Zeichenfolge.	m[^aeiou] findet mb, mc, md usw., d. h. für "m" gefolgt von einem beliebigen Zeichen mit Ausnahme eines Vokals.
{ }	Geschweifte Klammern geben eine bestimmte Anzahl von Instanzen des davor stehenden Elements an. Ein einzelner Wert innerhalb der Klammern bedeutet, dass nur diese Anzahl von Instanzen gesucht wird. Mehrere durch Komma getrennte Werte stehen für eine Reihe gültiger Instanzen des davor stehenden Zeichens. Eine einzelne Ziffer vor einem Komma gibt eine Mindestanzahl ohne Obergrenze an.	mi{3} findet miii, also m gefolgt von genau drei Instanzen von ia. mi{2,4} findet mii, miii, miiii (aber nicht miiiii), also m gefolgt von zwei, drei oder vier Instanzen von i. mi{4,} findet miiii, miiiii, miiiiii usw., also m gefolgt von mindestens vier Instanzen von i.

Tabelle D-4. Zeichenklassen (Kurzschrift)

Element	Bedeutung	Beispiel
\d	Eine beliebige Ziffer, die funktional den Werten [0-9] oder [[:ziffer:]] entspricht.	\d findet 1, 12, 123 usw. (aber nicht 1b7), also eine Kombination aus einer oder mehreren Ziffern.
\D	Ein beliebiges Zeichen mit Ausnahme von Ziffern, das funktional den Werten [^0-9] oder [^[:digit:]] entspricht	\D entspicht a, ab, ab& usw. (aber nicht 1), also mindestens einem beliebigen Zeichen mit Ausnahme von Ziffern (0, 1, 2, 3, 4, 5, 6, 7, 8 oder 9)
\w	Beliebiges "Wort"-Zeichen, also ein beliebiges alphanumerisches Zeichen, das funktional den Werten [_A-Za-z0-9] oder [_[:alnum:]] entspricht	\w entspricht a, ab, a1, usw. (aber nicht !&), also einem oder mehreren groß oder klein geschriebenen Buchstaben oder Ziffern, nicht jedoch Satzzeichen oder Sonderzeichen

Element	Bedeutung	Beispiel
\W	Ein beliebiges, nicht-alphanumerisches Zeichen, das funktional den Werten [^_A-Za-z0-9] or [^_[:alnum:]] entspricht	\W entspricht *, & usw. (aber nicht ace oder a1), also einem oder mehreren beliebigen Zeichen mit Ausnahme von groß oder klein geschriebenen Buchstaben und Ziffern.
\s	Ein beliebiges Textumbruchzeichen, wie z. B. Leerzeichen, geschütztes Leerzeichen, das funktional den Werten [[:space]] entspricht	mutter\s findet 'mutter' gefolgt von einem beliebigen Textumbruchzeichen. Der Satz "Mutter kocht leckere Suppe" ist ein regulärer Ausdruck, nicht aber "Mir schmeckt Mutters Suppe".
\S	Ein beliebiges Nicht-Textumbruchzeichen, also kein Leerzeichen, geschütztes Leerzeichen usw., das funktional den Werten [^[:space]] entspricht	mutter\S findet 'mutter' gefolgt von einem beliebigen Zeichen mit Ausnahme von Textumbruchzeichen. Der Satz "Mutter kocht leckere Suppe" ist ein regulärer Ausdruck, nicht aber "Mir schmeckt Mutters Suppe".

Tabelle D-5. Zeichenklassen

Element	Bedeutung	Beispiel
[:alpha:]	Ein Zeichen des Alphabets	.REG. [[:alpha:]] findet abc, def, xxx, nicht aber 123 oder @#$.
[:digit:]	Eine beliebige Ziffer; entspricht funktional dem Ausdruck \d	.REG. [[:digit:]] steht für 1, 12, 123, usw.
[:alnum:]	Ein beliebiges alphanumerisches "Wort"-Zeichen; entspricht funktional dem Ausdruck \w	.REG. [[:alnum:]] findet abc, 123, nicht aber ~!@.

Element	Bedeutung	Beispiel
[:space:]	Ein beliebiges Textumbruchzeichen, wie z. B. Leerzeichen, geschütztes Leerzeichen; entspricht funktional dem Ausdruck [[:space]]	.REG. (mutter)[[:space:]] findet "mutter" gefolgt von einem beliebigen Textumbruchzeichen. Der Satz "Mutter kocht leckere Suppe" ist ein regulärer Ausdruck, nicht aber "Mir schmeckt Mutters Suppe".
[:graph:]	Ein beliebiges Zeichen mit Ausnahme von Leer-, Steuer- und ähnlichen Zeichen	.REG. [[:graph:]] findet 123, abc, xxx, ><”, nicht aber Leer- oder Steuerzeichen.
[:print:]	Ein beliebiges Zeichen (ähnlich dem Ausdruck [:graph:]), einschließlich Leerzeichen	.REG. [[:print:]] findet 123, abc, xxx, ><” und Leerzeichen.
[:cntrl:]	Ein beliebiges Steuerzeichen (z. B. STRG + C, STRG + X)	.REG. [[:cntrl:]] findet 0x03, 0x08, nicht aber abc, 123, !@#.
[:blank:]	Leer- und Tabulatorzeichen	.REG. [[:blank:]] findet Leer- und Tabulatorzeichen, nicht aber für 123, abc, !@#
[:punct:]	Satzzeichen	.REG. [[:punct:]] steht für ; : ? ! ~ @ # $ % & * ‘ “ , usw., nicht aber für 123, abc
[:lower:]	Ein beliebiger Kleinbuchstabe des Alphabets (Hinweis: Die Funktion „Übereinstimmung: Unterscheidung Groß-/ Kleinschreibung“ muss aktiviert sein, da sonst die Funktion [:alnum:] ausgeführt wird)	.REG. [[:lower:]] findet abc, Def, sTress, Do, usw., nicht aber für ABC, DEF, STRESS, DO, 123, !@#.
[:upper:]	Ein beliebiger Großbuchstabe des Alphabets (Hinweis: Die Funktion „Übereinstimmung: Unterscheidung Groß-/ Kleinschreibung“ muss aktiviert sein, da sonst die Funktion [:alnum:] ausgeführt wird)	.REG. [[:upper:]] findet ABC, DEF, STRESS, DO usw., nicht aber abc, Def, Stress, Do, 123, !@#.

Element	Bedeutung	Beispiel
[:xdigit:]	Die in einer Hexadezimalzahl zulässigen Ziffern (0-9a-fA-F)	.REG. [[:xdigit:]] steht für 0a, 7E, 0f usw.

Tabelle D-6. Pattern-Anker

Element	Bedeutung	Beispiel
^	Bezeichnet den Anfang einer Zeichenkette.	^(ungeachtet) findet einen beliebigen Textblock, der mit 'ungeachtet' beginnt. Der Satz 'Ungeachtet der Tatsache, dass mir Mutters Suppe schmeckt' ist ein regulärer Ausdruck, nicht aber 'Mutters Suppe schmeckt mir ungeachtet der Tatsache, dass'.
$	Bezeichnet das Ende einer Zeichenkette.	(ungeachtet)$ findet einen beliebigen Textblock, der mit 'ungeachtet' endet. Der Satz 'Mutters Suppe schmeckt mir der Tatsache ungeachtet' ist ein regulärer Ausdruck, nicht aber 'Ungeachtet der Tatsache, dass mir Mutters Suppe schmeckt'.

Tabelle D-7. Escape-Sequenzen und Literale

Element	Bedeutung	Beispiel
\	Zeichen, die in regulären Ausdrücken eine besondere Bedeutung haben (zum Beispiel "+").	(1) .REG. C\\C\+\+ steht für "C\C++". (2) .REG. * steht für *. (3) .REG. \? steht für ?.
\t	Bezeichnet ein Tabulatorzeichen.	(Stress)\t findet einen beliebigen Textblock, der die Zeichenfolge 'Stress', gefolgt von einem Tabulatorzeichen (ASCII 0x09) enthält.

Element	Bedeutung	Beispiel
\n	Bezeichnet ein Zeilenumbruchzeichen. **Hinweis** Ein Zeilenumbruchzeichen wird je nach Plattform unterschiedlich interpretiert. Unter Windows ist ein Zeilenumbruch ein Zeichenpaar, bestehend aus einem Wagenrücklauf und einem Zeilenvorschub. Unter Unix oder Linux wird beim Zeilenumbruch ein Zeilenvorschub und auf einem Macintosh ein Wagenrücklauf ausgeführt.	(Stress)\n\n steht für einen beliebigen Textblock, der die Zeichenkette 'Stress' gefolgt von zwei Zeilenumbruchzeichen (ASCII 0x0A) enthält.
\r	Bezeichnet ein Wagenrücklaufzeichen.	(Stress)\r steht für einen beliebigen Textblock, der die Zeichenkette 'Stress' gefolgt von einem Wagenrücklaufzeichen (ASCII 0x0D) enthält.

Element	Bedeutung	Beispiel
\b	Bezeichnet ein Rücksprungzeichen. OR Bezeichnet Grenzen.	(Stress)\b steht für einen beliebigen Textblock, der die Zeichenkette "Stress" gefolgt von einem Rücksprungzeichen (ASCII 0x08) enthält. Eine Wortgrenze (\b) bezeichnet eine Stelle zwischen einem Zeichen aus \w und einem aus \W (oder umgekehrt). Innerhalb der Zeichenklassen steht \b meist für ein Rücksprungzeichen, nicht für ein Wortgrenze. So kann der folgende reguläre Ausdruck der Sozialversicherungsnummer entsprechen: .REG. \b\d{3}-\d{2}-\d{4}\b
\xhh	Bezeichnet ein ASCII-Zeichen in Hexadezimalschreibweise, wobei hh für den zweistelligen Hexadezimalwert steht.	\x7E(\w){6} steht für einen beliebigen Textblock, der ein 'Wort' mit genau sechs alphanumerischen Zeichen mit vorangestellter Tilde (~) enthält. Die Wörter '~ab12cd' oder '~Pa3499' wären also reguläre Ausdrücke, das Wort '~hoppla' jedoch nicht.

Generator für reguläre Ausdrücke

Bei der Entscheidung, wie Regeln für die Funktion "Prävention vor Datenverlust" konfiguriert werden sollten, berücksichtigen Sie, dass der Generator für reguläre Ausdrücke nur einfache Ausdrücke gemäß den folgenden Regeln und Einschränkungen erzeugen kann:

- Variablen können nur alphanumerische Zeichen enthalten.
- Alle anderen Zeichen, wie [-], [/] usw., können nur als Konstanten verwendet werden.

- Variablenbereiche können nur von A-Z und 0-9 definiert werden, Bereiche könne nicht begrenzt werden, beispielsweise auf A-D.
- Bei regulären Ausdrücken, die von diesem Tool erzeugt wurden, wird die Groß-/Kleinschreibung berücksichtigt.
- Reguläre Ausdrücke, die von diesem Tool erzeugt wurden, können nur eine positive Übereinstimmung ergeben, keine negativen Übereinstimmungen ('wenn keine Übereinstimmung').
- Ausdrücke, die auf Ihrem Beispiel basieren, können nur mit genau derselben Anzahl von Zeichen und Leerzeichen wie in Ihrem Beispiel übereinstimmen. Das Tool kann keine Pattern erzeugen, die mit 'einem oder mehreren' eines bestimmten Zeichens oder einer Zeichenfolge übereinstimmen.

Komplexe Syntax von Ausdrücken

Ein Schlüsselwort-Ausdruck setzt sich aus Tokens zusammen. Dies ist die kleinste Einheit beim Vergleich einer Übereinstimmung zwischen Ausdruck und Inhalt. Ein Token kann ein Operator, ein logisches Symbol oder der Operand sein, z. B. das Argument oder der Wert, der den Operator auslöst.

Operatoren umfassen .AND., .OR., .NOT., .NEAR., .OCCUR., .WILD., .(. und .). Der Operand und der Operator müssen durch eine Leerstelle getrennt sein. Ein Operand kann außerdem mehrere Tokens enthalten. Weitere Informationen finden Sie unter *Schlüsselwörter auf Seite D-5*.

Funktionsweise regulärer Ausdrücke

Das folgende Beispiel beschreibt die Funktionsweise eines der Standardfilter, des Content-Filters für Sozialversicherungsnummern:

[Format] .REG. \b\d{3}-\d{2}-\d{4}\b

Der obere Ausdruck verwendet \b für ein Rücksprungzeichen, gefolgt von \d für eine beliebige Ziffer und dann von {x} für die Anzahl der Ziffern. Zum Schluss folgt - für einen Gedankenstrich. Dieser Ausdruck stimmt mit der Sozialversicherungsnummer überein. Die folgende Tabelle beschreibt die Zeichenfolgen, die mit dem Beispiel für reguläre Ausdrücke gefunden werden:

TABELLE D-8. Zahlen, die mit dem regulären Ausdruck für die Sozialversicherungsnummer übereinstimmen

.REG. \b\d{3}-\d{2}-\d{4}\b	
333-22-4444	Übereinstimmung
333224444	keine Übereinstimmung
333 22 4444	keine Übereinstimmung
3333-22-4444	keine Übereinstimmung
333-22-44444	keine Übereinstimmung

Wenn Sie den Ausdruck wie folgt ändern,

[Format] .REG. \b\d{3}\x20\d{2}\x20\d{4}\b

stimmt der neue Ausdruck mit der folgenden Sequenz überein:

333 22 4444

Ausschlussliste für Virensuche

Ausschlussliste für Security Agents

Diese Ausschlussliste enthält alle Trend Micro Produkte, die standardmäßig von der Suche ausgeschlossen werden.

TABELLE D-9. Security Agent Ausschlussliste

PRODUKTNAME	PFAD ZUM INSTALLATIONSORT
InterScan eManager 3.5x	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan eManager\CurrentVersion` `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` `ProgramDirectory=`

Produktname	Pfad zum Installationsort

ScanMail for Lotus Notes (SMLN) eManager NT	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Lotus Notes\CurrentVersion`
	`AppDir=`
	`DataDir=`
	`IniDir=`

InterScan Web Security Suite (IWSS)	`HKEY_LOCAL_MACHINE\Software\TrendMicro\Interscan Web Security Suite` `Programmverzeichnis = C:\Programme\Trend Micro\IWSS`
InterScan WebProtect	`HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\InterScan WebProtect\CurrentVersion` `ProgramDirectory=`
InterScan FTP VirusWall	`HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan FTP VirusWall\CurrentVersion` `ProgramDirectory=`
InterScan Web VirusWall	`HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan Web VirusWall\CurrentVersion` `ProgramDirectory=`
InterScan E-Mail VirusWall	`HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall\CurrentVersion` `ProgramDirectory={Installationslaufwerk}:\INTERS~1`
InterScan NSAPI Plug-In	`HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan NSAPI Plug-In\CurrentVersion` `ProgramDirectory=`
InterScan E-Mail VirusWall	`HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall \CurrentVersion` `ProgramDirectory=`

Produktname	Pfad zum Installationsort

IM Security (IMS)	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IM Security \CurrentVersion`
	`HomeDir=`
	`VSQuarantineDir=`
	`VSBackupDir=`
	`FBArchiveDir=`
	`FTCFArchiveDir=`

Produktname	Pfad zum Installationsort

ScanMail for Microsoft Exchange (SMEX)	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion`
	`TempDir=`
	`DebugDir=`
	
	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption`
	`BackupDir=`
	`MoveToQuarantineDir=`
	
	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption\Advance`
	`QuarantineFolder=`
	
	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption`
	`BackupDir=`
	`MoveToQuarantineDir=`
	
	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption\Advance`
	`QuarantineFolder=`

Produktname	Pfad zum Installationsort
ScanMail for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\ManualScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\QuarantineManager QMDir= Ermitteln Sie den Dateipfad für exclusion.txt aus HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion\HomeDir. Wechseln Sie in das Installationsverzeichnis (z. B. C:\Programme\Trend Micro\Messaging Security Agent\). Öffnen Sie die Datei exclusion.txt. C:\Programme\Trend Micro\Messaging Security Agent \Temp\ C:\Programme\Trend Micro\Messaging Security Agent \storage\quarantine\ C:\Programme\Trend Micro\Messaging Security Agent \storage\backup\ C:\Programme\Trend Micro\Messaging Security Agent \storage\archive\ C:\Programme\Trend Micro\Messaging Security Agent \SharedResPool

Suchausschlussliste für Messaging Security Agent (nur Advanced)

Wenn der Messaging Security Agent auf einem Microsoft Exchange Server (2000 oder höher) installiert wird, werden Microsoft Exchange-Datenbanken, Microsoft Exchange-Protokolldateien, Ordner des virtuellen Servers und das

Laufwerk M standardmäßig nicht durchsucht. Die Ausschlussliste wird in folgendem Verzeichnis gespeichert:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp
\CurrentVersion\Misc.

ExcludeExchangeStoreFiles=C:\Programme\Exchsrvr\mdbdata\

priv1.stm|C:\Programme\Exchsrvr\mdbdata\

priv1.edb|C:\Programme\Exchsrvr\mdbdata\

pub1.stm|C:\Programme\Exchsrvr\mdbdata\pub1.edb

ExcludeExchangeStoreFolders=C:\Programme\Exchsrvr\mdbdata\

|C:\Programme\Exchsrvr\Mailroot\vsi 1\Queue\

|C:\Programme\Exchsrvr\Mailroot\vsi 1\PickUp\

|C:\Programme\Exchsrvr\Mailroot\vsi 1\BadMail\
```

Fügen Sie andere für Microsoft Exchange empfohlene Ordner manuell zur Ausschlussliste hinzu. Siehe http://support.microsoft.com/kb/245822/.

SBS 2003 Ausschlüsse

Fügen Sie für SBS 2003 Folgendes manuell hinzu:

Microsoft Exchange Ausschlüsse	
Microsoft Exchange Server Datenbank	`C:\Programme\Exchsrvr\MDBDATA`
Microsoft Exchange MTA Dateien	`C:\Programme\Exchsrvr\Mtadata`
Microsoft Exchange Message Protokolldateien	`C:\Programme\Exchsrvr\server_name.log`
Microsoft Exchange SMTP Mailroot	`C:\Programme\Exchsrvr\Mailroot`
Microsoft Exchange Arbeitsdateien	`C:\Programme\Exchsrvr\MDBDATA`
Site Replication Service	`C:\Programme\Exchsrvr\srsdata` `C:\Programme\Exchsrvr\conndata`

IIS Ausschlüsse	
IIS Systemdateien	`C:\WINDOWS\system32\inetsrv`
IIS Komprimierungsordner	`C:\WINDOWS\IIS Temporary Compressed Files`
Ausschlüsse für den Domänencontroller	
Active Directory Datenbankdateien	`C:\WINDOWS\NTDS`
SYSVOL	`C:\WINDOWS\SYSVOL`
NTFRS Datenbankdateien	`C:\WINDOWS\ntfrs`
Windows SharePoint Services Ausschlüsse	
Temporäre SharePoint Ordner	`C:\windows\temp\FrontPageTempDir`
Ordnerausschlüsse für Client-Desktops	
Windows Update Speicher	`C:\WINDOWS\SoftwareDistribution\DataStore`
Weitere Ausschlüsse	
Datenbanken auf Wechseldatenträgern (bei SBS Backups)	`C:\Windows\system32\NtmsData`
"Failed Mail"-Ordner für SBS POP3 Connector	`C:\Programme\Microsoft Windows Small Business Server\Networking\POP3\Failed Mail`
Ordner für eingehende Nachrichten für SBS POP3 Connector	`C:\Programme\Microsoft Windows Small Business Server\Networking\POP3\Incoming Mail`

Windows Update Speicher	`C:\WINDOWS\SoftwareDistribution\DataStore`
DHCP Datenbankspeicher	`C:\WINDOWS\system32\dhcp`
WINS Datenbankspeicher	`C:\WINDOWS\system32\wins`

Service Pack

Ein Service Pack ist eine Kombination von Hotfixes, Patches und Funktionserweiterungen, die den Status eines Produkt-Upgrades haben. Service Packs (sowohl von Windows als auch andere) verfügen über ein Setup-Programm und ein Setup-Skript.

Trojanerports

Trojaner-Ports werden häufig von Trojanern zum Verbindungsaufbau mit Clients verwendet. Während eines Ausbruchs blockiert Worry-Free Business Security die folgenden Portnummern, die eventuell von Trojanern verwendet werden.

Tabelle D-10. Trojanerports

Portnummer	Trojaner	Portnummer	Trojanisches Pferd
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

Portnummer	Trojaner	Portnummer	Trojanisches Pferd
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
7300	Net Spy	1234	Valvo line

Dateien, die nicht gesäubert werden können

Die Viren-Scan-Engine kann folgende Dateien nicht säubern:

Tabelle D-11. Lösungen bei nicht zu säubernden Dateien

Nicht zu säubernde Datei	Erklärung und Lösung
Mit Trojanern infizierte Dateien	Trojaner sind Programme, die unerwartete oder unberechtigte, in der Regel aber schädliche Aktionen durchführen. Es werden beispielsweise Meldungen angezeigt, Dateien gelöscht oder Festplatten formatiert. Da Trojaner keine Dateien infizieren, ist kein Säubern erforderlich. Lösung: Die Damage Cleanup Engine und die Damage Cleanup Template entfernen Trojaner.
Mit Würmern infizierte Dateien	Ein Wurm ist ein eigenständiges Programm (oder eine Gruppe von Programmen), das funktionsfähige Kopien von sich selbst oder seinen Segmenten an andere Client-Systeme verteilen kann. Würmer verbreiten sich normalerweise über Netzwerkverbindungen oder E-Mail-Anhänge. Würmer sind eigenständige Programme und können deshalb nicht gesäubert werden. Lösung: Trend Micro empfiehlt, Würmer zu löschen.
Infizierte, schreibgeschützte Dateien	Lösung: Heben Sie den Schreibschutz auf, damit die Datei gesäubert werden kann.
Kennwortgeschützte Dateien	Kennwortgeschützte Dateien umfassen kennwortgeschützte, komprimierte Dateien oder kennwortgeschützte Microsoft Office-Dateien. Lösung: Heben Sie den Kennwortschutz auf, damit die Datei gesäubert werden kann.
Sicherungsdateien	Bei Dateien mit den Erweiterungen RB0~RB9 handelt es sich um Sicherungskopien infizierter Dateien. Beim Säuberungsprozess werden diese Kopien für den Fall erstellt, dass der Virus/die Malware die infizierte Datei beim Säubern beschädigt. Lösung: Wenn die Datei gesäubert werden konnte, müssen Sie die Sicherungskopie der infizierten Datei nicht aufbewahren. Wenn der Client fehlerfrei funktioniert, können Sie die Kopie löschen.
Infizierte Dateien im Papierkorb	Infizierte Dateien im Papierkorb des Systems können möglicherweise nicht entfernt werden, wenn das System aktiv ist. Lösung:

Nicht zu säubernde Datei	Erklärung und Lösung

	1. Starten Sie den Client im MS-DOS Modus neu.
	2. Öffnen Sie ein Eingabeaufforderungsfenster.
	3. Geben Sie zum Löschen der Dateien folgende Befehle ein:
	`cd \`
	`cd recycled`
	`del *.* /S`
	Mit dem letzten Befehl werden alle Dateien im Papierkorb gelöscht.

Infizierte Dateien im Windows Ordner "Temp" oder im Internet Explorer-Ordner "Temporary Internet Files"	Dateien in diesen Ordnern können möglicherweise nicht gesäubert werden, da sie vom Client verwendet werden. Möglicherweise handelt es sich bei den Dateien, die gesäubert werden sollen, um temporäre Dateien, die für den Betrieb von Windows benötigt werden.
	Lösung:
	1. Starten Sie den Client im MS-DOS Modus neu.
	2. Wenn sich die infizierte Datei im Windows Ordner "Temp" befindet:
	a. Öffnen Sie eine Eingabeaufforderung und navigieren Sie zum Windows-Ordner 'Temp' (standardmäßig unter `C:\Windows\Temp`).
	b. Geben Sie zum Löschen der Dateien folgende Befehle ein:
	`cd temp`
	`attrib -h`
	`del *.* /S`
	Mit dem letzten Befehl werden alle Dateien im Windows Temp-Ordner gelöscht.
	c. Starten Sie den Client im Normalmodus neu.
	3. Wenn sich die infizierte Datei im tempoären Ordner von Internet Explorer befindet:
	a. Öffnen Sie eine Eingabeaufforderung und navigieren Sie zum Internet Explorer-Ordner 'Temp' (standardmäßig unter

Nicht zu säubernde Datei	Erklärung und Lösung

	C:\Users\<Your user name>\AppData\Local \Microsoft\Windows\Temporary Internet Files).
	b. Geben Sie zum Löschen der Dateien folgende Befehle ein:
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	Mit dem letzten Befehl werden alle Dateien im temporären Ordner des Internet Explorers gelöscht.
	c. Starten Sie den Client im Normalmodus neu.

Dateien, die mit einem unbekannten Komprimierungs-Tool bearbeitet wurden.	Lösung: Dekomprimieren Sie die Dateien.
Gesperrte Dateien oder Dateien, die gerade ausgeführt werden.	Lösung: Entsperren Sie die Dateien oder warten Sie, bis die Dateien ausgeführt wurden.
Beschädigte Dateien.	Lösung: Löschen Sie die Dateien.

Stichwortverzeichnis

A

Abfragehandhabung für kontextbezogene Intelligenz, 8-7
ActiveAction, 7-16
Anmeldeskript-Setup, 3-7, 3-8, 3-12
Anregungen und Kritik, C-6
ARP-Konflikt, D-4
Aufgaben vor der Installation, 3-10, 3-18, 3-22
AutoPcc.exe, 3-7, 3-8, 3-12

B

Bootsektorvirus, 1-10
Bösartiger ActiveX-Code, 1-10
Bösartiger Java-Code, 1-10

C

Client-Installation
    Anmeldeskript-Setup, 3-12
    Client Packager, 3-14
    mit Vulnerability Scanner, 3-22
Client Packager, 3-8, 3-14–3-16
    Einstellungen, 3-15
    Verteilung, 3-17
COM-Dateiinfektor, 1-10

D

Damage Cleanup Engine, 8-6
Damage Cleanup Services, 3-4
Damage Cleanup Template, 8-6
Deinstallation
    Verwenden des Deinstallationsprogramms, 3-43
DHCP-Einstellungen, 3-25
Dokumentation, xiv

E

Early Boot Cleanup Driver, 8-7
EICAR-Testskript, 1-10
Einheitliches Skriptanalysemuster, 8-10
Erkennungs-Pattern der Verhaltensüberwachung, 8-8
EXE-Dateiinfektor, 1-10
Externe Geräte, Schutz, 8-9

F

file reputation, 1-4
Firewall
    Vorteile, 5-30
Fortgeschrittenes Bedrohungssuchmaschine, 8-7
Fragmentiertes IGMP, D-5
Fragment zu groß, D-4

H

Herkömmliche Suche, 5-4
Hotfixes, 8-10
HTML-Virus, 1-10

I

IDS, D-3
Inkrementelles Pattern, 8-12
Installationsmethoden für den Security Agent, 3-7
IntelliTrap Ausnahme-Pattern, 8-5
IntelliTrap Pattern, 8-5
Intrusion Detection System, D-3
IPv6-Unterstützung, B-2
    Einschränkungen, B-3, B-4
    IPv6-Adressen anzeigen, B-6

J
JavaScript-Virus, 1-10

K
Kennwortkomplexität, 6-63
Kerndienst der Verhaltensüberwachung, 8-9
Komponenten, 8-4
Komponentenduplizierung, 8-12
Kontextintelligenz-Pattern, 8-7

L
LAND Attack, D-5

M
Makrovirus, 1-10
Maschine für Kontextbezogene Intelligenz, 8-7
Muster der Programmsinspektionsüberwachung, 8-9

N
Netzwerkvirus, 5-30
Neue Funktionen, 1-2

P
Packer, 1-10
Patches, 8-10
Pattern der allgemeinen Firewall, 8-8
Pattern der erweiterten Bedrohungskorrelation, 8-7
Pattern der Richtliniendurchsetzung, 8-9
Pattern für die Prävention von Angriffen auf Browser, 8-10
Pattern für digitale Signaturen, 8-9
Pattern zur Konfiguration der Verhaltensüberwachung, 8-9
Ping-of-Death, D-4
Plug-in Manager, 3-4
Programme, 8-4

Q
Quarantäne-Ordner, 5-18, 14-19

R
Remote-Installation, 3-8
Rootkit-Erkennung, 8-9

S
Schadensbehebungsmuster, 8-9
Scherzprogramm, 1-9
Security Agent-Installation
    über die Webkonsole, 3-18
Server-Update
    Komponentenduplizierung, 8-12
    manuelles Update, 8-14
    Zeitgesteuertes Update, 8-15
Sicherheits-Patches, 8-10
Sicherheitsrichtlinien
    Kennwortkomplexität
        Voraussetzungen, 6-63
Sicherheitsrisiken, 1-11, 1-12
    Spyware/Grayware, 1-11, 1-12
smart protection, 1-3, 1-4
    Smart Protection Network, 1-3
Smart Protection
    File-Reputation-Dienste, 1-4
    Web Reputation-Dienste, 1-4
Smart Protection Network, 1-3
Smart Scan, 5-4
spyware/grayware
    spyware, 1-11

Spyware/Grayware, 1-11, 1-12
adware, 1-11
Anwendungen zum Entschlüsseln von Kennwörtern, 1-12
Dialer, 1-11
Hacker-Tools, 1-12
Scherzprogramme, 1-11
Tools für den Remote-Zugriff, 1-12
Spyware/Grayware-Pattern, 8-8
Spyware/Grayware Scan Engine, 8-8
Suchaktionen
Spyware/Grayware, 7-15
Sucharten, 3-4
Suche nach Spyware/Grayware
Aktionen, 7-15
Suchmethode, 3-15
support
Probleme schneller beheben, C-4
SYN-Flooding, D-4

T

Teardrop, D-4
Testvirus, 1-10
Tiny Fragment Attack, D-4
Treiber der Verhaltensüberwachung, 8-8
Trojanisches Pferd, 1-10, 8-6

U

Überlappendes Fragment, D-4
Update Agent, 3-4

V

VBScript-Virus, 1-10
Verschlüsselte Dateien, 14-18
Viren-Enzyklopädie, 1-9
Viren-Pattern, 8-5, 8-17
Viren-Scan-Engine, 8-5
virus/malware, 1-9
Virus/Malware, 1-9, 1-10
Bootsektorvirus, 1-10
Bösartiger ActiveX-Code, 1-10
Bösartiger Java-Code, 1-10
COM- und EXE-Dateien-Infektor, 1-10
Makrovirus, 1-10
packer, 1-10
Scherzprogramm, 1-9
testvirus, 1-10
Trojanisches Pferd, 1-10
Typen, 1-9, 1-10
VBScript-, JavaScript- oder HTML-Virus, 1-10
Wahrscheinlich Virus/Malware, 1-9
Wurm, 1-10
Vulnerability Scanner, 3-8, 3-22
Beschreibung des Computers, Abfrage, 3-31
DHCP-Einstellungen, 3-25
Ping-Einstellungen, 3-32

W

Wahrscheinlich Virus/Malware, 1-9
Web-Installationsseite, 3-7
Webkonsole, 2-4, 2-5
Info über, 2-4
Voraussetzungen, 2-5
web reputation, 1-4, 3-4, 5-2
WFBS
Dokumentation, xiv
Wurm, 1-10

TREND MICRO INCORPORATED
Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland
Tel.: +49 (0) 811 88990-700 Fax: +4981188990799 info@trendmicro.com

www.trendmicro.com

Item Code: WFGM108699/190701