TREND MICRO

XG

OfficeScan™

Service Pack 1

Administratorhandbuch

Für große und mittelständische Unternehmen

Endpoint Security

Protected Cloud

Web Security

Trend Micro Deutschland GmbH 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/enterprise/officescan.aspx

Trend Micro, the Trend Micro t-ball logo, OfficeScan, Control Manager, Damage Cleanup Services, eManager, InterScan, Network VirusWall, ScanMail, ServerProtect, and TrendLabs sind Marken oder eingetragene Marken von Trend Micro Deutschland GmbH. Alle anderen Produkt- oder Firmennamen können Marken oder eingetragene Marken ihrer Eigentümer sein.

Copyright © 2018. Trend Micro Deutschland GmbH. Alle Rechte vorbehalten.

Dokument-Nr.: OSEMXG7952/170822

Release-Datum: Januar 2018

Geschützt durch U.S. Patent-Nr.: 5,951,698

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:

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

Inhaltsverzeichnis

Vorwort

Vorwort xi

OfficeScan Dokumentation xii

Zielgruppe xiii

Dokumentationskonventionen xiii

Begriffe xiv

Teil I: Einführung und erste Schritte

Kapitel 1: Einführung in OfficeScan

Info über OfficeScan 1-2

Was ist neu in OfficeScan XG Service Pack 1 1-2

Wichtigste Funktionen und Vorteile 1-7

Der OfficeScan Server 1-11

Das OfficeScan Agent 1-13

Integration in Trend Micro Produkte und Services 1-13

Kapitel 2: Erste Schritte in OfficeScan

Die Webkonsole 2-2

Die Dashboard 2-5

Active Directory-Integration 2-36

Die OfficeScan Agent-Hierarchie 2-40

OfficeScan Domänen 2-54

Kapitel 3: Erste Schritte mit Datenschutz

Datenschutzinstallation 3-2
Datenschutzlizenz 3-4
Datenschutz auf OfficeScan Agenten verteilen 3-6
Ordner der forensischen Daten und DLP-Datenbank 3-9
Den Datenschutz deinstallieren 3-15

Teil II: Schützen OfficeScan Agenten

Kapitel 4: Trend Micro Smart Protection verwenden

Info über Trend Micro Smart Protection 4-2
Smart Protection Dienste 4-3
Smart Protection Quellen 4-6
Pattern-Dateien von Smart Protection 4-8
Smart Protection Services einrichten 4-13
Smart Protection Services verwenden 4-33

Kapitel 5: Den OfficeScan Agent installieren

OfficeScan Agent Erstinstallationen 5-2
überlegungen zur Installation 5-2
Überlegungen zur Verteilung 5-12
Zu OfficeScan Agent migrieren 5-67
Nach der Installation 5-71
OfficeScan Agent deinstallieren 5-74

Kapitel 6: Schutzfunktionen aktuell halten

OfficeScan Komponenten und Programme 6-2
Update-Übersicht 6-12

OfficeScan Server-Updates 6-16
Updates für den integrierten Smart Protection Server 6-29
OfficeScan Agent-Updates 6-29
Update-Agents 6-59
Komponenten-Update - Zusammenfassung 6-68

Kapitel 7: Nach Sicherheitsrisiken suchen

Info über Sicherheitsrisiken 7-2
Suchmethodentypen 7-9
Suchtypen 7-16
Gemeinsame Einstellungen für alle Suchtypen 7-29
Suchberechtigungen und andere Einstellungen 7-62
Allgemeine Sucheinstellungen 7-79
Benachrichtigungen bei Sicherheitsrisiken 7-90
Sicherheitsrisiko-Protokolle 7-101
Ausbrüche von Sicherheitsrisiken 7-117

Kapitel 8: Schutz vor unbekannten Bedrohungen

Vorausschauendes Maschinenlernen 8-2
Verdächtiger Verbindungsdienst 8-6
Exemplar Zusendung 8-11
Protokolle unbekannter Bedrohungen 8-12

Kapitel 9: Verhaltensüberwachung verwenden

Verhaltensüberwachung 9-2
Einstellungen der globalen Verhaltensüberwachung konfigurieren 9-19
Verhaltensüberwachungsberechtigungen 9-21

Benachrichtigungen der Verhaltensüberwachung für OfficeScan Agent-Benutzer 9-23

Verhaltensüberwachungsprotokolle 9-24

Kapitel 10: Die Gerätesteuerung verwenden

Gerätesteuerung 10-2

Berechtigungen für Speichergeräte 10-4

Berechtigungen für Nicht-Speichergeräte 10-11

Zugriff auf externe Geräte verwalten (Datenschutz aktiviert) 10-11

Zugriff auf externe Geräte verwalten (Datenschutz nicht aktiviert) .. 10-16

Gerätesteuerungsbenachrichtigungen ändern 10-19

Protokolle der Gerätesteuerung 10-19

Kapitel 11: Prävention vor Datenverlust verwenden

Prävention vor Datenverlust (Data Loss Prevention, DLP) 11-2

Richtlinien für 'Prävention vor Datenverlust' 11-3

Datenbezeichnertypen 11-6

Vorlagen für 'Prävention vor Datenverlust' 11-22

DLP-Kanäle 11-27

Aktionen der Funktion "Prävention vor Datenverlust" 11-42

Ausnahmen für Prävention vor Datenverlust 11-45

Richtlinienkonfiguration der Funktion "Prävention vor Datenverlust" 11-51

Benachrichtigungen der Funktion "Prävention vor Datenverlust" 11-58

Protokolle für 'Prävention vor Datenverlust' 11-63

Kapitel 12: Verwenden von Web Reputation

Info über Internet-Bedrohungen 12-2

Command & Control-Kontaktalarmdienste 12-2

Web Reputation 12-4
Web-Reputation-Richtlinien 12-5
Benachrichtigungen über Internet-Bedrohungen für Agent-Benutzer 12-14
C&C-Callback-Benachrichtigungen für Administratoren 12-15
C&C-Kontaktalarmbenachrichtigungen für Agent-Benutzer 12-19
C &C-Callback-Ausbrüche 12-20
Protokolle für Internet-Bedrohungen 12-23

Kapitel 13: Die OfficeScan Firewall verwenden

Die OfficeScan Firewall 13-2
Die OfficeScan Firewall aktivieren oder deaktivieren 13-6
Firewall-Richtlinien und -Profile 13-8
Firewall-Berechtigungen 13-26
Allgemeine Firewall-Einstellungen 13-28
Benachrichtigungen bei Firewall-Verstößen für OfficeScan Agent-Benutzer 13-31
Firewall-Protokolle 13-32
Ausbrüche bei Firewall-Verstoß 13-34
Die OfficeScan Firewall testen 13-36

Teil III: OfficeScan Server und Agents verwalten

Kapitel 14: Den OfficeScan Server verwalten

Rollenbasierte Administration 14-3
Trend Micro Control Manager 14-25
Das Einstellungsexporttool von OfficeScan 14-33
Einstellungen für Liste der verdächtigen Objekte 14-38

Referenzserver 14-40
Einstellungen für die Administratorbenachrichtigungen 14-43
Systemereignisprotokolle 14-45
Protokollmanagement 14-47
Lizenzen 14-51
OfficeScan Datenbanksicherung 14-54
SQL Server Migration Tool 14-56
Einstellungen des OfficeScan Webservers/Agents 14-61
Kommunikation zwischen Server und Agents 14-62
Kennwort der Webkonsole 14-68
Einstellungen der Webkonsole konfigurieren 14-69
Quarantäne-Manager 14-70
Server Tuner 14-71
Smart Feedback 14-73

Kapitel 15: OfficeScan Agent verwalten

Endpunktspeicherort 15-2
OfficeScan Agent Programmverwaltung 15-6
Agent-Server-Verbindung 15-28
OfficeScan Agent Proxy-Einstellungen 15-53
OfficeScan Agent-Informationen anzeigen 15-60
Agent-Einstellungen importieren und exportieren 15-60
Einhaltung von Sicherheitsrichtlinien 15-62
Unterstützung für Trend Micro Virtual Desktop 15-84
Globale Agent-Einstellungen 15-99
Agent-Berechtigungen und weitere Einstellungen konfigurieren 15-101

Teil IV: Zusätzlichen Schutz bereitstellen

Kapitel 16: Schützen externer Agents

Edge-Relais-Server 16-2
Systemanforderungen des Edge-Relais-Servers 16-3
Installieren des Edge-Relais-Servers 16-4
Herstellen einer Verbindung zum Edge-Relais-Server 16-13
Verwalten der Edge-Relais-Server-Verbindung 16-15
Verwalten von Edge-Relais-Server-Zertifikaten 16-16

Kapitel 17: Plug-in Manager verwenden

Info über den Plug-in Manager 17-2
Plug-in Manager Installation 17-3
Verwaltung nativer OfficeScan Funktionen 17-4
Plug-in-Programme verwalten 17-5
Plug-in Manager deinstallieren 17-12
Fehlersuche in Plug-in Manager 17-13

Kapitel 18: Ressourcen zur Fehlerbehebung

Support-Informationssystem 18-2
Case Diagnostic Tool 18-2
Trend Micro Performance Tuning Tool 18-2
OfficeScan Serverprotokolle 18-3
OfficeScan Agent Protokolle 18-15

Kapitel 19: Technischer Support

Ressourcen zur Fehlerbehebung 19-2
Kontaktaufnahme mit Trend Micro 19-3
Verdächtige Inhalte an Trend Micro senden 19-4
Sonstige Ressourcen 19-6

Anhänge

Anhang A: IPv6-Unterstützung in OfficeScan

IPv6-Unterstützung für OfficeScan Server und Agents A-2
IPv6-Adressen konfigurieren A-6
Fenster, auf denen IP-Adressen angezeigt werden A-7

Anhang B: Unterstützung für Windows Server Core

Unterstützung für Windows Server Core B-2
Installationsmethoden für Windows Server Core B-2
OfficeScan Agent-Funktionen unter Windows Server Core B-6
Windows Server Core Befehle B-7

Anhang C: Unterstützung für Windows 8/8.1/10 und Windows Server 2012/2016

Informationen zu Windows 8/8.1/10 und Windows Server 2012/2016 ..... C-2
OfficeScan Funktionsunterstützung im Benutzeroberflächenmodus ... C-5
Internet Explorer 10/11 und Microsoft Edge C-6

Anhang D: OfficeScan Rollback

Durchführen eines Rollbacks des OfficeScan Servers und der OfficeScan Agenten mit dem Serversicherungspaket D-2

Anhang E: Glossar

ActiveUpdate E-2
Komprimierte Datei E-2
Cookie E-2
Denial-of-Service-Angriff E-2
DHCP E-3

DNS E-3
Domänenname E-3
Dynamische IP-Adresse E-4
ESMTP E-4
Endbenutzer-Lizenzvereinbarung E-4
Fehlalarm E-4
FTP E-5
GeneriClean E-5
Hotfix E-5
HTTP E-6
HTTPS E-6
ICMP E-6
IntelliScan E-6
IntelliTrap E-7
IP E-7
Java-Datei E-8
LDAP E-8
Listening-Port E-8
MCP Agent E-8
Kombinierte Bedrohungen E-9
NAT E-9
NetBIOS E-9
Ein-Wege-Kommunikation E-9
Patch E-10
Phishing-Angriff E-10
Ping E-11
POP3 ..... E-11

Proxy-Server E-11
RPC E-11
Sicherheits-Patch E-11
Service Pack E-12
SMTP E-12
SNMP E-12
SNMP-Trap E-12
SSL E-13
SSL-Zertifikat E-13
TCP E-13
Telnet E-13
Trojanerports E-13
Vertrauenswürdiger Port E-15
Zwei-Wege-Kommunikation E-16
UDP E-16
Dateien, die nicht gesäubert werden können E-16

Stichwortverzeichnis

Stichwortverzeichnis IN-1

Vorwort

Vorwort

Dieses Dokument enthält Informationen über die ersten Schritte, die Verfahren zur agent-Installation und die Verwaltung von OfficeScan Server und agent.

Es werden folgende Themen behandelt:

- *OfficeScan Dokumentation auf Seite xii*
- *Zielgruppe auf Seite xiii*
- *Dokumentationskonventionen auf Seite xiii*
- *Begriffe auf Seite xiv*

OfficeScan Dokumentation

Die OfficeScan Dokumentation umfasst Folgendes:

TABELLE 1. OfficeScan Dokumentation

DOKUMENTATION	BESCHREIBUNG
Installations- und Upgrade-Handbuch	Ein PDF-Dokument mit einer Beschreibung der Anforderungen und Verfahren zum Installieren des OfficeScan Servers sowie zum Aktualisieren des Servers und der Agents **Hinweis** Das Installations- und Upgrade-Handbuch enthält möglicherweise keine Informationen zu Nebenversionen, Service Packs oder Patches.
Systemvoraussetzungen	Ein PDF-Dokument, in dem die Mindest- und die empfohlenen Systemanforderungen für die Installation des OfficeScan Servers und die Aktualisierung des Servers und der Agents beschrieben werden
Administratorhandbuch	Ein PDF-Dokument mit Informationen über die ersten Schritte, die Verfahren zur OfficeScan Agent-Installation sowie über die OfficeScan Server- und Agent-Verwaltung
Hilfe	Im WebHelp- oder CHM-Format erstellte HTML-Dateien, die Anleitungen, allgemeine Benutzerhinweise und feldspezifische Informationen enthalten. Auf die Hilfe kann über die OfficeScan Server- und Agent-Konsolen sowie über das OfficeScan Master Setup zugegriffen werden.
Readme-Datei	Enthält eine Liste bekannter Probleme und grundlegende Installationsschritte. Die Datei kann auch neueste Produktinformationen enthalten, die noch nicht in der Hilfe oder in gedruckter Form zur Verfügung stehen.

DOKUMENTATION	BESCHREIBUNG
Knowledge Base	Eine Online-Datenbank mit Informationen zur Problemlösung und Fehlerbehebung. Sie enthält aktuelle Hinweise zu bekannten Softwareproblemen. Die Knowledge Base finden Sie im Internet unter folgender Adresse: http://esupport.trendmicro.com

Sie können die neueste Version der PDF-Dokumente und Readme-Dateien von der folgenden Adresse herunterladen:

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

Zielgruppe

Die OfficeScan Dokumentation ist für die folgenden Benutzergruppen gedacht:

- OfficeScan Administratoren: Verantwortlich für die Verwaltung von OfficeScan, einschließlich Installation und Verwaltung von OfficeScan Servern und OfficeScan Agent. Von diesen Benutzern wird erwartet, dass sie über detaillierte Kenntnisse im Zusammenhang mit der Netzwerk- und Serververwaltung verfügen.
- Endbenutzer: Benutzer, auf deren Endpunkte der OfficeScan Agent installiert ist. Die Endpunktkenntnisse dieser Benutzergruppe reichen vom Anfänger bis zum erfahrenen Anwender.

Dokumentationskonventionen

Die Dokumentation verwendet die folgenden Konventionen:

TABELLE 2. Dokumentationskonventionen

KONVENTION	BESCHREIBUNG
GROSSSCHRIFT	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur

KONVENTION	BESCHREIBUNG
Fettdruck	Menüs und Menübefehle, Schaltflächen, Registerkarten und Optionen
Kursivdruck	Verweise auf andere Dokumente
`Schreibmaschinenschrift`	Muster für Befehlszeilen, Programmcode, Internet-Adressen, Dateinamen und Programmanzeigen
Navigation > **Pfad**	Der Navigationspfad zu einem bestimmten Fenster **Datei** > **Speichern** bedeutet beispielsweise, dass Sie in der Benutzeroberfläche im Menü **Datei** auf **Speichern** klicken
Hinweis	Konfigurationshinweise
Tipp	Empfehlungen oder Vorschläge
Wichtig	Informationen zu den erforderlichen oder standardmäßigen Konfigurationseinstellungen und Produktbeschränkungen
Warnung!	Wichtige Aktionen und Konfigurationsoptionen

Begriffe

Die folgende Tabelle enthält die offizielle Terminologie, die innerhalb der OfficeScan Dokumentation verwendet wird:

TABELLE 3. OfficeScan Terminologie

BEGRIFFE	BESCHREIBUNG
OfficeScan Agent	Das OfficeScan agent Programm

Begriffe	Beschreibung
Agent-Endpunkt	Der Endpunkt, auf dem der OfficeScan Agent installiert ist
Agent-Benutzer (oder Benutzer)	Die Person, die den OfficeScan Agent auf dem Agent-Endpunkt verwaltet
Server	Das OfficeScan Server-Programm.
Server-Computer	Der Endpunkt, auf dem der OfficeScan Server installiert ist
Administrator (oder OfficeScan Administrator)	Die Person, die den OfficeScan Server verwaltet.
Konsole	Die Benutzeroberfläche zur Konfiguration und Verwaltung der Einstellungen für den OfficeScan Server und Agent Die Konsole für das OfficeScan Server-Programm wird "Webkonsole" und die Konsole für das OfficeScan Agent-Programm wird "Agent-Konsole" genannt.
Sicherheitsrisiko	Der Oberbegriff für Viren/Malware, Spyware/Grayware und Internet-Bedrohungen
Lizenz-Dienst	Umfasst die Module Antivirus, Damage Cleanup Services, Web Reputation und Anti-Spyware, die alle bei der Installation von OfficeScan Server aktiviert werden.
OfficeScan Dienst	über die Microsoft Management-Konsole (MMC) verwaltete Dienste. Beispiel: `ofcservice.exe`, der OfficeScan Master Service.
Programm	Hierzu gehören der OfficeScan Agent und der Plug-in Manager.
Komponenten	Suchen und entdecken Sicherheitsrisiken und führen Aktionen gegen sie durch.

BEGRIFFE	BESCHREIBUNG

`Installationsordner des Agents`	Der Ordner auf dem Endpunkt, der die OfficeScan Agent-Dateien enthält. Wenn Sie während der Installation die Standardeinstellungen akzeptieren, finden Sie den Installationsordner an einem der folgenden Speicherorte:
	`C:\Programme\Trend Micro\OfficeScan Client`
	`C:\Programme (x86)\Trend Micro\OfficeScan Client`

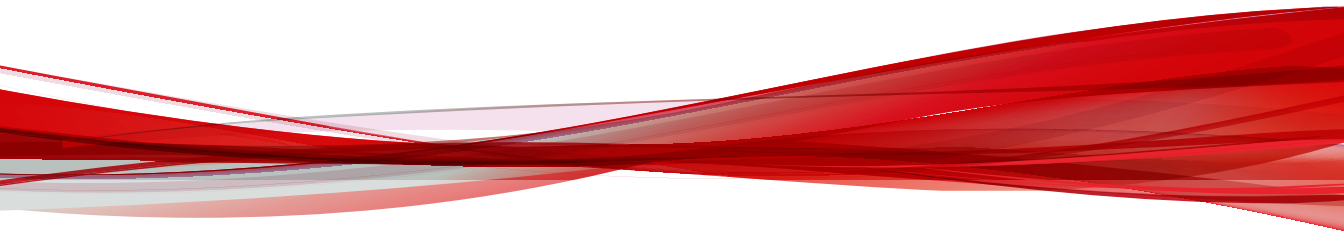
`Installationsordner des Servers`	Der Ordner auf dem Endpunkt, der die OfficeScan-Serverdateien enthält. Wenn Sie während der Installation die Standardeinstellungen akzeptieren, finden Sie den Installationsordner an einem der folgenden Speicherorte:
	`C:\Programme\Trend Micro\OfficeScan`
	`C:\Programme (x86)\Trend Micro\OfficeScan`
	Wenn sich z. B. eine bestimmte Datei im Installationsordner des Servers unter `\PCCSRV` befindet, lautet der vollständige Pfad der Datei:
	`C:\Programme\Trend Micro\OfficeScan\PCCSRV \<file_name>`.

Agent der intelligenten Suche	Ein OfficeScan Agent wurde so konfiguriert, dass die intelligente Suche verwendet wird.
Agent der herkömmlichen Suche	Ein OfficeScan Agent wurde so konfiguriert, dass die herkömmliche Suche verwendet wird.

Begriffe	Beschreibung
Dual-stack	Elemente, die sowohl über IPv4- als auch IPv6-Adressen verfügen. Beispiel: • Endpunkte mit IPv4- und IPv6-Adressen • OfficeScan Agents auf Dual-Stack-Endpunkten installiert • Update-Agents, die Updates an Agents verteilen • Ein Dual-Stack-Proxy-Server, wie etwa DeleGate, kann zwischen IPv4- und IPv6-Adressen konvertieren
Reines IPv4	Ein Gerät, das nur über IPv4-Adressen verfügt
Reines IPv6	Ein Gerät, das nur über IPv6-Adressen verfügt
Plug-in-Lösungen	Native OfficeScan Funktionen und Plug-in-Programme, die über Plug-in Manager bereitgestellt werden

Teil I

Einführung und erste Schritte



Kapitel 1

Einführung in OfficeScan

Dieses Kapitel enthält eine Einführung in Trend Micro™ OfficeScan™ und bietet einen überblick über die einzelnen Funktionen.

Es werden folgende Themen behandelt:

- *Info über OfficeScan auf Seite 1-2*
- *Was ist neu in OfficeScan XG Service Pack 1 auf Seite 1-2*
- *Wichtigste Funktionen und Vorteile auf Seite 1-7*
- *Der OfficeScan Server auf Seite 1-11*
- *Das OfficeScan Agent auf Seite 1-13*
- *Integration in Trend Micro Produkte und Services auf Seite 1-13*

Info über OfficeScan

Trend Micro™ OfficeScan™ schützt Unternehmensnetzwerke vor Malware, Netzwerkviren, webbasierten Bedrohungen, Spyware und kombinierten Bedrohungen. OfficeScan ist eine integrierte Lösung und besteht aus dem OfficeScan Agent-Programm am Endpunkt sowie einem Serverprogramm, das alle agents verwaltet. Der OfficeScan Agent überwacht den Endpunkt und sendet dessen Sicherheitsstatus an den Server. Über die webbasierte Management-Konsole vereinfacht der Server das Festlegen koordinierter Sicherheitsrichtlinien und verteilt Updates an alle agents.

OfficeScan wird vom Trend Micro Smart Protection Network™ unterstützt, einer Sicherheitsinfrastruktur mit webbasiertem Client der nächsten Generation, die intelligentere Sicherheit als herkömmliche Ansätze liefert. Die einzigartige In-the-Cloud-Technologie und ein leichtgewichtiger agent verringern die Abhängigkeit von herkömmlichen Pattern-Downloads und sorgen dafür, dass im Zusammenhang mit Desktop-Updates keine Verzögerungen mehr auftreten. Unternehmen profitieren von der größeren Netzwerkbandbreite, dem reduzierten Verarbeitungsaufwand und den damit verbundenen Kostenersparnissen. Benutzer können standortunabhängig auf die neuesten Sicherheitsfunktionen zugreifen – innerhalb des Unternehmensnetzwerks, von zu Hause oder von unterwegs.

Was ist neu in OfficeScan XG Service Pack 1

Diese Version von OfficeScan umfasst die folgenden neuen Funktionen und Verbesserungen.

FUNKTION	BESCHREIBUNG
Verbesserte Erkennung „dateiloser“ Skripts	• Die Verhaltensüberwachung wurde hinsichtlich der Erkennung schädlicher von berechtigten Windows-Programmen ausgeführter Skripts verbessert, um Endpunkte vor Malware zu schützen, die dateilose Angriffswege nutzt. • "Vorausschauendes Maschinenlernen" und Verhaltensüberwachung können darüber hinaus den effektiven Nutzlastpfad von Skriptdateien bestimmen, die von berechtigten Windows-DLLs ausgeführt werden.

FUNKTION	BESCHREIBUNG
Update-Agent-Verbindungen	Sie können OfficeScan Agents so konfigurieren, dass das HTTPS-Protokoll verwendet wird, wenn ein Update-Agent als Update-Adresse verwendet wird. Weitere Informationen finden Sie unter *Benutzerdefinierte Update-Adressen für OfficeScan Agenten konfigurieren auf Seite 6-35*.
Ausschlussliste für Verhaltensüberwachung	Die Ausnahmeliste unterstützt jetzt die Verwendung von Platzhalterzeichen. Weitere Informationen finden Sie unter *Ausnahmeliste, Unterstützung von Platzhaltern auf Seite 9-11*.
Vorausschauendes Maschinenlernen	Vorausschauendes Maschinenlernen wurde verbessert, um die Ausführung bösartiger Skripts zu erkennen. Weitere Informationen finden Sie unter *Vorausschauendes Maschinenlernen auf Seite 8-2*.
Cloud-Synchronisierungskanal für Ransomware-Funde	OfficeScan Agents erkennen über unterstützte Cloud-Synchronisierungskanäle heruntergeladene Ransomware. Weitere Informationen finden Sie unter *Widget für Ransomware-Zusammenfassung auf Seite 2-16*.
Verbesserungen bei den Proxy-Einstellungen	Alle Proxy-Einstellungen für den OfficeScan Server und OfficeScan Agents wurden am selben Speicherort konsolidiert. Weitere Informationen finden Sie unter *Proxy für Updates von OfficeScan Server auf Seite 6-20* und *OfficeScan Agent Proxy-Einstellungen auf Seite 15-53*.
Listen der verdächtigen Objekte	OfficeScan unterstützt die Erkennung von verdächtigen Domänenobjekten durch die Vernetzung mit Control Manager. Weitere Informationen finden Sie unter *Einstellungen für Liste der verdächtigen Objekte auf Seite 14-38*.

Was ist neu in OfficeScan XG

Diese Version von OfficeScan umfasst die folgenden neuen Funktionen und Verbesserungen.

Funktion	Beschreibung
Verbesserung des Ransomwareschutzes	Der Schutz vor Ransomware-Angriffen wurde weiter verbessert. OfficeScan Agents können nun von Ransomware-Bedrohungen verschlüsselte Dateien wiederherstellen, Ransomware zugeordnete Prozesse sperren und gefährdete ausführbare Dateien daran hindern, das Netzwerk zu infizieren. Weitere Informationen finden Sie unter *Ransomware-Schutz auf Seite 9-3*.
Verbesserung beim Schutz vor neu erkannten Programmen	Zur Optimierung der Sicherheitsrichtlinie zum Ransomware-Schutz auf einzelnen Agents wurde die Funktion zum Schutz vor neu erkannten Programmen in das Fenster mit den Einstellungen für die Verhaltensüberwachung verschoben. Weitere Informationen finden Sie unter *Schutz vor neu erkannten Programmen auf Seite 9-6*. Darüber hinaus können Sie die Nachricht anpassen, die auf Agent-Endpunkten angezeigt wird, nachdem ein Benutzer ein neu erkanntes Programm heruntergeladen und ausgeführt hat. Weitere Informationen finden Sie unter *Inhalt der Benachrichtigung ändern auf Seite 9-24*.
Vorausschauendes Maschinenlernen	Das Modul für "Vorausschauendes Maschinenlernen" kann Ihr Netzwerk mit Hilfe erweiterter Dateifunktionsanalysen und heuristischer Prozessüberwachung vor neuen, zuvor unerkannten oder unbekannten Gefahren schützen. Mit der Funktion "Vorausschauendes Maschinenlernen" können Zero-Day-Angriffe verhindert werden, indem die Wahrscheinlichkeit für das Vorhandensein einer Bedrohung in einer Datei oder einem Prozess und die mögliche Bedrohungsart ermittelt werden.

FUNKTION	BESCHREIBUNG
OfficeScan Edge-Relais-Server	Der OfficeScan Edge-Relais-Server bietet Ihnen mehr Transparenz und verbesserten Schutz für Endpunkte, die das lokale Intranet verlassen, indem folgende Funktionen bereitgestellt werden: • Synchronisierung der Listen der verdächtigen Objekte • Exemplar Zusendung • Protokollweiterleitung • Übermittlung von Statusinformationen des Agents, wie z. B. aktuelles Pattern und Komponentenversionen Weitere Informationen finden Sie unter *Edge-Relais-Server auf Seite 16-2*.
Zusendung einer Verdächtige Datei	Zur weiteren Verbesserung Ihrer Integration mit einem Deep Discovery Virtual Analyzer können OfficeScan Agents nun verdächtige Dateien, die unter Umständen noch unbekannte Bedrohungen enthalten, erkennen und zu Analysezwecken direkt an den Virtual Analyzer senden. Nachdem das Vorhandensein einer Bedrohung bestätigt wurde, werden die Listen verdächtiger Objekte sofort aktualisiert und mit allen Agents synchronisiert, wodurch die Verbreitung der Bedrohung im Netzwerk verhindert wird. Weitere Informationen finden Sie unter *Exemplar Zusendung auf Seite 8-11*.
Verbesserungen der Dashboard-Benutzeroberfläche	Das Dashboard wurde umgestaltet und bietet nun mehr Transparenz im Hinblick auf den Schutzstatus des Netzwerks.
Verbesserungen bei der Integration des Control Managers	Zur Vermeidung unbefugter Kommunikation zwischen dem Control Manager Server und dem OfficeScan Server muss bei der Registrierung beim Control Manager Zertifikatsauthentifzierung durchgeführt werden und die Richtlinienverwaltung über den Control Manager Server erfolgt unter Verwendung der Verschlüsselung mit öffentlichen Schlüsseln. Weitere Informationen finden Sie unter *Autorisierung von Control Manager-Zertifikaten auf Seite 14-31*.

FUNKTION	BESCHREIBUNG
Schwachstellenschutz	Bei der Echtzeitsuche können Sie mit Hilfe von CVE-Schwachstellen (Common Vulnerabilities and Exposures) Bedrohungen erkennen und sperren. Weitere Informationen finden Sie unter *Sucheinstellungen auf Seite 7-31*. Bei der Verhaltensüberwachung kann darüber hinaus ungewöhnliches Programmverhalten erkannt werden, das im Zusammenhang mit Angriffen auf Schwachstellen üblich ist. Weitere Informationen finden Sie unter *Schwachstellenschutz auf Seite 9-5*.
Verbesserung bei verdächtigen Verbindungen	Sie können die Funktion für verdächtige Verbindungen jetzt so konfigurieren, dass von der globalen C&C-IP-Liste und dem Malware-Fingerabdruck für Netzwerke erkannte Netzwerkverbindungen protokolliert oder gesperrt werden können. Weitere Informationen finden Sie unter *Verdächtige Verbindungseinstellungen konfigurieren auf Seite 8-9*.
Verbesserungen bei Firewalls	Der Anwendungsfilter der OfficeScan Firewall bietet nun Unterstützung für Windows 8 und höhere Plattformen. Sie können OfficeScan Agents-Benutzern die Berechtigung zum Konfigurieren der Sicherheitsstufe und der Ausnahmenliste der Firewall erteilen. Weitere Informationen finden Sie unter *Firewall-Profil hinzufügen auf Seite 13-23*.
Unabhängiger Modus	Der zuvor verwendete Begriff „Roaming“-Modus wurde in „unabhängiger“ Modus umbenannt. Weitere Informationen finden Sie unter *Verbindungsstatus des Agents auf Seite 2-40*.

FUNKTION	BESCHREIBUNG
Plattform- und Browser-Unterstützung	Diese Version von OfficeScan bietet Unterstützung für Folgendes: • Microsoft™ Windows™ Server 2016 **Hinweis** Diese Version von OfficeScan bietet keine weitere Unterstützung für den Apache Webserver.

Wichtigste Funktionen und Vorteile

OfficeScan bietet die folgenden Funktionen und Vorteile.

TABELLE 1-1. Wichtigste Funktionen und Vorteile

FUNKTION	VORTEILE
Schutz vor Ransomware	Mit verbesserten Suchfunktionen können Ransomware-Programme gefunden und blockiert werden, die auf Dokumente abzielen, die auf Endpunkten ausgeführt werden. Bei diesem Verfahren werden allgemeine Verhaltensweisen identifiziert und Prozesse blockiert, die normalerweise mit Ransomware-Programmen verknüpft sind.

FUNKTION	VORTEILE
Verbundene Bedrohungsabwehr	Konfigurieren Sie OfficeScan, um die Liste der verdächtigen Objekte auf dem Control Manager-Server zu abonnieren. Unter Verwendung der Control Manager-Konsole können Sie benutzerdefinierte Aktionen für die mit Hilfe der Liste der verdächtigen Objekte erkannten Objekte ausführen, um eine benutzerdefinierte Verteidigung gegen Bedrohungen auf Endpunkten sicherzustellen, die von spezifischen auf Ihre Umgebung abgestimmten Trend Micro Produkten geschützt werden. Sie können OfficeScan Agents so konfigurieren, dass Dateiobjekte, die unter Umständen zuvor nicht erkannte Bedrohungen enthalten, zur weiteren Analyse an Virtual Analyzer weitergeleitet werden. Nach der Bewertung der Objekte fügt Virtual Analyzer alle Objekte, in denen unbekannte Bedrohungen gefunden wurden, zu den Virtual Analyzer-Listen mit verdächtigen Objekten hinzu und verteilt die Listen über das Netzwerk an andere OfficeScan Agents.
Plug-in Manager und Plug-in-Lösungen	Plug-in Manager erleichtert die Installation, Verteilung und Verwaltung von Plug-in-Lösungen. Administratoren können zwei Arten von Plug-in-Lösungen installieren: • Plug-in-Programme • Native OfficeScan Funktionen

FUNKTION	VORTEILE
Zentrale Verwaltung	Die webbasierte Management-Konsole ermöglicht dem Administrator transparenten Zugriff auf alle agents und Server im Netzwerk. über diese Webkonsole wird außerdem die automatische Verteilung von Sicherheitsrichtlinien, Pattern-Dateien und Software-Updates auf allen agents und Servern koordiniert. Mit Hilfe der Ausbruchsprävention werden Infektionswege gesperrt und angriffsspezifische Sicherheitsrichtlinien zur Vermeidung bzw. Eindämmung von Ausbrüchen umgehend verteilt, noch bevor die entsprechenden Pattern-Dateien verfügbar sind. OfficeScan überwacht das System in Echtzeit, versendet Ereignisbenachrichtigungen und erstellt umfassende Berichte. Der Administrator kann das Netzwerk remote verwalten, benutzerdefinierte Richtlinien für bestimmte Desktops oder Gruppen festlegen und agent-Sicherheitseinstellungen sperren.
Schutz vor Sicherheitsbedrohungen	OfficeScan schützt Computer vor Sicherheitsrisiken. Hierbei werden zunächst Dateien durchsucht und anschließend wird eine bestimmte Aktion für jedes entdeckte Sicherheitsrisiko durchgeführt. Eine über einen kurzen Zeitraum entdeckte extrem hohe Anzahl an Sicherheitsrisiken deutet auf einen Virenausbruch hin. Um Virenausbrüche einzudämmen, erzwingt OfficeScan Richtlinien zur Virenausbruchsprävention und isoliert infizierte Computer so lange, bis sie kein Risiko mehr darstellen. OfficeScan verwendet die intelligente Suche, um den Suchvorgang effizienter zu gestalten. Diese Technologie basiert darauf, dass eine Vielzahl von zuvor auf dem lokalen Endpunkt gespeicherten Signaturen auf Smart Protection Quellen geladen werden. Mit dieser Methode werden sowohl das System als auch das Netzwerk von der stetig zunehmenden Anzahl an Signatur-Updates auf Endpunktsysteme entlastet. Informationen über die intelligente Suche und die Verteilung auf agents finden Sie unter *Suchmethodentypen auf Seite 7-9*.

FUNKTION	VORTEILE
Damage Cleanup Services	Die Damage Cleanup Services™ beseitigen vollautomatisch dateibasierte und Netzwerkviren sowie überreste von Viren und Würmern (Trojanern, Registrierungseinträgen, Virendateien) auf Computern. Zur Abwehr von Bedrohungen und Störungen durch Trojaner verfügen die Damage Cleanup Services über folgende Funktionen: • Entdeckt und entfernt aktive Trojaner • Beendet durch Trojaner ausgelöste Prozesse • Repariert von Trojanern geänderte Systemdateien • Löscht von Trojanern hinterlassene Dateien und Anwendungen Die Damage Cleanup Services werden automatisch im Hintergrund ausgeführt. Es ist deshalb keine Konfiguration erforderlich. Die Benutzer bemerken nichts von diesem Vorgang. In einigen Fällen wird der Benutzer jedoch von OfficeScan aufgefordert, den Endpunkt zur vollständigen Entfernung eines Trojaners neu zu starten.
Web Reputation	Die Web-Reputation-Technologie schützt Agent-Endpunkte innerhalb oder außerhalb des Unternehmensnetzwerks proaktiv vor bösartigen und potenziell gefährlichen Websites. Web Reputation durchbricht die Infektionskette und verhindert den Download von bösartigem Code. Sie können die Glaubwürdigkeit der Websites und Webseiten überprüfen, indem Sie OfficeScan in den Smart Protection Server oder das Trend Micro Smart Protection Network integrieren.
OfficeScan Firewall	Die OfficeScan Firewall schützt agents und Server im Netzwerk mit Hilfe von Stateful-Inspection-Technologie und leistungsstarken Funktionen zur Virensuche. Sie können Regeln erstellen, um Verbindungen nach Anwendung, IP-Adresse, Portnummer oder Protokoll zu filtern, und anschließend die Regeln auf unterschiedliche Benutzergruppen anwenden.

FUNKTION	VORTEILE
Prävention vor Datenverlust	Die Funktion "Prävention vor Datenverlust" schützt die digitalen Assets einer Organisation vor versehentlichen oder beabsichtigten Lecks. Die Funktion "Prävention vor Datenverlust" ermöglicht Administratoren Folgendes: • Die zu schützenden digitalen Assets erkennen • Richtlinien erstellen, die die übertragung von digitalen Assets über gemeinsam genutzte übertragungskanäle wie E-Mail-Nachrichten und externe Geräte einschränken oder verhindern • Die Einhaltung bewährter Datenschutzstandards durchsetzen
Gerätesteuerung	Die Gerätesteuerung reguliert den Zugriff auf externe Speichergeräte und Netzwerkressourcen, die an Computer angeschlossen sind. Die Gerätesteuerung trägt dazu bei, Datenverluste und Datenlecks zu verhindern und bietet, gemeinsam mit der Virensuche, Schutz vor Sicherheitsrisiken.
Verhaltensüberwachung	Die Verhaltensüberwachung überprüft regelmäßig agents auf ungewöhnliche änderungen am Betriebssystem oder der installierten Software.

Der OfficeScan Server

Der OfficeScan Server ist der zentrale Speicherort für Informationen über alle vorhandenen agent-Konfigurationen, Sicherheitsrisiko-Protokolle und Updates.

Der Server erfüllt zwei wichtige Funktionen:

- Er installiert, überwacht und verwaltet die OfficeScan Agents.
- Lädt die meisten Komponenten herunter, die von agents benötigt werden. Der OfficeScan Server lädt Komponenten vom Trend Micro ActiveUpdate Server herunter und verteilt sie dann auf die agents.

Hinweis

Einige Komponenten werden von den Smart Protection Quellen heruntergeladen. Weitere Informationen finden Sie unter *Smart Protection Quellen auf Seite 4-6*.

ABBILDUNG 1-1. Informationen zur Funktionsweise des OfficeScan Servers

Der OfficeScan Server ermöglicht eine bidirektionale Kommunikation zwischen dem Server und den OfficeScan Agents in Echtzeit. Sie können die agents über eine browserbasierte Webkonsole verwalten, die Administratoren von einer beliebigen Stelle des Netzwerks aus aufrufen können. Der Server kommuniziert mit dem agent (und der agent mit dem Server) über HTTP (HyperText Transfer Protocol).

Das OfficeScan Agent

Installieren Sie den OfficeScan Agent auf jedem Endpunkt, um Ihre Windows-Computer vor Sicherheitsrisiken zu schützen.

Der OfficeScan Agent berichtet an den übergeordneten Server, von dem aus er installiert wurde. Mit dem Agent Mover-Tool können Sie agents so konfigurieren, dass diese ihre Meldungen an andere Server senden. Der agent sendet Ereignis- und Statusinformationen in Echtzeit an den Server. Beispiele für Ereignisse sind entdeckte Viren/Malware, das Starten des agents und das Herunterfahren des agents, der Startzeitpunkt einer Virensuche oder ein abgeschlossener Update-Vorgang.

Integration in Trend Micro Produkte und Services

OfficeScan lässt sich in die in der folgenden Tabelle aufgeführten Produkte und Services von Trend Micro integrieren. Zur nahtlosen Integration müssen Sie sicherstellen, dass die Produkte die erforderliche oder empfohlene Version haben.

TABELLE 1-2. Produkte und Services, die mit OfficeScan integriert werden können

PRODUKT/ SERVICE	BESCHREIBUNG	VERSION
ActiveUpdate Server	Liefert alle Komponenten, die der OfficeScan Agent benötigt, um Endpunkte vor Sicherheitsbedrohungen zu schützen.	Nicht zutreffend
Smart Protection Network	Bietet File-Reputation-Dienste und Web-Reputation-Dienste für Agents. Smart Protection Network wird von Trend Micro gehostet.	Nicht zutreffend

PRODUKT/ SERVICE	BESCHREIBUNG	VERSION
Eigenständiger Smart Protection Server	Bietet die gleichen File-Reputation-Dienste und Web-Reputation-Dienste, die auch vom Smart Protection Network angeboten werden. Ein Standalone Smart Protection Server ist dafür da, den Service lokal im Firmennetzwerk zur Verfügung zu stellen, um die Effizienz zu erhöhen. **Hinweis** Ein integrierter Smart Protection Server wird zusammen mit dem OfficeScan Server installiert. Er besitzt die gleichen Funktionen wie sein Standalone-Gegenstück, seine Kapazität ist aber eingeschränkt.	• 3.0
Control Manager	Eine Software-Management-Lösung, die es Ihnen ermöglicht, Antiviren- und Content-Sicherheitsprogramme zentral zu überwachen – unabhängig von der Plattform oder dem physikalischen Speicherort des Programms.	• 7,0 • 6.0 SP3 Patch 2 (empfohlen) • 6.0 SP3 • 6.0 SP2 • 6.0 SP1
Deep Discovery Analyzer	Deep Discovery bietet netzwerkweite Überwachung, gestärkt durch benutzerdefinierte Sandbox-Funktionen und Informationen in Echtzeit, um Angriffe früh zu erkennen, umgehende Isolierung zu ermöglichen und maßgeschneiderte Sicherheitsupdates bereitzustellen, mit denen sofortiger Schutz gegen weitere Attacken gewährleistet wird.	5.1 und höher

Kapitel 2

Erste Schritte in OfficeScan

In diesem Kapitel werden der Einstieg in OfficeScan und die anfänglichen Konfigurationseinstellungen beschrieben.

Es werden folgende Themen behandelt:

- *Die Webkonsole auf Seite 2-2*
- *Die Dashboard auf Seite 2-5*
- *Das Einstellungsexporttool von OfficeScan auf Seite 14-33*
- *Active Directory-Integration auf Seite 2-36*
- *Die OfficeScan Agent-Hierarchie auf Seite 2-40*
- *OfficeScan Domänen auf Seite 2-54*

Die Webkonsole

Die Webkonsole ist die zentrale Stelle zur überwachung von OfficeScan Produkten 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 JavaScript, CGI, HTML und HTTPS.

Hinweis

Konfigurieren Sie Einstellungen für die Zeitüberschreitung über die Webkonsole.

Weitere Informationen finden Sie unter *Einstellungen der Webkonsole konfigurieren auf Seite 14-69*.

über die Webkonsole können Sie folgende Aktionen ausführen:

- Auf vernetzten Endpunkten installierte Agents verwalten
- Agents zur gleichzeitigen Konfiguration und Verwaltung in logischen Domänen gruppieren
- Auf einem oder mehreren Netzwerkendpunkten die Virensucheinstellungen festlegen und die manuelle Suche starten
- Benachrichtigungen über Sicherheitsrisiken im Netzwerk konfigurieren und von Agents gesendete Protokolle anzeigen
- Ausbruchskriterien und Benachrichtigungen konfigurieren
- Administrationsaufgaben für die Webkonsole an andere OfficeScan Administratoren delegieren, indem Rollen und Benutzerkonten konfiguriert werden
- Sicherstellen, dass Agents die Sicherheitsrichtlinien einhalten

Hinweis

Windows 8, 8.1, 10 oder Windows Server 2012 im Windows-Benutzeroberflächenmodus wird von der Webkonsole nicht unterstützt.

Voraussetzungen für das Öffnen der Web-Konsole

Die Webkonsole von einem beliebigen Endpunkt im Netzwerk aus öffnen, der über die folgenden Ressourcen verfügt:

- 300 MHz Intel™ Pentium™ oder vergleichbarer Prozessor
- 128 MB Arbeitsspeicher
- Mindestens 30 MB verfügbarer Festplattenspeicher
- Monitor mit einer Mindestauflösung von 1366 x 768 bei 256 Farben oder mehr
- Unterstützung für Webbrowser:
  - Microsoft Internet Explorer™ 10.0 (oder höher)
  - Microsoft Edge
  - Chrome

Hinweis

OfficeScan unterstützt nur HTTPS-Datenverkehr zum Anzeigen der Webkonsole.

Geben Sie dazu im Webbrowser je nach Installationsart des OfficeScan Servers eine der folgenden Adressen in die Adressleiste ein:

TABELLE 2-1. URLs der OfficeScan Webkonsole

INSTALLATIONSART	URL
Mit SSL am Standard-Standort	`https://<FQDN oder IP-Adresse des OfficeScan Servers>/OfficeScan`
Mit SSL am virtuellen Standort	`https://<OfficeScan Server FQDN oder IP-Adresse>:<Portnummer>/OfficeScan`

Hinweis

Nach einem Upgrade von einer Vorgängerversion von OfficeScan verhindern Dateien des Webbrowsers und des Proxy-Server-Caches möglicherweise das ordnungsgemäße Starten der OfficeScan Webkonsole. Löschen Sie den Cache-Speicher auf dem Browser und allen Proxyservern, die sich zwischen dem OfficeScan Server und dem Endpunkt befinden, der für den Zugriff auf die Webkonsole verwendet wird.

Anmeldekonto

Während der Installation des OfficeScan Servers erstellt Setup ein Root-Konto und fordert Sie auf, das Kennwort für dieses Konto einzugeben. Wenn Sie die Webkonsole zum ersten Mal öffnen, geben Sie als Benutzernamen "root" und das Kennwort für das Root-Konto ein. Wenn Sie das Kennwort vergessen, wenden Sie sich zur Unterstützung beim Zurücksetzen des Kennworts an Ihren Support-Anbieter.

Definieren Sie Benutzerrollen und richten Sie Benutzerkonten ein, damit andere Benutzer auf die Webkonsole zugreifen können, ohne das Root-Konto zu verwenden. Wenn sich Benutzer an der Konsole anmelden, können diese die Benutzerkonten verwenden, die für sie eingerichtet wurden. Weitere Informationen finden Sie unter *Rollenbasierte Administration auf Seite 14-3*.

Das Banner der Webkonsole

Im Bannerbereich der Webkonsole sind die folgenden Optionen verfügbar:

ABBILDUNG 2-1. Der Bannerbereich der Webkonsole

- **<Kontoname>**: Klicken Sie auf den Kontonamen (z. B. root), um bestimmte Einzelheiten für das Konto, wie etwa das Kennwort, zu ändern.
- **Abmelden**: Meldet Benutzer von der Webkonsole ab.

Hilfe anfordern

Im Menü **Hilfe** erhalten Sie Zugriff auf die folgenden Informationen:

- **Inhalt & Index**: öffnet die Online-Hilfe
- **Support**: Zeigt die Webseite vom Trend Micro Support an, auf der Sie eine Anfrage an das Support-Team von Trend Micro stellen können und Antworten auf häufig gestellte Fragen zu den Produkten von Trend Micro finden.
- **Bedrohungsenzyklopädie**: Zeigt die Bedrohungsenzyklopädie-Website an, auf der Sie Informationen von Trend Micro zu Malware finden. Sicherheitsexperten von Trend Micro veröffentlichen regelmäßig erkannte Malware, Spam, bösartige URLs und Schwachstellen. In der Bedrohungsenzyklopädie werden außerdem wichtige Internet-Angriffe erläutert und entsprechende Informationen dazu angeboten.
- **Kontaktaufnahme mit Trend Micro**: Zeigt die Trend Micro Website **Kontaktaufnahme** mit Informationen zu Niederlassungen weltweit an.
- **Info**: Bietet einen überblick über das Produkt, Anweisungen zur überprüfung der Komponentenversionen und einen Link zum Support-Informationssystem.

  Weitere Informationen finden Sie unter *Support-Informationssystem auf Seite 18-2*.

Die Dashboard

Die **Dashboard** wird angezeigt, wenn Sie die OfficeScan Webkonsole öffnen oder im Hauptmenü auf **Dashboard** klicken.

Jedes Benutzerkonto einer Webkonsole verfügt über ein völlig unabhängiges Dashboard. Alle Änderungen eines Dashboards eines Benutzerkontos haben keine Auswirkungen auf die Dashboards anderer Benutzerkonten.

Enthält ein Dashboard OfficeScan agent-Daten, bestimmen die agent-Domänenberechtigungen für das Benutzerkonto, welche Daten angezeigt werden. Wenn beispielsweise das Dashboard eines Benutzerkontos die Berechtigung hat, die Domänen A und B zu verwalten, zeigt das Dashboard des Benutzerkontos nur Daten von agents an, die zu den Domänen A und B gehören.

Weitere Informationen zu Benutzerkonten finden Sie unter *Rollenbasierte Administration auf Seite 14-3*.

Das Fenster **Dashboard** enthält folgende Informationen:

- Abschnitt Status der Produktlizenz
- Widgets
- Registerkarten

Abschnitt Status der Produktlizenz

Dieser Abschnitt befindet sich im oberen Bereich des Dashboards und zeigt den Status der OfficeScan Lizenz an.

ABBILDUNG 2-2. Abschnitt Status der Produktlizenz

In folgenden Fällen werden Hinweise zum Status der Lizenz angezeigt:

- Wenn Sie eine Lizenz der Vollversion haben:
  - 60 Tage vor Ablauf einer Lizenz
  - Während der Übergangsfrist des Produkts. Die Dauer der Übergangsfrist ist regional verschieden. Erkunden Sie sich bei Ihrem Trend Micro Vertriebspartner über die Länge der Übergangsfrist.
  - Bei Ablauf der Lizenz und der Übergangsfrist. Innerhalb dieses Zeitraums erhalten Sie keinen technischen Support und können keine Komponenten-Updates durchführen. Die Scan Engine durchsucht die Computer unter Verwendung nicht aktueller Komponenten weiterhin. Diese veralteten Komponenten schützen Sie möglicherweise nicht vollständig vor den aktuellen Sicherheitsrisiken.

- Wenn Sie eine Testversionslizenz haben:
  - 14 Tage vor Ablauf einer Lizenz
  - Bei Ablauf der Lizenz Innerhalb dieses Zeitraums deaktiviert OfficeScan Komponenten-Updates, Suchfunktionen und alle agent-Funktionen.

Wenn Sie über einen Aktivierungscode verfügen, können Sie die Lizenz unter **Administration** > **Einstellungen** > **Produktlizenz** verlängern.

Produktinformationsleisten

OfficeScan zeigt oben im Fenster **Dashboard** eine Reihe von Nachrichten an, die Administratoren zusätzliche Informationen liefern.

Folgende Informationen werden angezeigt:

- Neueste verfügbare Service Packs oder Patches für OfficeScan

Hinweis

Klicken Sie auf **Weitere Informationen**, um den Patch aus dem Trend Micro Download Center herunterzuladen (http://downloadcenter.trendmicro.com/index.php?regs=DE).

- Verfügbare neue Widgets
- Benachrichtigungen zum Wartungsvertrag, wenn der Vertrag kurz vor dem Ablaufdatum steht
- Benachrichtigungen zum Bewertungsmodus
- Benachrichtigungen zur Authentizität

Hinweis

Eine Informationsmeldung wird angezeigt, wenn die für OfficeScan verwendetet Lizenz ungültig ist. Wenn Sie sich keine gültige Lizenz besorgen, zeigt OfficeScan eine Warnung an und beendet die Updates.

Registerkarten und Widgets

Widgets sind die Hauptkomponenten des Dashboards. Widgets liefern spezielle Informationen über unterschiedliche sicherheitsrelevante Ereignisse. Manche Widgets lassen es zu, bestimmte Aufgaben durchzuführen, wie beispielsweise abgelaufene Komponenten zu aktualisieren.

Die Informationen, die Widgets anzeigen, stammen von:

- OfficeScan Server und agents
- Plug-in-Lösungen und ihren Agents
- Trend Micro Smart Protection Network

Hinweis

Aktivieren Sie Smart Feedback , um Daten vom Smart Protection Network anzuzeigen. Weitere Informationen über Smart Feedback finden Sie unter *Smart Feedback auf Seite 14-73*.

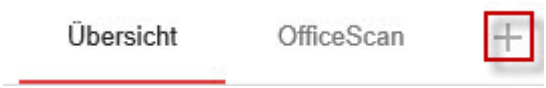
Registerkarten stellen einen Container für Widgets zur Verfügung. Die **Dashboard** unterstützt bis zu 30 Registerkarten.

Mit Registerkarten arbeiten

Verwalten Sie Registerkarten, indem Sie das Layout hinzufügen, umbenennen oder ändern und automatisch zwischen Registerkartenansichten wechseln.

Prozedur

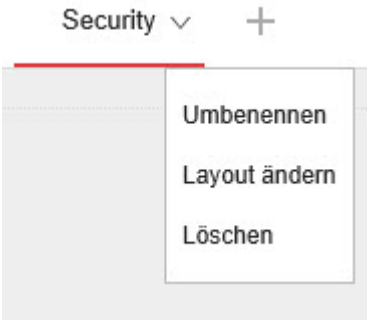
1. Navigieren Sie zu **Dashboard**.
2. So fügen Sie eine neue Registerkarte hinzu:
   a. Klicken Sie auf das Symbol "Hinzufügen".



b. Geben Sie einen Namen für die neue Registerkarte ein.

3. So benennen Sie eine Registerkarte um:

a. Bewegen Sie den Mauszeiger über den Namen der Registerkarte und klicken Sie auf den Abwärtspfeil.



b. Klicken Sie auf **Umbenennen** und geben Sie den neuen Registerkartennamen ein.

4. So ändern Sie das Layout der Widgets für eine Registerkarte:

a. Bewegen Sie den Mauszeiger über den Namen der Registerkarte und klicken Sie auf den Abwärtspfeil.

b. Klicken Sie auf **Layout ändern**.

c. Wählen Sie das neue Layout im angezeigten Fenster aus.

d. Klicken Sie auf **Speichern**.

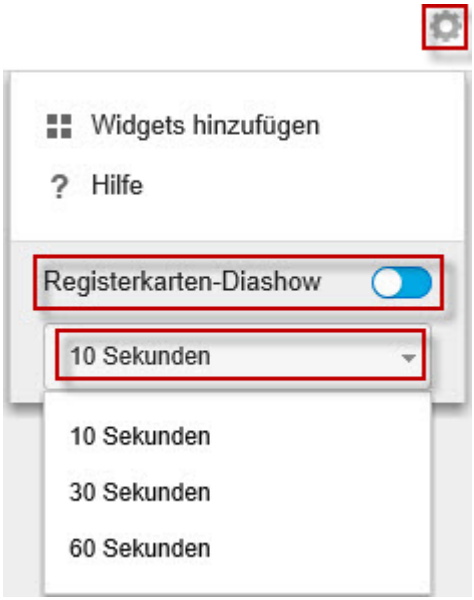
5. So löschen Sie eine Registerkarte:

a. Bewegen Sie den Mauszeiger über den Namen der Registerkarte und klicken Sie auf den Abwärtspfeil.

b. Klicken Sie auf **Löschen** und bestätigen Sie den Vorgang.

6. So geben Sie eine Bildschirmpräsentation der Registerkarten wieder:

a. Klicken Sie rechts neben der Registerkartenanzeige auf die Schaltfläche **Einstellungen**.



b. Aktivieren Sie das Steuerelement **Bildschirmpräsentation mit Registerkarte wiedergeben**.

c. Wählen Sie den Zeitraum aus, der zwischen der Anzeige der Registerkarten vergehen soll.

Mit Widgets arbeiten

Verwalten Sie Widgets durch Hinzufügen, Verschieben, Ändern, Umbenennen und Löschen von Elementen.

Prozedur

1. Navigieren Sie zu **Dashboard**.

2. Klicken Sie auf eine Registerkarte.

3. So fügen Sie ein Widget hinzu:

   a. Klicken Sie rechts neben der Registerkartenanzeige auf die Schaltfläche **Einstellungen**.

   b. Klicken Sie auf **Widgets hinzufügen**.

   c. Wählen Sie die hinzuzufügenden Widgets aus.

      - Wählen Sie in der Dropdown-Liste oberhalb der Widgets eine Kategorie aus, um die Auswahl einzugrenzen.
      - Verwenden Sie das Suchtextfeld im Fenster oben, um nach einem bestimmten Widget zu suchen.

   d. Klicken Sie auf **Hinzufügen**.

4. Zum Verschieben eines Widgets an eine neue Position auf derselben Registerkarte ziehen Sie es an die neue Position und legen Sie es dort ab.

5. Sie können die Größe von Widgets in einer mehrspaltigen Registerkarte anpassen, indem Sie mit dem Cursor auf den rechten Rand des Widgets zeigen und den Cursor nach links oder rechts bewegen.

6. So benennen Sie ein Widget um:

a. Klicken Sie auf das Symbol "Einstellungen" (>).

b. Geben Sie einen neuen Titel ein.

Hinweis

Bei bestimmten Widgets, wie z. B. dem **OfficeScan- und Plug-in-Mashup**, können Sie Widget-bezogene Elemente ändern.

c. Klicken Sie auf **Speichern**.

7. Klicken Sie zum Löschen eines Widgets auf das Symbol "Löschen" (>).

Widgets für die Registerkarten der Zusammenfassung

Die Registerkarte **Zusammenfassung** enthält eine übersicht über den Sicherheitsstatus aller OfficeScan Agents im Netzwerk.

Hinweis

Sie können die auf der Registerkarte **Zusammenfassung** angezeigten Widgets weder hinzufügen, löschen noch ändern.

Verfügbare Widgets:

- *Widget für die allgemeine Bedrohungserkennung und Richtlinienverstöße auf Seite 2-13*
- *Endpunktstatus-Widget auf Seite 2-14*
- *Widget für Ransomware-Zusammenfassung auf Seite 2-16*
- *Widget für die häufigsten Ransomware-Funde auf Seite 2-19*
- *Widget für die Erkennung von Sicherheitsrisiken im Zeitverlauf auf Seite 2-21*

Widget für die allgemeine Bedrohungserkennung und Richtlinienverstöße

Dieses Widget bietet einen Überblick über alle erkannten Bedrohungen und Richtlinienverstöße im Netzwerk während der letzten 24 Stunden.

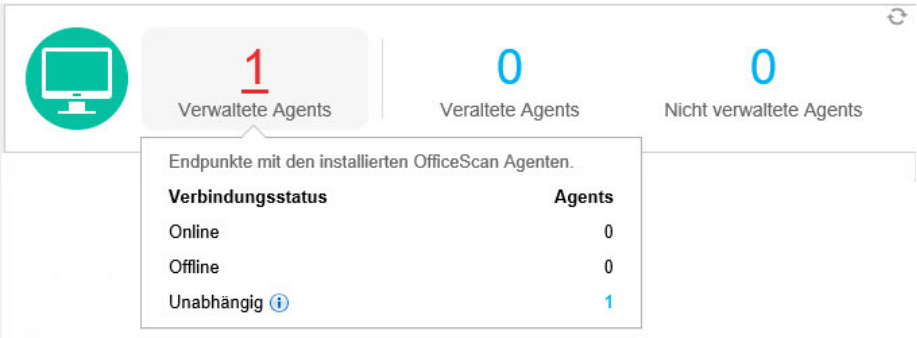
Bewegen Sie den Mauszeiger über den Zähler für Bedrohungen oder Verstöße, um eine Gliederung der spezifischen Erkennungstypen anzuzeigen, die für jede Gruppe aufgetreten sind. Klicken Sie zur Anzeige der Protokolle für eine bestimmte Funktion rechts auf die Anzahl.

TABELLE 2-2. Erkennungskategorien

KATEGORIE	BESCHREIBUNG
Bekannte Bedrohungen	Zeigt alle Funktionen an, die von Trend Micro bestätigte Sicherheitsrisiken erkennen. • Viren/Malware • Spyware / Grayware • Web Reputation

KATEGORIE	BESCHREIBUNG
Unbekannte Bedrohungen	Zeigt alle Funktionen an, die mögliche Bedrohungen mit Hilfe erweiterter heuristischer Verfahren, Analysen oder Funktionsmodellierung erkennen. • Vorausschauendes Maschinenlernen • Verhaltensüberwachung • Verdächtige Verbindungen • Verdächtige Dateiobjekte
Richtlinienverstöße	Zeigt alle Funktionen mit Richtlinienverstößen an, die für die Sicherheitsstandards Ihres Unternehmens spezifisch sind. • Firewall • Gerätesteuerung • Prävention vor Datenverlust

Endpunktstatus-Widget



Dieses Widget stellt eine übersicht über den Verbindungs- und Update-Status der OfficeScan Agents im Netzwerk sowie die aktuelle Anzahl der Sicherheitsrichtlinieneinhaltungen auf nicht verwalteten Endpunkten bereit, die keine Berichte für den OfficeScan Server erstellen.

Bewegen Sie den Mauszeiger über eine Anzahl, um die Verteilung der verschiedenen Statusarten anzuzeigen. Zum Anzeigen der Protokolle für einen bestimmten Status klicken Sie rechts auf die Anzahl.

TABELLE 2-3. Agent-/Endpunktgruppen

GRUPPE	BESCHREIBUNG
Verwaltete Agents	Zeigt den letzten gemeldeten Verbindungsstatus der OfficeScan Agents im Netzwerk an. • Online • Offline • Unabhängig
Veraltete Agents	Zeigt eine Liste der Komponentenkategorien und die Anzahl der OfficeScan Agents mit einer veralteten Komponente in jeder Kategorie an.
Nicht verwaltete Endpunkte	Zeigt eine Liste aller Endpunkte an, die der OfficeScan erkennen kann, auf denen aber kein OfficeScan Agent Programm installiert ist oder die keinen Bericht an den OfficeScan Server senden. **Hinweis** So stellen Sie sicher, dass der OfficeScan Server die Anzahl der nicht verwalteten Endpunkte regelmäßig aktualisiert: 1. Definieren Sie den Active Directory-/IP-Adressenbereich für eine Bewertung. Weitere Informationen finden Sie unter *Active Directory-Integration auf Seite 2-36*. 2. Konfigurieren Sie eine zeitgesteuerte Bewertung. Weitere Informationen finden Sie unter *Einhaltung der Sicherheitsrichtlinien für nicht verwaltete Endpunkte auf Seite 15-78*.

Widget für Ransomware-Zusammenfassung

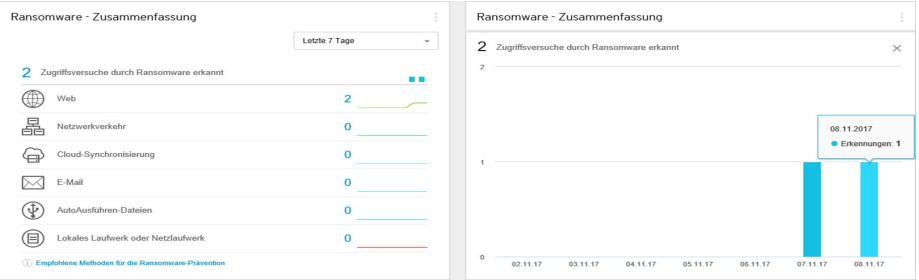


ABBILDUNG 2-3. Standardansicht zur Anzeige aller Ransomware-Daten und eine erweiterte Ansicht des Balkendiagramms "Erkannte Ransomware-Versuche"

Dieses Widget bietet eine übersicht über alle Ransomware-Angriffsversuche während eines bestimmten Zeitraums.

In der Standardansicht wird eine Zusammenfassung aller Ransomware-Erkennungen angezeigt. Darüber hinaus werden die Versuche auf Basis des Infektionskanals weiter kategorisiert.

- Klicken Sie in der Standardansicht auf die Anzahl der Ransomware-Erkennungen, um das Fenster mit den **Sicherheitsrisiken - Ransomware**-Protokollen zu öffnen, in dem die Details der Ransomware-Erkennungen aufgeführt werden.

Klicken Sie auf eines der Diagramme auf der rechten Seite des Widgets, um eine erweiterte Ansicht der Diagrammdaten zu öffnen.

- Bewegen Sie den Mauszeiger über einen bestimmten Tag, um die Gesamtzahl der Erkennungen für die angezeigte Erkennungskategorie einzublenden. Klicken Sie auf einen Knoten, um zum Fenster mit den **Sicherheitsrisiken - Ransomware**-Protokollen zurückzukehren, in dem die Details der Ransomware-Erkennungen für den entsprechenden Tag aufgelistet werden.

TABELLE 2-4. Ransomware-Erkennungskanäle

KANAL	BESCHREIBUNG	ENTDECKT DURCH
Web	Dateien, die über einen Web-Client heruntergeladen wurden (z. B. Browser oder FTP-Client)	• Web Reputation • Echtzeitsuche • Verhaltensüberwachung
Netzwerkverkehr	Ransomware, die von der Funktion "Verdächtige Verbindungen" erkannt wurde	• Verdächtige Verbindungen
Cloud-Synchronisierung	Dateien, die mit Hilfe der folgenden unterstützten Cloud Storage Services im lokalen Synchronisierungsordner synchronisiert werden • Microsoft™ OneDrive™ • Box	• Echtzeitsuche • Verhaltensüberwachung • Vorausschauendes Maschinenlernen
E-Mail	Mit Microsoft Outlook geöffnete E-Mail-Anhänge **Hinweis** OfficeScan klassifiziert alle Anhänge, die mit Hilfe anderer E-Mail-Client-Anwendungen im Kanal **Lokales Laufwerk oder Netzlaufwerk** geöffnet wurden.	• Echtzeitsuche • Verhaltensüberwachung

KANAL	BESCHREIBUNG	ENTDECKT DURCH
AutoAusführen-Dateien	Programme, die auf Wechselmedien gespeichert sind und von einer automatisch ausgeführten Datei ausgeführt werden **Hinweis** OfficeScan klassifiziert alle anderen Dateien/ Programme, die nicht über ein automatisch ausgeführtes Programm auf Wechselmedien im Kanal **Lokales Laufwerk oder Netzlaufwerk** ausgeführt werden.	• Echtzeitsuche • Verhaltensüberwachung
Lokales Laufwerk oder Netzlaufwerk	Auf lokalen oder Netzlaufwerken erkannte Ransomware, einschließlich: • E-Mail-Anhänge, die unter Verwendung von anderen E-Mail-Clients als Microsoft Outlook geöffnet wurden • Dateien auf Wechselmedien, die nicht von einem automatisch ausgeführten Programm ausgeführt werden	• Echtzeitsuche • Manuelle Suche • Zeitgesteuerte Suche • Jetzt durchsuchen • Verhaltensüberwachung

Sicherheitsrisiken – Ransomware-Protokolle

Die Sicherheitsrisiken – Ransomware-Protokolle bieten eine Übersicht über alle auf einem Netzwerk erkannten Ransomware-Bedrohungen, unabhängig vom Suchtyp, anhand dessen die Bedrohung gefunden wurde.

VORGANG	BESCHREIBUNG
Datum/Uhrzeit	Zeitpunkt der Erkennung
Sicherheitsbedrohung	Der Name der Sicherheitsbedrohung
Kategorie	Der Typ der Suche, bei der die Bedrohung erkannt wurde
Dateipfad/URL/Listenquelle	Der Speicherort, in dem die Bedrohung erkannt wurde, oder die zum Erkennen der bösartigen Website verwendete Liste
Aktion	Hinsichtlich der Bedrohung ergriffene Aktion
Infektionskanal	Der Kanal, aus dem die Bedrohung stammt
Endpunkt	Endpunkt, auf dem die Erkennung erfolgte

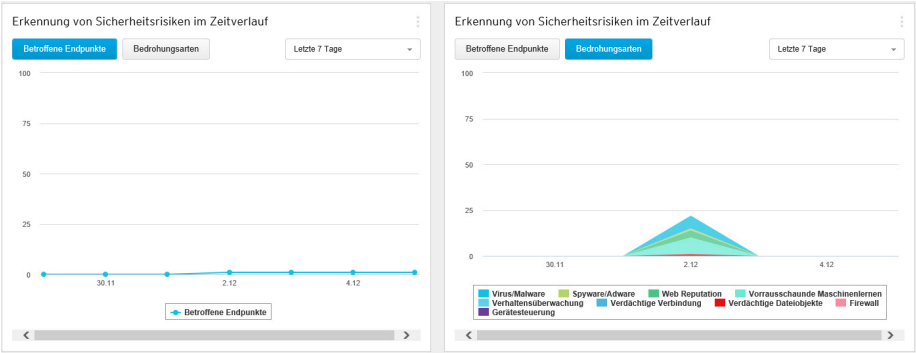
Widget für die häufigsten Ransomware-Funde

Dieses Widget bietet einen Überblick über die häufigsten Ransomware-Funde während eines bestimmten Zeitraums.

Verwenden Sie die Dropdown-Liste, um den Typ der anzuzeigenden Ransomware-Daten auszuwählen.

Ansicht	Beschreibung
Endpunkte	Zeigt die Endpunkte mit der größten Anzahl an Ransomware-Erkennungen im Netzwerk an. Klicken Sie auf die Anzahl der Ransomware-Erkennungen, um das Fenster mit den **Sicherheitsrisiken - Ransomware**-Protokollen zu öffnen, in dem die Details der Ransomware-Erkennungen aufgeführt werden.
Ransomware-Typen	Zeigt die Ransomware-Typen mit der größten Anzahl an Erkennungen im Netzwerk an. Klicken Sie auf den Link **Bedrohungsname**, um die Trend Micro Bedrohungsenzyklopädie mit weiteren Informationen zur jeweiligen Bedrohungsart zu öffnen.
Domänen	Zeigt die Ransomware-Domäne mit der größten Anzahl an Erkennungen im Netzwerk an. Klicken Sie auf den Link **Bedrohungsname**, um die Trend Micro Bedrohungsenzyklopädie mit weiteren Informationen zur jeweiligen Domäne zu öffnen.

Widget für die Erkennung von Sicherheitsrisiken im Zeitverlauf



Dieses Widget bietet eine übersicht über die Endpunkte im Netzwerk mit erkannten Bedrohungen sowie über die Bedrohungsarten, die sich während eines bestimmten Zeitraums auf Ihr Netzwerk ausgewirkt haben.

Klicken Sie auf die Schaltfläche **Betroffene Endpunkte** oder die Schaltfläche **Bedrohungsarten**, um zwischen den verschiedenen Ansichten zu wechseln.

Ansicht	Beschreibung
Betroffene Endpunkte	Zeigt die Anzahl der Endpunkte mit Bedrohungserkennungen oder Richtlinienverstößen für den angegebenen Zeitraum an. Klicken Sie auf den Knoten für einen bestimmten Tag, um zum Fenster **Agent-Verwaltung** weitergeleitet zu werden, in dem alle betroffenen Endpunkte für diesen Tag in der Agent-Hierarchie aufgelistet werden.

ANSICHT	BESCHREIBUNG
Bedrohungsarten	Zeigt ein Diagramm an, in dem die für den angegebenen Zeitraum protokollierte Anzahl an Bedrohungen und Richtlinienverstößen angezeigt wird. • Klicken Sie im unteren Bereich des Diagramms auf die Namen der Bedrohungsarten, um Informationen zur Erkennung im Diagramm anzuzeigen. • Bewegen Sie den Mauszeiger über einen bestimmten Tag, um die Gesamtzahl der Erkennungen für die angezeigten Bedrohungsarten einzublenden. Klicken Sie auf einen Knoten, um zum Protokollfenster für die in der Liste hervorgehobene Bedrohungsart weitergeleitet zu werden.

Tipp

Sie können dieses Widget mehrmals hinzufügen, um beide Ansichten anzuzeigen. Suchen Sie unter dem Widget-Typ **OfficeScan** nach dem Widget, wenn Sie Widgets zu anderen Registerkarten hinzufügen.

Datenschutz-Widgets

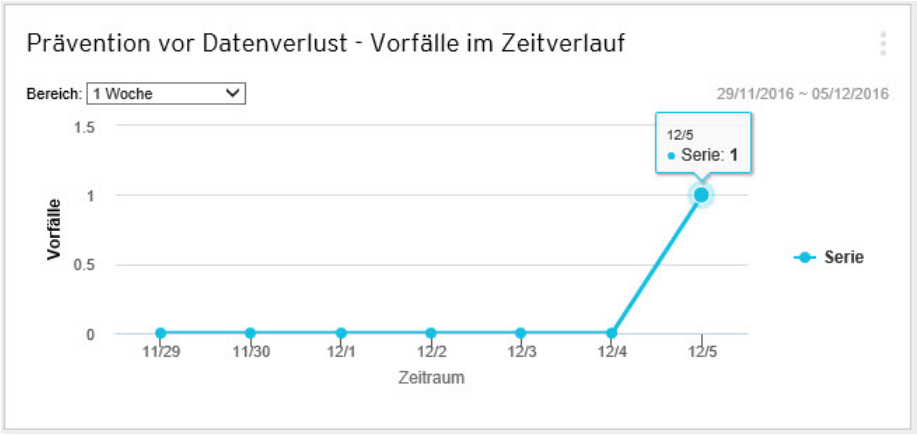
Hinweis

Die Datenschutz-Widgets stehen nach der Aktivierung von OfficeScan Datenschutz zur Verfügung.

Verfügbare Widgets:

- *Prävention vor Datenverlust - Vorfälle im Zeitverlauf-Widget auf Seite 2-23*
- *Häufigste Vorfälle bei "Prävention vor Datenverlust"-Widget auf Seite 2-24*

Prävention vor Datenverlust - Vorfälle im Zeitverlauf-Widget

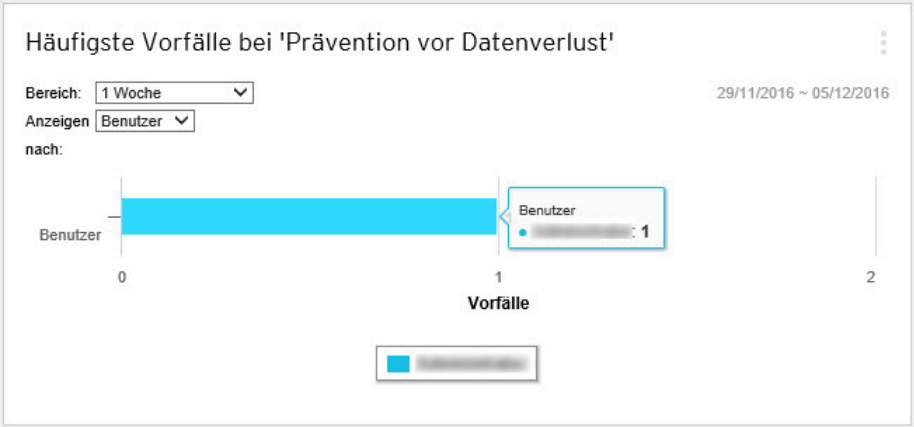


Dieses Widget zeigt die Gesamtzahl der Datenverlustpräventionsvorfälle für einen bestimmten Zeitraum an.

Hinweis

Die Erkennungen umfassen alle Datenverlustpräventionsvorfälle unabhängig von der durchgeführten Aktion („Sperren“ oder „Übergehen“).

Häufigste Vorfälle bei "Prävention vor Datenverlust"-Widget



Dieses Widget zeigt die häufigsten Benutzer, Kanäle, Vorlagen oder Endpunkte an, die Datenverlustpräventionsvorfälle während eines bestimmten Zeitraums ausgelöst haben.

Hinweis

- Dieses Widget zeigt maximal 10 Benutzer, Kanäle, Vorlagen oder Endpunkte an.
- Die Erkennungen umfassen alle Datenverlustpräventionsvorfälle unabhängig von der durchgeführten Aktion („Sperren“ oder „Übergehen“).

Wählen Sie den Typ der anzuzeigenden Datenverlustpräventionsdaten mit Hilfe der Dropdown-Liste **Anzeigen nach** an.

TABELLE 2-5. Ansichten der Datenverlustprävention

ANSICHT	BESCHREIBUNG
Benutzer	Benutzer, die die höchste Anzahl an digitalen Assets übertragen haben • Klicken Sie auf die Benutzernamen unten im Diagramm, um Erkennungsinformationen im Diagramm anzuzeigen/ auszublenden. • Bewegen Sie den Mauszeiger über die Erkennungsbalken, um den Benutzernamen und die Anzahl der Datenverlustpräventionsvorfälle für diesen Benutzer anzuzeigen.
Kanal	Kanäle, die am häufigsten für Übertragungen digitaler Assets benutzt werden • Klicken Sie auf die Kanalnamen unten im Diagramm, um Erkennungsinformationen im Diagramm anzuzeigen/ auszublenden. • Bewegen Sie den Mauszeiger über die Erkennungsbalken, um den Namen des Kanals und die Anzahl der Datenverlustpräventionsvorfälle für diesen Kanal anzuzeigen.
Vorlage	Vorlagen für digitale Assets, die die häufigsten Entdeckungen auslösen • Klicken Sie auf die Vorlagennamen unten im Diagramm, um Erkennungsinformationen im Diagramm anzuzeigen/ auszublenden. • Bewegen Sie den Mauszeiger über die Erkennungsbalken, um den Namen der Vorlage und die Anzahl der Datenverlustpräventionsvorfälle für diese Vorlage anzuzeigen.

ANSICHT	BESCHREIBUNG
Endpunkte	Endpunkte, die die höchste Anzahl an digitalen Assets übertragen • Klicken Sie auf die Endpunktnamen unten im Diagramm, um Erkennungsinformationen im Diagramm anzuzeigen/ auszublenden. • Bewegen Sie den Mauszeiger über die Erkennungsbalken, um den Namen des Endpunkts und die Anzahl der Datenverlustpräventionsvorfälle für diesen Endpunkt anzuzeigen.

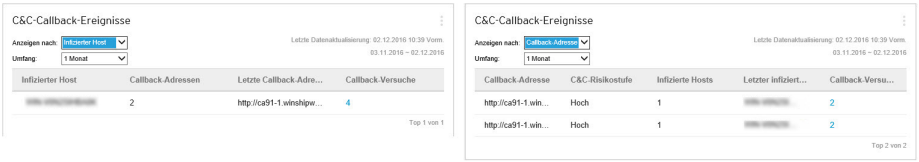
OfficeScan Widgets

Die OfficeScan Widgets bieten eine Kurzübersicht über Angaben zum Sicherheitsstatus sowie Erkennungen von OfficeScan Agent, Plug-in-Programminformationen und Ausbruchsvorfälle.

Verfügbare Widgets:

- *C&C-Callback-Ereignisse-Widget auf Seite 2-26*
- *Erkennung von Sicherheitsrisiken-Widget auf Seite 2-28*
- *OfficeScan- und Plug-in-Mashup-Widget auf Seite 2-29*
- *Antivirus-Agent-Konnektivität-Widget auf Seite 2-30*
- *Mit dem Edge-Relais-Server-Widget verbundene Agents auf Seite 2-32*
- *Virenausbrüche-Widget auf Seite 2-33*
- *Agent-Updates-Widget auf Seite 2-35*

C&C-Callback-Ereignisse-Widget



Das Widget zeigt alle Informationen zu C&C-Callback-Ereignissen an, einschließlich des Angriffsziels sowie der Callback-Adresse der Quelle.

Sie können C&C-Callback-Informationen aus einer bestimmten C&C-Serverliste anzeigen. Klicken Sie zur Auswahl der Listenquelle (Global Intelligence, Virtual Analyzer) auf das Symbol "Bearbeiten" (>) und wählen Sie die gewünschte Liste in der Dropdown-Liste **C&C-Listenquelle** aus.

Verwenden Sie die Dropdown-Liste **Anzeigen nach**, um den Typ der angezeigten C&C-Callback-Daten auszuwählen:

- **Infizierter Host**: Zeigt aktuelle C&C-Informationen nach Ziel-Endpunkt an.

  TABELLE 2-6. Angaben zu infizierten Hosts

SPALTE	BESCHREIBUNG
Infizierter Host	Der Name des Endpunkts, der das Ziel eines C&C-Angriffs ist
Callback-Adressen	Die Anzahl der Callback-Adressen, mit denen der Endpunkt eine Verbindung herstellen wollte
Letzte Callback-Adresse	Die letzte Callback-Adresse, mit der der Endpunkt eine Verbindung herstellen wollte
Callback-Versuche	Die Anzahl der Versuche der Verbindungsaufnahme mit der Callback-Adresse durch den angegriffenen Endpunkt **Hinweis** Klicken Sie auf den Link, um den Bildschirm **C&C-Callback-Protokolle** mit detaillierteren Angaben zu öffnen.

- **Callback-Adresse**: Zeigt aktuelle C&C-Informationen nach C&C-Callback-Adresse an.

  TABELLE 2-7. Angaben zu C&C-Adressen

SPALTE	BESCHREIBUNG
Callback-Adresse	Die Adresse von aus dem Netzwerk stammenden C&C-Callbacks

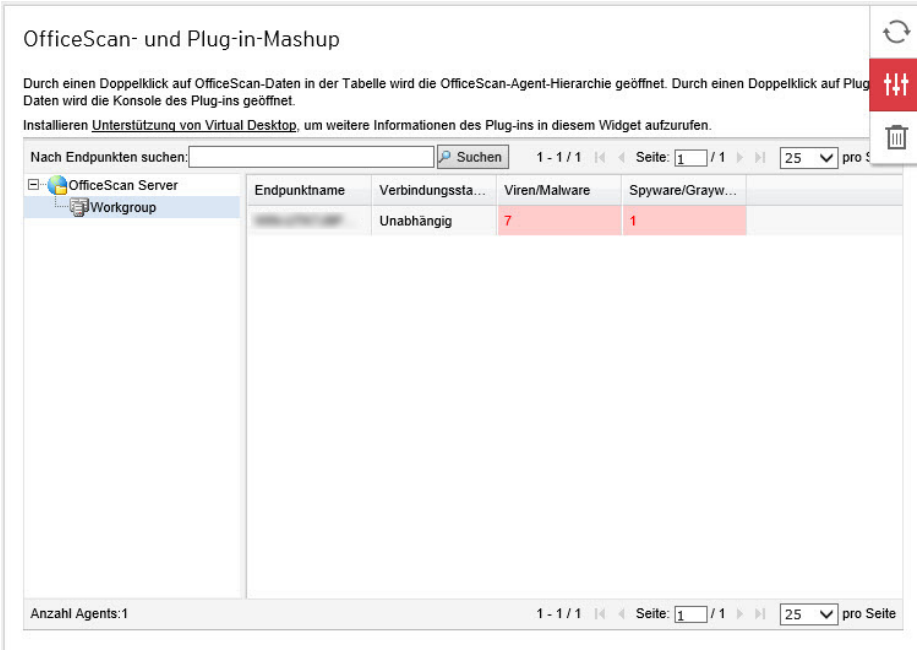
Spalte	Beschreibung
C&C-Risikostufe	Die Risikostufe der Callback-Adresse laut Global Intelligence- oder Virtual Analyzer-Liste
Infizierte Hosts	Die Anzahl der von der Callback-Adresse angegriffenen Endpunkte
Letzter infizierter Host	Der Name des Endpunkts, der zuletzt eine Verbindung mit der C&C-Callback-Adresse herstellen wollte
Callback-Versuche	Die Anzahl der Callback-Versuche vom Netzwerk an die Adresse **Hinweis** Klicken Sie auf den Link, um den Bildschirm **C&C-Callback-Protokolle** mit detaillierteren Angaben zu öffnen.

Erkennung von Sicherheitsrisiken-Widget

Dieses Widget zeigt die Anzahl der erkannten Sicherheitsrisiken sowie die Anzahl der betroffenen Endpunkte an.

Klicken Sie auf die Endpunktanzahl, um das Fenster **Agent-Verwaltung** zu öffnen, in dem die betroffenen OfficeScan Agents in der Agent-Hierarchie angezeigt werden.

OfficeScan- und Plug-in-Mashup-Widget



Das Widget kombiniert Daten aus OfficeScan Agents und installierten Plug-in-Programmen und stellt diese Daten dann in der Agent-Hierarchie dar. Dieses Widget unterstützt Sie dabei, den Schutzumfang der Agents schnell zu bewerten und den erforderlichen Verwaltungsaufwand der individuellen Plug-in-Programme zu reduzieren.

Dieses Widget zeigt Daten aus den folgenden Plug-in-Programmen an:

- Unterstützung für Trend Micro Virtual Desktop

Wichtig

Sie müssen zuerst ein unterstütztes Plug-in-Programm aktivieren, damit die entsprechenden Daten im Mashup-Widget angezeigt werden können. Aktualisieren Sie die Plug-in-Programme, wenn neuere Versionen verfügbar sind.

Zur Auswahl der in der Agent-Hierarchie angezeigten Spalten klicken Sie auf die Schaltfläche **Weitere Optionen** oben rechts im Widget und dann auf die Schaltfläche **Einstellungen**.

Klicken Sie auf die Daten in einer beliebigen Spalte, um die Konsole des entsprechenden Plug-in-Programms oder das OfficeScan Fenster **Agent-Verwaltung** zu öffnen. Das angezeigte Fenster richtet sich nach dem ausgewählten Datentyp.

Antivirus-Agent-Konnektivität-Widget

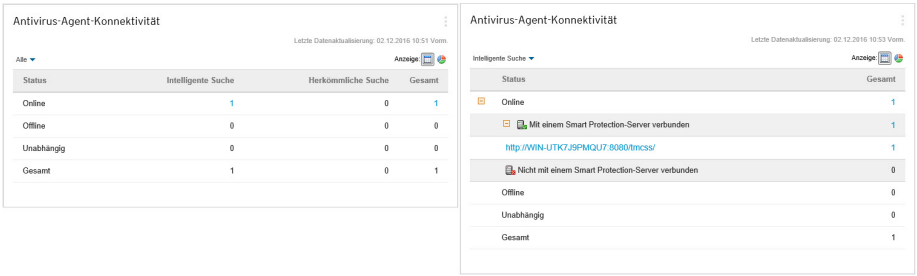


ABBILDUNG 2-4. Standardansicht zur Anzeige aller Agents der intelligenten und herkömmlichen Suche sowie eine erweiterte Ansicht des Agents der intelligenten Suche mit Smart Protection Servern

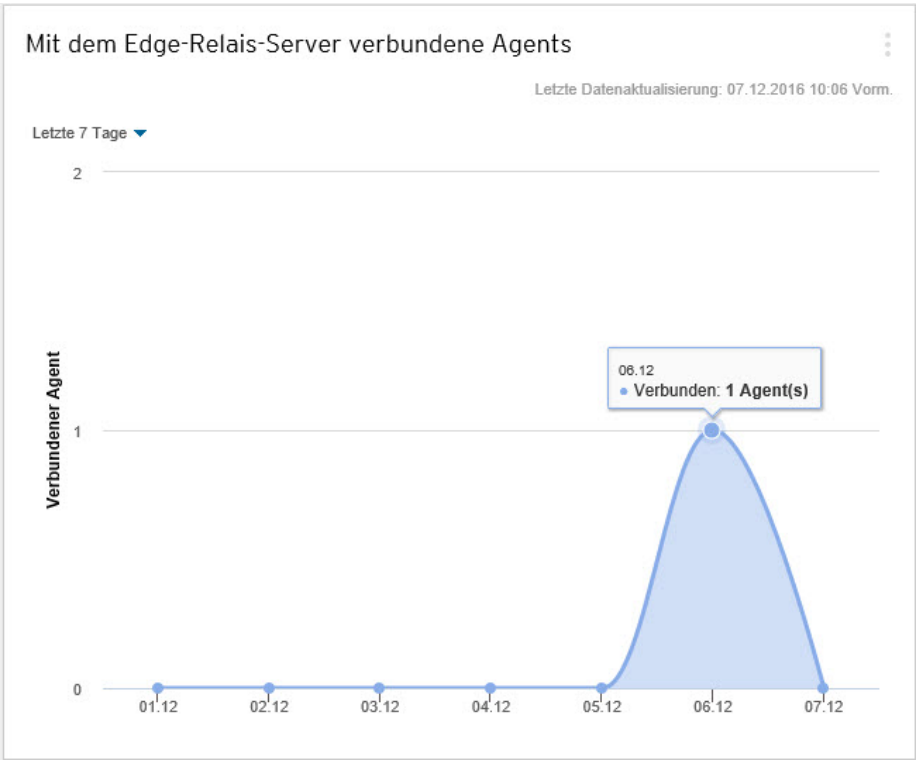
Dieses Widget zeigt den Verbindungsstatus von OfficeScan Agents für den OfficeScan Server in Bezug auf die konfigurierte Suchmethode (intelligente und herkömmliche Suche).

Sie können die Daten in einer Tabelle oder einem Tortendiagramm anzeigen, indem Sie auf die Anzeigesymbole klicken ( ).

Verwenden Sie die Dropdown-Liste oberhalb der Tabelle/des Diagramms, um den Typ der angezeigten Daten zu ändern. Klicken Sie auf die Anzahl für jeden Status, um das Fenster **Agent-Verwaltung** zu öffnen, in dem die zugehörigen OfficeScan Agents in der Agent-Struktur aufgelistet werden.

Ansicht	Beschreibung
Alle	Zeigt den Verbindungsstatus aller OfficeScan Agents für beide Suchmethoden an.
Herkömmliche Suche	Zeigt den Verbindungsstatus aller OfficeScan Agents an, die die herkömmliche Suche verwenden.
Intelligente Suche	Zeigt den Verbindungsstatus aller OfficeScan Agents an, die die intelligente Suche verwenden. Gehen Sie bei der Anzeige des Agent-Verbindungsstatus in einer Tabelle folgendermaßen vor: • Erweitern Sie die Informationen des „Online“-Agents, um den Status der Verbindungen zwischen Agents und einem Smart Protection Server anzuzeigen. • Klicken Sie auf die URL, um die Management-Konsole des Smart Protection Servers zu öffnen. **Hinweis** Nur Online-Agents (die Berichte für den OfficeScan Server erstellen) können den Status ihrer Verbindung mit Smart Protection Servern melden. Informationen zur Wiederherstellung der Verbindung eines Offline-Agents mit einem Smart Protection Server finden Sie unter *Lösungen für Probleme, die durch OfficeScan Agent-Symbole angezeigt werden auf Seite 15-43*.

Mit dem Edge-Relais-Server-Widget verbundene Agents



Dieses Widget zeigt die Anzahl der OfficeScan Agents, die für einen bestimmten Zeitraum mit dem OfficeScan Edge-Relais-Server verbunden sind.

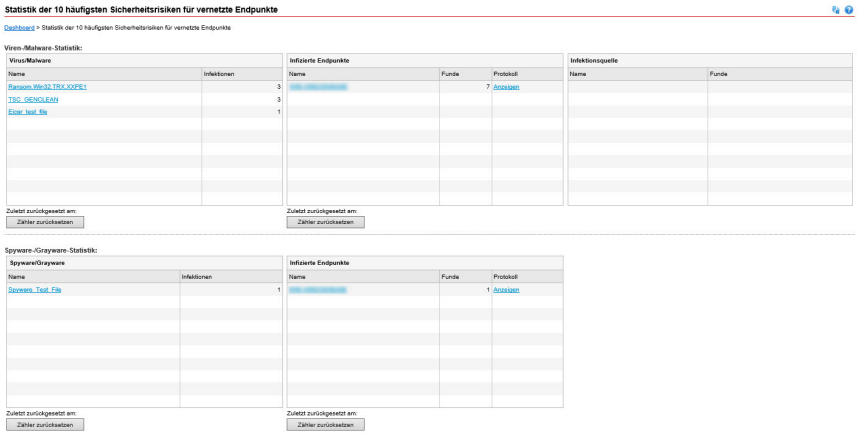
Virenausbrüche-Widget

Das Widget **Virenausbrüche** zeigt den Status aller derzeitigen Ausbrüche von Sicherheitsrisiken und den letzten Ausbruchsalarm an.

- Klicken Sie auf das Datum oder die Uhrzeit der Warnung, um weitere Details zum Ausbruch anzuzeigen.
- Wenn OfficeScan einen Ausbruch erkennt, können Sie den Status der Ausbruchswarnungen mit Hilfe der Option **Zurücksetzen** ändern und sofort Maßnahmen zur Ausbruchsprävention ergreifen.

  Weitere Informationen über die Durchsetzung von Maßnahmen zur Ausbruchsprävention finden Sie unter *Ausbruchpräventionsrichtlinien auf Seite 7-123*.

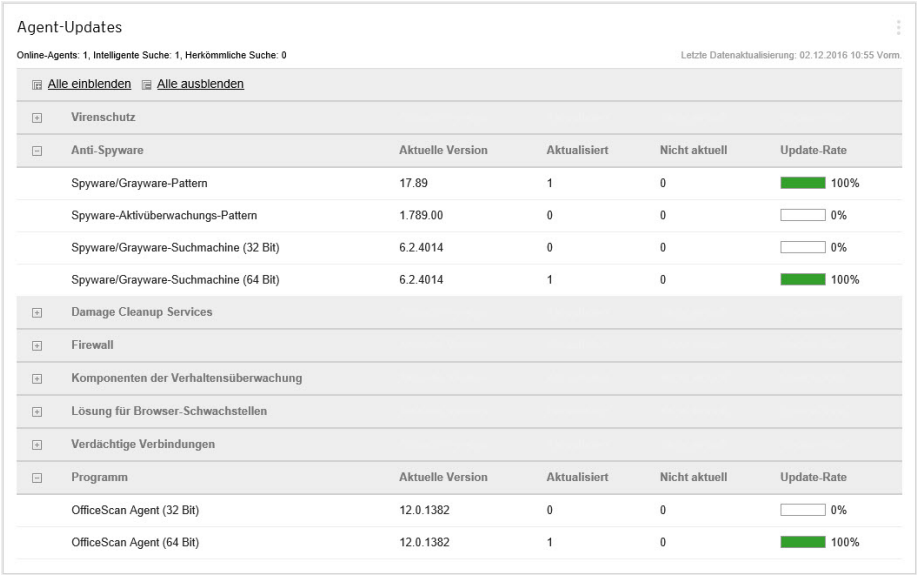
- Klicken Sie auf **Statistik der 10 häufigsten Sicherheitsrisiken anzeigen**, um die am häufigsten auftretenden Sicherheitsrisiken, die Endpunkte mit den meisten Sicherheitsrisiken und die häufigsten Infektionsquellen anzuzeigen.



Im Fenster **Statistik der 10 häufigsten Sicherheitsrisiken** können Sie:

- detaillierte Informationen zu einem Sicherheitsrisiko anzeigen (durch Klicken auf den Namen des Risikos)
- den allgemeinen Status eines bestimmten Endpunkts anzeigen (durch Klicken auf den Namen des Endpunkts)
- Protokolle zu Sicherheitsrisiken für den Endpunkt anzeigen (durch Klicken auf **Anzeigen** neben dem Endpunktnamen)
- die Statistiken in jeder Tabelle zurücksetzen (durch Klicken auf **Zähler zurücksetzen**)

Agent-Updates-Widget



Dieses Widget zeigt Komponenten und Programme an, die OfficeScan Agents vor Sicherheitsrisiken schützen.

Klicken Sie auf „Nicht aktuell“, um das Fenster **Agent-Verwaltung** zu öffnen, in dem die OfficeScan Agents, die Updates benötigen, in der Agent-Struktur aufgelistet werden.

Management-Widget

Das Management-Widget zeigt den Verbindungsstatus der OfficeScan Agents mit dem OfficeScan Server an.

Verfügbare Widgets:

- *Agent-Server-Konnektivität-Widget auf Seite 2-36*

Agent-Server-Konnektivität-Widget

Dieses Widget zeigt den Verbindungsstatus aller Agents mit dem OfficeScan Server an.

Sie können zwischen der Tabelle und dem Kreisdiagramm umschalten, indem Sie auf das entsprechende Anzeigesymbol klicken ( ).

Klicken Sie auf die Anzahl für jeden Status, um das Fenster **Agent-Verwaltung** zu öffnen, in dem die zugehörigen OfficeScan Agents in der Agent-Struktur aufgelistet werden.

Active Directory-Integration

Sie können OfficeScan in Ihre Microsoft™ Active Directory™-Struktur integrieren, um OfficeScan Agents effizienter zu verwalten, Berechtigungen für die Webkonsole mit Hilfe von Active Directory-Konten zuzuweisen und festzustellen, auf welchen Agents keine Sicherheitssoftware installiert ist. Alle Benutzer in der Netzwerkdomäne können sicheren Zugriff auf die OfficeScan Konsole haben. Sie können auch einen begrenzten Zugriff für bestimmte Benutzer konfigurieren, selbst wenn sich diese in einer anderen Domäne befinden. Über den Authentifizierungsprozess und den

Verschlüsselungsschlüssel können Sie die Gültigkeit der Anmeldedaten der Benutzer überprüfen.

Durch die Integration in Active Directory können Sie die folgenden Funktionen in vollem Umfang nutzen:

- **Benutzerdefinierte Agent-Gruppen**: In der OfficeScan Agent-Hierarchie können Sie die Agents manuell gruppieren und Domänen zuordnen, indem Sie Active Directory- oder IP-Adressen verwenden.

  Weitere Informationen finden Sie unter *Automatische Agent-Gruppierung auf Seite 2-56*.

- **Nicht verwaltete Endpunkte**: Stellen Sie sicher, dass die Endpunkte im Netzwerk, die nicht vom OfficeScan Server verwaltet werden, die Sicherheitsrichtlinien Ihres Unternehmens erfüllen.

  Weitere Informationen finden Sie unter *Einhaltung der Sicherheitsrichtlinien für nicht verwaltete Endpunkte auf Seite 15-78*.

Führen Sie mit dem OfficeScan Server eine manuelle oder periodische Synchronisation der Active Directory-Struktur durch, um Datenkonsistenz zu gewährleisten.

Weitere Informationen finden Sie unter *Daten mit Active Directory-Domänen synchronisieren auf Seite 2-39*.

Active Directory mit OfficeScan integrieren

Prozedur

1. Navigieren Sie zu **Administration** > **Active Directory** > **Active Directory-Integration**.
2. Geben Sie unter **Active Directory-Domänen** den Namen der Active Directory-Domäne an.
3. Geben Sie Anmeldedaten an, die der OfficeScan Server verwendet, wenn Daten mit der angegebenen Active Directory-Domäne synchronisiert werden. Wenn der Server nicht Teil der Domäne ist, sind Anmeldedaten erforderlich. Andernfalls sind Anmeldedaten optional. Stellen Sie sicher, dass diese Anmeldedaten nicht ablaufen, da der Server andernfalls keine Daten synchronisieren kann.

a. Klicken Sie auf **Anmeldedaten der Domäne angeben**.

b. Geben Sie im daraufhin geöffneten Popup-Fenster den Benutzernamen und das Kennwort ein. Für die Angabe des Benutzernamens kann eines der folgenden Formate verwendet werden:

- `Domäne\Benutzername`
- `Benutzername@Domäne`

c. Klicken Sie auf **Speichern**.

4. Klicken Sie auf die Schaltfläche (+), um weitere Domänen hinzuzufügen. Geben Sie, wenn nötig, die Domänen-Anmeldedaten für jede hinzugefügte Domäne an.

5. Klicken Sie auf die Schaltfläche (-), um Domänen zu löschen.

6. Legen Sie Verschlüsselungseinstellungen fest, wenn Sie Domänen-Anmeldedaten angegeben haben. Zur Sicherheit verschlüsselt OfficeScan die von Ihnen angegebenen Domänen-Anmeldedaten, bevor sie in der Datenbank gespeichert werden. Wenn OfficeScan Daten mit einer der angegebenen Domänen synchronisiert, wird ein Verschlüsselungsschlüssel verwendet, um die Domänen-Anmeldedaten zu entschlüsseln.

a. Wechseln Sie zum Abschnitt **Verschlüsselungseinstellungen für die Anmeldedaten für die Domäne**.

b. Geben Sie einen Verschlüsselungsschlüssel mit maximal 128 Zeichen ein.

c. Geben Sie eine Datei an, in der der Verschlüsselungsschlüssel gespeichert werden soll. Sie können ein gängiges Dateiformat wie beispielsweise `.txt` wählen. Geben Sie den vollständigen Pfad und Namen der Datei ein. Beispiel: `C:\AD_Encryption\EncryptionKey.txt`.

Warnung!

Wenn die Datei entfernt wird oder sich der Dateipfad ändert, kann OfficeScan die Daten nicht mit allen der angegebenen Domänen synchronisieren.

7. Klicken Sie auf eine der folgenden Optionen:

- **Speichern**: Nur die Einstellungen speichern. Da das Synchronisieren von Daten die Netzwerkressourcen belasten können, können Sie wählen, nur die Einstellungen zu speichern und das Synchronisieren zu einem späteren Zeit, wie z. B. außerhalb der Geschäftszeiten, durchzuführen.
- **Speichern und synchronisieren**: Einstellungen speichern und Daten mit den Active Directory-Domänen sychronisieren.

8. Planen Sie regelmäßige Synchronisierungsdurchläufe. Weitere Informationen finden Sie unter *Daten mit Active Directory-Domänen synchronisieren auf Seite 2-39*.

Daten mit Active Directory-Domänen synchronisieren

Synchronisieren Sie regelmäßig Daten mit Active-Directory-Domänen, um die Struktur der OfficeScan agent-Hierarchie auf dem aktuellen Stand zu halten und nicht verwaltete agents abzufragen.

Daten mit Active Directory-Domänen manuell synchronisieren

Prozedur

1. Navigieren Sie zu **Administration** > **Active Directory** > **Active Directory-Integration**.
2. Stellen Sie sicher, dass sich die Anmeldedaten für die Domäne und die Verschlüsselungseinstellungen nicht geändert haben.
3. Klicken Sie auf **Speichern und synchronisieren**.

Daten mit Active Directory-Domänen automatisch synchronisieren

Prozedur

1. Navigieren Sie zu **Administration** > **Active Directory** > **Zeitgesteuerte Synchronisierung**.
2. Wählen Sie **Zeitgesteuerte Synchronisierung des Active Directory aktivieren**.
3. Geben Sie den Synchronisierungszeitplan an.

   Hinweis

   Bei der täglichen, wöchentlichen und monatlichen Synchronisierung handelt es sich beim Zeitraum um die Stunden, während der OfficeScan Active Directory mit dem OfficeScan Server synchronisiert.

4. Klicken Sie auf **Speichern**.

Die OfficeScan Agent-Hierarchie

In der OfficeScan Agent-Hierarchie werden alle in Domänen gruppierten agents angezeigt, die zurzeit vom Server verwaltet werden. Agents werden in Domänen gruppiert, so dass Sie für alle Domänenmitglieder gleichzeitig dieselbe Konfiguration festlegen, verwalten und übernehmen können.

Verbindungsstatus des Agents

Der OfficeScan Agent-Verbindungsstatus richtet sich danach, wie der OfficeScan Server mit dem OfficeScan Agent kommuniziert. In der folgenden Tabelle werden die verschiedenen Verbindungsstatus für den OfficeScan Agent erläutert.

TABELLE 2-8. Verbindungsstatus des Office Agents

STATUS	BESCHREIBUNG
Online	Der OfficeScan Agent kann eine Verbindung zum OfficeScan Server herstellen, um die bidirektionale Kommunikation zwischen folgenden Objekten zu ermöglichen: • Richtlinieneinstellungen • Updates • Suchbefehle • Synchronisierung der Listen der verdächtigen Objekte • Exemplar Zusendung • Protokollweiterleitung
Offline	Der OfficeScan Agent weist keine funktionierende Verbindung mit dem OfficeScan Server oder dem Edge-Relais-Server auf.
Unabhängig	Der OfficeScan Agent kann eine Verbindung zum Server herstellen, die Kommunikation ist jedoch eingeschränkt. Unabhängiger Modus: • In diesem Modus akzeptiert der OfficeScan Agent keine Richtlinieneinstellungen vom Server. • In diesem Modus startet der OfficeScan Agent Suchbefehle über den Server. • In diesem Modus sendet der OfficeScan Agent keine Protokolle an den Server. Sie können unabhängige Agents mit Berechtigungen zum Zulassen oder Blockieren von Komponenten-Updates konfigurieren, wenn eine funktionierende Verbindung zum OfficeScan Server verfügbar ist. Endbenutzer können Suchläufe und Updates auf Agents im unabhängigen Modus manuell starten.

Status	Beschreibung
Extern	Der OfficeScan Agent befindet sich außerhalb des Netzwerks und kann keine direkte Verbindung zum OfficeScan Server herstellen. Der OfficeScan Agent kann jedoch eine Verbindung zu einem Edge-Relais-Server für die folgenden Objekte herstellen: • Synchronisierung der Listen der verdächtigen Objekte • Exemplar Zusendung • Protokollweiterleitung **Hinweis** Als **Verbindungsstatus** für einen externen Agent wird „Offline“ in der Agent-Hierarchie angezeigt, da der OfficeScan-Server nicht direkt mit dem OfficeScan Agent verbunden ist.

Symbole in der Agent-Ansicht

Die Symbole in der OfficeScan agent-Hierarchie bieten optische Hinweise auf den Endpunkttyp und den Status der OfficeScan Agents, die von OfficeScan verwaltet werden.

Tabelle 2-9. OfficeScan Symbole in der Agent-Ansicht

Symbol	Beschreibung
	Domäne
	Root
	Update-Agent
	Agent der herkömmlichen Suche

SYMBOL	BESCHREIBUNG
	Intelligente Suche verfügbar – OfficeScan Agent
	Intelligente Suche nicht verfügbar – OfficeScan Agent
	Intelligente Suche verfügbar - Update-Agent
	Intelligente Suche nicht verfügbar - Update-Agent

Agent-Hierarchie durchsuchen

Verwenden Sie die Such- und Anzeigefunktionen über der Agent-Hierarchie (**Agents** > **Agent-Verwaltung**), um bestimmte von OfficeScan verwaltete Endpunkte zu ermitteln.

Prozedur

- Sie können nach einem bestimmten zu verwaltenden Agent suchen, indem Sie seinen Namen in das Textfeld **Nach Endpunkten suchen** eingeben.

  Eine Liste mit den Ergebnissen wird nun in der Agent-Hierarchie angezeigt. Um weitere Suchoptionen anzuzeigen, klicken Sie auf **Erweiterte Suche**.

  Hinweis

  Sie müssen die erweiterte Suchfunktion verwenden, um Endpunkte mit IPv4- oder IPv6-Adressen zu suchen.

  Weitere Informationen finden Sie unter *Erweiterte Suchoptionen auf Seite 2-44*.

- Nach Auswahl einer Domäne wird die Agent-Hierarchie erweitert, so dass alle zu dieser Domäne gehörenden Agents und alle Spalten mit wichtigen Informationen zu jedem Agent angezeigt werden. Um nur bestimmte zusammengehörige Spalten anzuzeigen, wählen Sie ein Element in der Agent-Hierarchie aus.

- **Alle anzeigen**: Zeigt alle Spalten an.
- **Update-Ansicht**: Zeigt alle Komponenten und Programme an.
- **Virenschutz-Ansicht**: Zeigt Virenschutzkomponenten an.
- **Anti-Spyware-Ansicht**: Zeigt Anti-Spyware-Komponenten an.
- **Datenschutzansicht**: Zeigt den Status des Datenschutzmoduls auf den Agents an.
- **Firewall-Ansicht**: Zeigt Firewall-Komponenten an.
- **Smart Protection Ansicht**: Zeigt die Suchmethode, die von den Agents verwendet wird (konventionell oder intelligente Suche), und die Smart Protection Komponenten an.
- **Ansicht 'Update-Agent'**: Zeigt Informationen zu allen Update-Agents an, die vom OfficeScan Server verwaltet werden.
- **Ansicht 'Externer Agent'**: Zeigt Informationen für alle Agents an, die an den Edge-Relais-Server berichten.

Erweiterte Suchoptionen

Suchen Sie anhand der folgenden Kriterien nach Agents:

Abschnitt	Beschreibung
Grundlegende Kriterien	Beinhaltet grundlegende Informationen über Endpunkte wie IP-Adresse, Betriebssystem, Domäne, MAC-Adresse, Suchmethode und Web-Reputation-Status. • Bei der Suche nach IPv4-Segment müssen Sie einen Teil einer IP-Adresse, beginnend mit den ersten 8 Bit, eingeben. Das Suchergebnis enthält alle Endpunkte, deren IP-Adressen diesen Eintrag enthalten. Beispielsweise werden bei der Eingabe von "10.5" alle Computer mit einer IP-Adresse im Bereich zwischen 10.5.0.0 und 10.5.255.255 gefunden. • Bei der Suche nach dem IPv6-Adressbereich müssen Sie Präfix und Länge der IP-Adresse eingeben. • Die Suche nach MAC-Adresse erfordert die Eingabe eines MAC-Adressbereichs in der hexadezimalen Notation, z. B. 000A1B123C12.
Komponenten version	Aktivieren Sie das Kontrollkästchen neben dem Computernamen, grenzen Sie das Kriterium durch Auswahl von **Älter als** oder **Bis einschließlich** ein und geben Sie dann eine Versionsnummer ein. Die aktuelle Versionsnummer wird standardmäßig angezeigt.
Status	Beinhaltet Agent-Einstellungen

Klicken Sie nach Eingabe Ihrer Suchkriterien auf **Suchen**. Eine Liste der Endpunkte, die die Kriterien erfüllen, wird in der Agent-Hierarchie angezeigt.

Bestimmte Aufgaben in der Agent-Hierarchie

Die agent-Hierarchie wird angezeigt, wenn Sie bestimmte Fenster auf der Webkonsole öffnen. Oberhalb der agent-Hierarchie befinden sich Menübefehle, die sich auf das gerade geöffnete Fenster beziehen. Mit Hilfe dieser Menübefehle können Sie bestimmte Aufgaben ausführen, z. B. die Konfiguration der agent-Einstellungen oder die Initiierung von agent-Aufgaben. Um eine Aufgabe durchzuführen, wählen Sie zuerst das Aufgabenziel und dann einen Menüeintrag aus.

Die agent-Hierarchie wird in den folgenden Fenstern angezeigt:

- *Fenster Agent-Verwaltung auf Seite 2-46*

- *Ausbruchsprävention auf Seite 2-50*
- *Fenster Agent-Auswahl auf Seite 2-51*
- *Rollback auf Seite 2-51*
- *Sicherheitsrisiko-Protokolle auf Seite 2-52*

Fenster Agent-Verwaltung

Um dieses Fenster anzuzeigen, navigieren Sie zu **Agents** > **Agent-Verwaltung**.

Im Fenster **Agent-Verwaltung** können Sie allgemeine Agent-Einstellungen verwalten und Statusinformationen zu bestimmten Agents anzeigen (z. B. **Benutzer anmelden**, **IP-Adresse** und **Verbindungsstatus**).

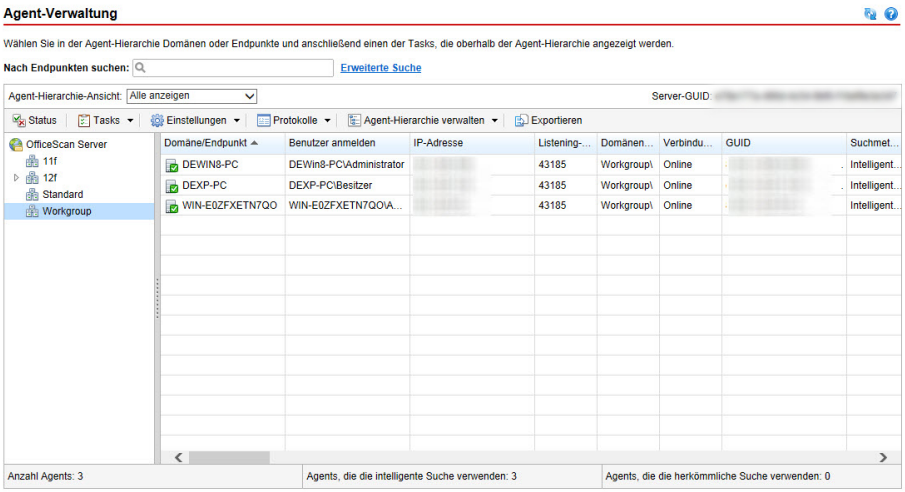


ABBILDUNG 2-5. Fenster Agent-Verwaltung

Die Aufgaben, die Sie durchführen können, werden in der folgenden Tabelle aufgeführt:

TABELLE 2-10. Aufgaben zur Agent-Verwaltung

MENÜSCHALTFLÄCHE	AUFGABE
Status	Detaillierte Agent-Informationen anzeigen. Weitere Informationen finden Sie unter *OfficeScan Agent-Informationen anzeigen auf Seite 15-60*.
Aufgaben	• Die Funktion "Jetzt durchsuchen" auf Agent-Endpunkten ausführen. Weitere Informationen finden Sie unter *Jetzt durchsuchen starten auf Seite 7-28*. • Agent deinstallieren. Weitere Informationen finden Sie unter *Den OfficeScan Agent von der Webkonsole aus deinstallieren auf Seite 5-75*. • Erkannte verdächtige Dateien wiederherstellen. Weitere Informationen finden Sie unter *Dateien in der Quarantäne wiederherstellen auf Seite 7-50*. • Spyware-/Grayware-Komponenten wiederherstellen. Weitere Informationen finden Sie unter *Spyware/Grayware wiederherstellen auf Seite 7-59*.

Einstellungen	• Konfigurieren Sie die Sucheinstellungen. Weitere Informationen finden Sie unter den folgenden Themen:
	  • *Suchmethodentypen auf Seite 7-9*
	  • *Manuelle Suche auf Seite 7-20*
	  • *Echtzeitsuche auf Seite 7-17*
	  • *Zeitgesteuerte Suche auf Seite 7-22*
	  • *Jetzt durchsuchen auf Seite 7-25*
	• Web-Reputation-Einstellungen konfigurieren. Weitere Informationen finden Sie unter *Web-Reputation-Richtlinien auf Seite 12-5*.
	• Konfigurieren Sie Einstellungen für "Vorausschauendes Maschinenlernen". Weitere Informationen finden Sie unter *Konfigurieren der Einstellungen für "Vorausschauendes Maschinenlernen" auf Seite 8-4*.

Menüschaltfläche	Aufgabe
	• Verdächtige Verbindungseinstellungen konfigurieren. Weitere Informationen finden Sie unter *Verdächtige Verbindungseinstellungen konfigurieren auf Seite 8-9*. • Konfugurieren Sie die Einstellungen der Verhaltensüberwachung. Weitere Informationen finden Sie unter *Verhaltensüberwachung auf Seite 9-2*. • Konfigurieren Sie die Einstellungen der Gerätesteurung. Weitere Informationen finden Sie unter *Gerätesteuerung auf Seite 10-2*. • Konfigurieren Sie Richtlinien für die Prävention vor Datenverlust. Weitere Informationen finden Sie unter *Richtlinienkonfiguration der Funktion "Prävention vor Datenverlust" auf Seite 11-51*. • Konfigurieren Sie die Einstellungen für die Exemplarzusendung. Weitere Informationen finden Sie unter *Konfigurieren der Exemplar Zusendung auf Seite 8-12*. • Agents als Update-Agents zuweisen. Weitere Informationen finden Sie unter *Konfiguration des Update-Agents auf Seite 6-59*. • Agent-Berechtigungen und andere Einstellungen konfigurieren. Weitere Informationen finden Sie unter *Agent-Berechtigungen und weitere Einstellungen konfigurieren auf Seite 15-101*. • OfficeScan Agent-Dienste aktivieren oder deaktivieren. Weitere Informationen finden Sie unter *OfficeScan Agent Dienste auf Seite 15-7*. • Die Liste der zugelassenen Spyware/Grayware konfigurieren. Weitere Informationen finden Sie unter *Liste der zugelassenen Spyware/Grayware auf Seite 7-57*. • Liste der vertrauenswürdigen Programme konfigurieren. Weitere Informationen finden Sie unter *Liste der vertrauenswürdigen Programme konfigurieren auf Seite 7-61*. • Agent-Einstellungen importieren und exportieren. Weitere Informationen finden Sie unter *Agent-Einstellungen importieren und exportieren auf Seite 15-60*.

MENÜSCHALTFLÄCHE	AUFGABE
Protokolle	Die folgenden Protokolle anzeigen: • Viren/Malware-Protokolle (weitere Informationen hierzu finden Sie unter *Viren-/Malware-Protokolle anzeigen auf Seite 7-101*) • Spyware/Grayware-Protokolle (weitere Informationen hierzu finden Sie unter *Spyware/Grayware-Protokolle anzeigen auf Seite 7-110*) • Firewall-Protokolle (weitere Informationen hierzu finden Sie unter *Firewall-Protokolle auf Seite 13-32*) • Web-Reputation-Protokolle (weitere Informationen hierzu finden Sie unter *Protokolle für Internet-Bedrohungen auf Seite 12-23*) • Protokolle zu verdächtigen Verbindungen (weitere Informationen hierzu finden Sie unter *Protokolle zu verdächtigen Verbindungen anzeigen auf Seite 8-17*) • Protokolle zu verdächtigen Dateien (weitere Informationen hierzu finden Sie unter *Protokolle zu verdächtigen Dateien anzeigen auf Seite 7-115*) • C&C-Callback-Protokolle (weitere Informationen hierzu finden Sie unter *C&C Callback-Protokolle anzeigen auf Seite 12-25*) • Verhaltensüberwachungsprotokolle (weitere Informationen hierzu finden Sie unter *Verhaltensüberwachungsprotokolle auf Seite 9-24*) • Protokolldaten für "Vorausschauendes Maschinenlernen" (weitere Informationen hierzu finden Sie unter *Anzeigen von Protokolldaten für "Vorausschauendes Maschinenlernen" auf Seite 8-13*) • Protokolle der Gerätesteuerung (weitere Informationen hierzu finden Sie unter *Protokolle der Gerätesteuerung auf Seite 10-19*) • DLP-Protokolle (weitere Informationen hierzu finden Sie unter *Protokolle für 'Prävention vor Datenverlust' auf Seite 11-63*) • Protokolle zu Suchvorgängen (weitere Informationen hierzu finden Sie unter *Protokolle zu Suchvorgängen anzeigen auf Seite 7-116*)

MENÜSCHALTFLÄCHE	AUFGABE
	Protokolle löschen. Weitere Informationen finden Sie unter *Protokollmanagement auf Seite 14-47*.
Agent-Hierarchie verwalten	Die Agent-Hierarchie verwalten. Weitere Informationen finden Sie unter *Aufgaben zur Agent-Gruppierung auf Seite 2-61*.
Exportieren	Liste der Agents als komma-separierte Datei im CSV-Format (`.csv`) exportieren.

Ausbruchsprävention

Um dieses Fenster anzuzeigen, navigieren Sie zu **Agents** > **Ausbruchsprävention**.

Geben Sie die Einstellungen zur Ausbruchsprävention im Fenster **Ausbruchsprävention** ein und aktivieren Sie sie. Weitere Informationen finden Sie unter *Ausbruchsprävention bei Sicherheitsrisiken konfigurieren auf Seite 7-121*.

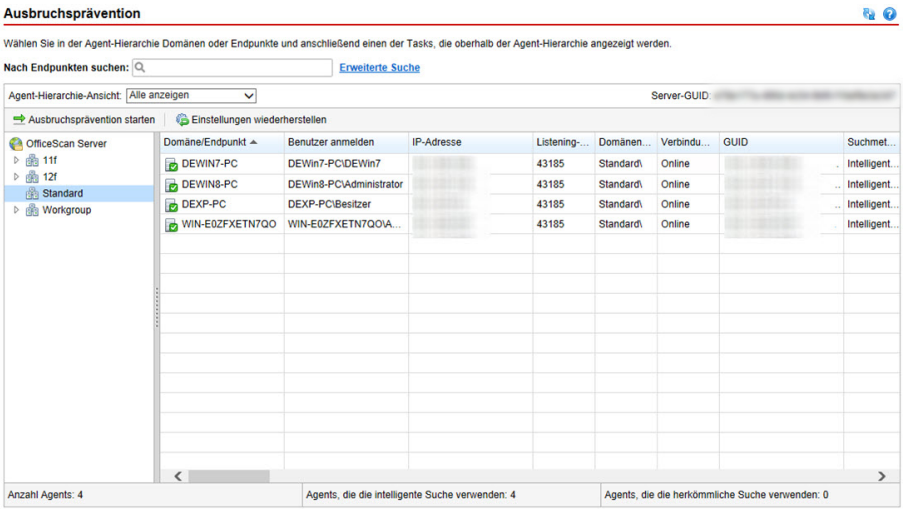


ABBILDUNG 2-6. Ausbruchsprävention

Fenster Agent-Auswahl

Um dieses Fenster anzuzeigen, navigieren Sie zu **Updates** > **Agents** > **Manuelles Update** Wählen Sie **Agents manuell auswählen**, und klicken Sie auf **Auswählen**.

Manuelles Update im Fenster **Agent-Auswahl** starten. Weitere Informationen finden Sie unter *OfficeScan Agent Manuelle Updates auf Seite 6-47*.

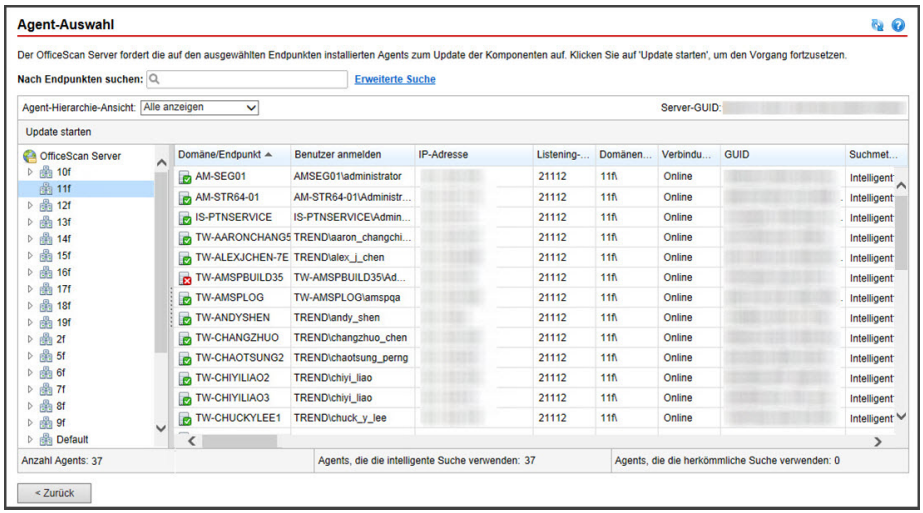


ABBILDUNG 2-7. Fenster Agent-Auswahl

Rollback

Um dieses Fenster anzuzeigen, navigieren Sie zu **Updates** > **Rollback**. Klicken Sie auf **Mit Server synchronisieren**.

Führen Sie ein Rollback der agent-Komponenten im Fenster **Rollback** durch. Weitere Informationen finden Sie unter *Durchführen eines Rollbacks der Komponenten für OfficeScan Agenten auf Seite 6-56*.

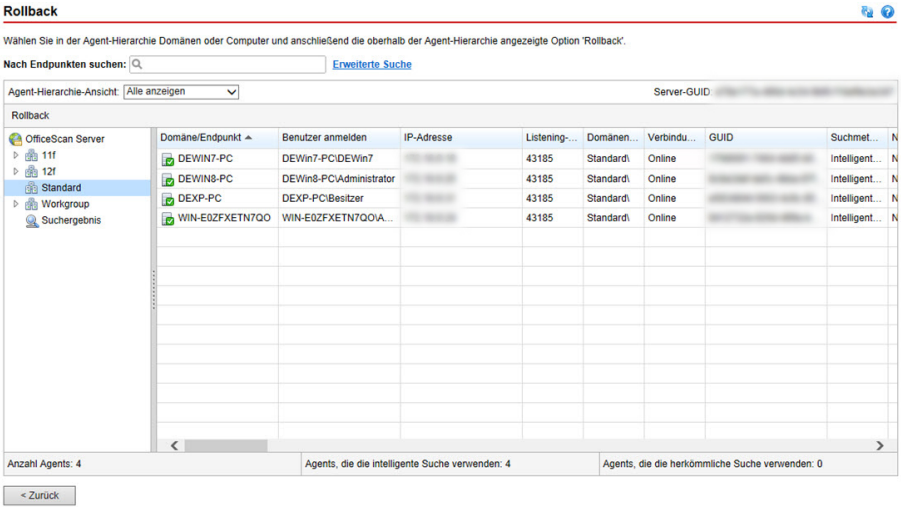


ABBILDUNG 2-8. Rollback

Sicherheitsrisiko-Protokolle

Um dieses Fenster anzuzeigen, navigieren Sie zu **Protokolle** > **Agents** > **Sicherheitsrisiken**.

Sie können Protokolle im Fenster **Sicherheitsrisiko-Protokolle** anzeigen und verwalten.

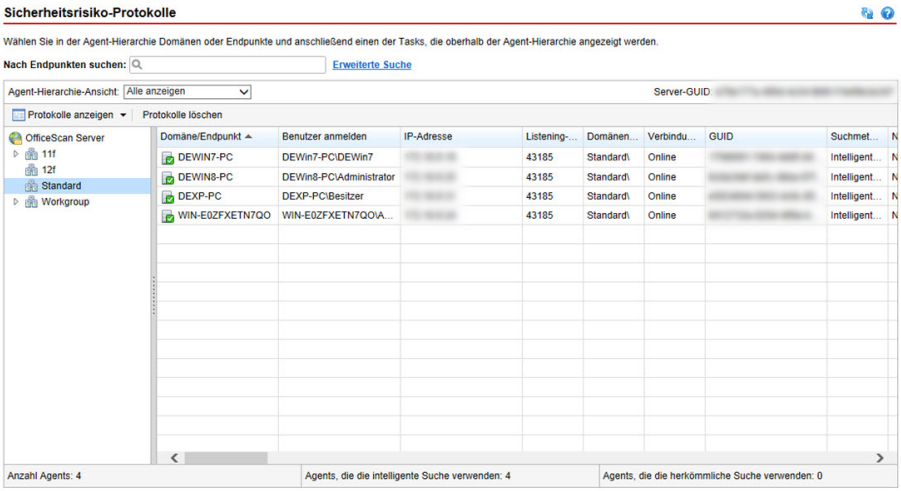


ABBILDUNG 2-9. Sicherheitsrisiko-Protokolle

Führen Sie folgende Aufgaben durch:

1. Protokolle anzeigen, die agents an den Server senden. Weitere Informationen finden Sie unter:

   - *Viren-/Malware-Protokolle anzeigen auf Seite 7-101*
   - *Spyware/Grayware-Protokolle anzeigen auf Seite 7-110*
   - *Firewall-Protokolle anzeigen auf Seite 13-33*
   - *Web-Reputation-Protokolle anzeigen auf Seite 12-23*
   - *Protokolle zu verdächtigen Verbindungen anzeigen auf Seite 8-17*
   - *Protokolle zu verdächtigen Dateien anzeigen auf Seite 7-115*
   - *C&C Callback-Protokolle anzeigen auf Seite 12-25*

- *Verhaltensüberwachungsprotokolle anzeigen auf Seite 9-25*
- *Anzeigen von Protokolldaten für "Vorausschauendes Maschinenlernen" auf Seite 8-13*
- *Protokolle der Gerätesteuerung anzeigen auf Seite 10-20*
- *Protokolle der Funktion "Prävention vor Datenverlust" anzeigen auf Seite 11-63*
- *Protokolle zu Suchvorgängen anzeigen auf Seite 7-116*

2. Protokolle löschen. Weitere Informationen finden Sie unter *Protokollmanagement auf Seite 14-47*.

OfficeScan Domänen

Eine Domäne in OfficeScan umfasst eine Gruppe von Agents mit derselben Konfiguration, die dieselben Aufgaben ausführen. Durch das Gruppieren von Agents in Domänen können Sie für alle Domänenmitglieder dieselbe Konfiguration festlegen, verwalten und übernehmen.

Weitere Informationen zur Agent-Gruppierung finden Sie unter *Agent-Gruppierung auf Seite 2-54*.

Agent-Gruppierung

Mit der Agent-Gruppierung können Sie manuell oder automatisch Domänen in der OfficeScan agent-Hierarchie erstellen oder verwalten.

Es gibt zwei Methoden, um agents in Domänen zu gruppieren.

TABELLE 2-11. Agent-Gruppierungsmethoden

METHODE	AGENT-GRUPPIERUNG	BESCHREIBUNGEN
Manuell	• NetBIOS-Domäne • Active Directory-Domäne • DNS-Domäne	Die manuelle agent-Gruppierung legt die Domäne fest, zu der ein kürzlich installierter agent gehören soll. Wenn der agent in der agent-Hierarchie angezeigt wird, können Sie ihn auf eine andere Domäne oder einen anderen OfficeScan Server verschieben. Die manuelle agent-Gruppierung ermöglicht es auch, Domänen in der agent-Hierarchie zu erstellen, zu verwalten und zu entfernen. Weitere Informationen finden Sie unter *Manuelle Agent-Gruppierung auf Seite 2-55*.
Automatisch	Benutzerdefinierte agent-Gruppen	Die automatische agent-Gruppierung wendet Regeln an, um agents in der agent-Hierarchie zu ordnen. Nachdem Sie diese Regeln festgelegt haben, können Sie auf die agent-Hierarchie zugreifen, um die agents manuell zu ordnen oder um zuzulassen, dass OfficeScan sie automatisch ordnet, wenn spezielle Ereignisse auftreten oder in regelmäßigen Zeitabständen. Weitere Informationen finden Sie unter *Automatische Agent-Gruppierung auf Seite 2-56*.

Manuelle Agent-Gruppierung

OfficeScan verwendet diese Einstellung nur während der agent-Erstinstallation. Das Installationsprogramm überprüft die Netzwerkdomäne, zu der der Ziel-Endpunkt gehört. Wenn der Domänenname bereits in der agent-Hierarchie vorhanden ist, gruppiert OfficeScan den agent auf dem Ziel-Endpunkt unter der entsprechenden Domäne und übernimmt die für die Domäne konfigurierten Einstellungen. Wenn der Domänenname nicht vorhanden ist, fügt OfficeScan die Domäne zur agent-Hierarchie hinzu, gruppiert den agent unter dieser Domäne und wendet dann die Stammeinstellungen auf die Domäne und den agent an.

Manuelle Agent-Gruppierungen konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Gruppierung**.
2. Sie können eine Methode zur Gruppierung von agents angeben:
   - NetBIOS-Domäne
   - Active Directory-Domäne
   - DNS-Domäne
3. Klicken Sie auf **Speichern**.

Nächste Maßnahme

Verwalten Sie Domänen und die agents, die unter ihnen gruppiert wurden, indem Sie folgende Aufgaben durchführen:

- Domäne hinzufügen
- Domäne oder agent löschen
- Domäne umbenennen
- agent in eine andere Domäne verschieben

Weitere Informationen finden Sie unter *Aufgaben zur Agent-Gruppierung auf Seite 2-61*.

Automatische Agent-Gruppierung

Die automatische agent-Gruppierung wendet Regeln an, die nach IP-Adressen oder Active Directory-Domänen festgelegt wurden. Wenn eine Regel eine IP-Adresse oder einen IP-Adressbereich festlegt, ordnet der OfficeScan Server agents mit einer passenden IP-Adresse einer bestimmten Domäne der agent-Hierarchie zu. Legt entsprechend eine Regel eine oder mehrere Active Directory-Domänen fest, ordnet der OfficeScan Server agents, die zu einer bestimmten Active Directory-Domäne gehören, einer bestimmten Domäne der agent-Hierarchie zu.

Agents können immer nur eine Regel auf einmal anwenden. Legen Sie Prioritäten fest, damit ein agent, der mehrere Regeln unterstützt, die Regel mit der höchsten Priorität anwendet.

Automatische Agent-Gruppierung konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Gruppierung**.
2. Navigieren Sie zum Abschnitt **Agent-Gruppierung** und wählen Sie **Benutzerdefinierte Agent-Gruppen für vorhandene OfficeScan Agents erstellen** aus.
3. Navigieren Sie zum Abschnitt **Automatische Agent-Gruppierung**.
4. Um Regeln zu erstellen, klicken Sie auf **Hinzufügen** und wählen Sie dann entweder **Active Directory** oder **IP-Adresse**.
   - Wenn Sie **Active Directory** ausgewählt haben, finden Sie die Konfigurationsanweisungen unter *Agent-Gruppierungsregeln nach Active Directory-Domänen festlegen auf Seite 2-58*.
   - Wenn Sie **IP-Adresse** ausgewählt haben, finden Sie die Konfigurationsanweisungen unter *Agent-Gruppierungsregeln nach IP-Adressen festlegen auf Seite 2-60*.
5. Wenn Sie mehr als eine Regel erstellt haben, legen Sie Prioritäten fest, indem Sie folgende Schritte ausführen:
   a. Wählen Sie eine Regel aus.
   b. Klicken Sie auf einen Pfeil unter der Spalte **Gruppenpriorität** und bewegen Sie die Regel in der Liste nach oben oder unten. Die ID-Nummer der Regel ändert sich entsprechend der neuen Position.
6. Die Regeln während der Agent-Zuordnung anwenden:
   a. Aktivieren Sie die Kontrollkästchen der Regeln, die Sie anwenden wollen.
   b. Aktivieren Sie die Regeln, indem Sie das Steuerelement **Status** auf **Ein** festlegen.

Hinweis

Wenn Sie keine Regel durch das Aktivieren von Kontrollkästchen auswählen, oder wenn Sie eine Regel deaktivieren, wird die Regel nicht angewendet, wenn die Agents in der Agent-Hierarchie geordnet werden. Wenn die Regel beispielsweise vorschreibt, dass ein Agent in eine neue Domäne verschoben werden soll, wird der Agent nicht verschoben und bleibt in seiner bisherigen Domäne.

7. Geben Sie im Abschnitt **Zeitgesteuerte Domänenerstellung** einen Sortierzeitplan ein.

   a. Wählen Sie **Zeitgesteuerte Domänenerstellung** aus.

   b. Geben Sie unter **Zeitgesteuerte Domänenerstellung** einen Zeitplan ein.

8. Wählen Sie dazu eine der folgenden Optionen aus:

   - **Jetzt speichern und Domäne erstellen**: Wählen Sie diese Option, wenn Sie in *Agent-Gruppierungsregeln nach IP-Adressen festlegen auf Seite 2-60*, Schritt 7, oder in *Agent-Gruppierungsregeln nach Active Directory-Domänen festlegen auf Seite 2-58*, Schritt 7, neue Domänen angegeben haben.

   - **Speichern**: Wählen Sie diese Option, wenn Sie keine neuen Domänen angegeben haben oder die neuen Domänen nur dann erstellen möchten, wenn die Agents sortiert werden.

Hinweis

Die Agents werden erst sortiert, nachdem dieser Schritt abgeschlossen wurde.

Agent-Gruppierungsregeln nach Active Directory-Domänen festlegen

Konfigurieren Sie die Integrationseinstellungen von Active Directory, bevor Sie die nachfolgenden Schritte ausführen. Weitere Informationen finden Sie unter *Active Directory-Integration auf Seite 2-36*.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Gruppierung**.
2. Navigieren Sie zum Abschnitt **Agent-Gruppierung** und wählen Sie **Benutzerdefinierte Agent-Gruppen für vorhandene OfficeScan Agents erstellen** aus.
3. Navigieren Sie zum Abschnitt **Automatische Agent-Gruppierung**.
4. Klicken Sie auf **Hinzufügen** und wählen Sie dann **Active Directory** aus.

   Ein neues Fenster wird angezeigt.
5. Wählen Sie **Gruppierung aktivieren** aus.
6. Geben Sie einen Namen für diese Regel an.
7. Wählen Sie unter **Active Directory Quelle** die Active Directory-Domäne(n) oder Subdomänen aus.
8. Wählen Sie unter **Agent-Hierarchie** eine bestehende OfficeScan Domäne aus, zu der die Active Directory-Domäne passt. Wenn die gewünschte OfficeScan Domäne nicht vorhanden ist, führen Sie folgende Schritte durch:
   a. Zeigen Sie mit dem Mauscursor auf eine bestimmte OfficeScan Domäne, und klicken Sie auf das Symbol zum Hinzufügen einer Domäne (➕).
   b. Geben Sie den Namen der Domäne in das entsprechende Textfeld ein.
   c. Klicken Sie auf das Häkchen neben dem Textfeld. Die neue Domäne wird hinzugefügt und automatisch ausgewählt.
9. Wahlweise aktivieren Sie **Active Directory-Struktur in der OfficeScan Agent-Hierarchie nachbilden**. Mit dieser Option bilden Sie die Hierarchie der ausgewählten Active Directory-Domäne auf der ausgewählten OfficeScan Domäne nach.
10. Klicken Sie auf **Speichern**.

Agent-Gruppierungsregeln nach IP-Adressen festlegen

Sie können benutzerdefinierte agent-Gruppen mit Netzwerk-IP-Adressen erstellen, um die agents in der OfficeScan agent-Hierarchie zu sortieren. Die Funktion kann Administratoren dabei unterstützen, die Struktur der OfficeScan-agent-Hierarchie anzuordnen, bevor der agent eine Registrierung am OfficeScan Server durchführt.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Gruppierung**.
2. Navigieren Sie zum Abschnitt **Agent-Gruppierung** und wählen Sie **Benutzerdefinierte Agent-Gruppen für vorhandene OfficeScan Agents erstellen** aus.
3. Navigieren Sie zum Abschnitt **Automatische Agent-Gruppierung**.
4. Klicken Sie auf **Hinzufügen** und wählen Sie dann **IP-Adresse**.

   Ein neues Fenster wird angezeigt.
5. Wählen Sie **Gruppierung aktivieren** aus.
6. Geben Sie einen Namen für die Gruppierung ein.
7. Geben Sie eines der folgenden Kriterien an:
   - Eine einzelne IPv4- oder IPv6-Adresse
   - Einen IPv4-Adressbereich
   - Ein IPv6-Präfix und die Länge

   Hinweis

   Wenn die IPv4- und IPv6-Adressen eines Dual-Stack-agents zu zwei verschiedenen agent-Gruppen gehören, wird der agent unter der IPv6-Gruppe eingeordnet. Wenn IPv6 auf dem Hostrechner des agents deaktiviert ist, wird der agent in die IPv4-Gruppe verschoben.
8. Wählen Sie die OfficeScan Domäne aus, der die IP-Adresse oder der IP-Adressbereich zugeordnet werden soll. Gehen Sie wie folgt vor, wenn die Domäne nicht vorhanden ist:

a. Zeigen Sie mit dem Mauscursor auf eine beliebige Stelle in der agent-Hierarchie und klicken Sie auf das Symbol zum Hinzufügen einer Domäne.

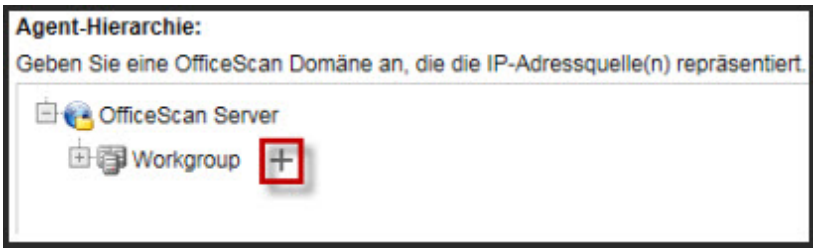


ABBILDUNG 2-10. Symbol "Domäne hinzufügen"

b. Tragen Sie die Domäne in das bereitgestellte Textfeld ein.

c. Klicken Sie auf das Häkchen neben dem Textfeld. Die neue Domäne wird hinzugefügt und automatisch ausgewählt.

9. Klicken Sie auf **Speichern**.

Aufgaben zur Agent-Gruppierung

Sie können die folgenden Aufgaben ausführen, wenn Sie agents in Domänen gruppieren:

- Domäne hinzufügen. Weitere Informationen finden Sie unter *Hinzufügen einer Domäne auf Seite 2-62*.
- Domäne oder agent löschen. Weitere Informationen finden Sie unter *Domäne oder Agent löschen auf Seite 2-62*.
- Domäne umbenennen. Weitere Informationen finden Sie unter *Umbenennen einer Domäne auf Seite 2-63*.
- Einen einzelnen agent in eine andere Domäne oder auf einen anderen OfficeScan Server verschieben. Weitere Informationen finden Sie unter *OfficeScan Agenten in eine andere Domäne oder auf einen anderen OfficeScan Server verschieben auf Seite 2-63*.

Hinzufügen einer Domäne

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie auf **Agent-Hierarchie verwalten** > **Domäne hinzufügen**.
3. Geben Sie einen Namen für die Domäne ein, die Sie hinzufügen möchten.
4. Klicken Sie auf **Hinzufügen**.

   Die neue Domäne wird nun in der Agent-Hierarchie angezeigt.
5. (Optional) Subdomänen erstellen.
   a. Wählen Sie die übergeordnete Domäne.
   b. Klicken Sie auf **Agent-Hierarchie verwalten** > **Domäne hinzufügen**.
   c. Geben Sie den Namen der Subdomäne ein.

Domäne oder Agent löschen

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Wählen Sie in der agent-Hierarchie:
   - Eine oder mehrere Domänen
   - Einen, mehrere oder alle agents, die zu einer Domäne gehören
3. Klicken Sie auf **Agent-Hierarchie verwalten** > **Domäne/Agent entfernen**.
4. Um eine leere Domäne zu löschen, klicken Sie auf **Domäne/Agent entfernen**. Wenn die Domäne agents enthält und Sie auf **Domäne/Agent entfernen** klicken, erstellt der OfficeScan Server diese Domäne erneut und gruppiert alle agents unter dieser Domäne, wenn sich agents das nächste Mal mit dem OfficeScan Server verbinden. Sie können folgende Aufgaben ausführen, bevor Sie die Domäne löschen:

a. Verschieben Sie die agents in andere Domänen. Um agents in andere Domänen zu verschieben, verschieben Sie die agents per Drag und Drop in die entsprechenden Zieldomänen.

b. Löschen Sie alle agents.

5. Um einen einzelnen agent zu löschen, klicken Sie auf **Domäne/Agent entfernen**.

Hinweis

Wenn Sie den agent aus der agent-Hierarchie löschen, wird der OfficeScan Agent nicht vom agent-Endpunkt entfernt. Der OfficeScan Agent kann noch immer serverunabhängige Funktionen durchführen, wie z. B. das Update der Komponenten. Der Server weiß jedoch nicht, dass der agent vorhanden ist, und wird deshalb auf dem agent weder Einstellungen verteilen noch ihm Benachrichtigungen senden.

Umbenennen einer Domäne

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Wählen Sie eine Domäne aus der agent-Hierarchie aus.
3. Klicken Sie auf **Agent-Hierarchie verwalten** > **Domäne umbenennen**.
4. Geben Sie einen neuen Namen für die Domäne ein.
5. Klicken Sie auf **Umbenennen**.

   Der neue Domänenname wird nun in der agent-Hierarchie angezeigt.

OfficeScan Agenten in eine andere Domäne oder auf einen anderen OfficeScan Server verschieben

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.

2. Wählen Sie in der Agent-Hierarchie einen, mehrere oder alle Agents aus.
3. Klicken Sie auf **Agent-Hierarchie verwalten** > **Agent verschieben**.
4. So verschieben Sie Agents in eine andere Domäne:
   - Wählen Sie **Ausgewählte(n) Agent(s) in andere Domäne verschieben** aus.
   - Wählen Sie eine Domäne aus.
   - (Optional) Übernehmen Sie die Einstellungen der neuen Domäne für die Agents.

Tipp

Sie können Agents auch per Drag & Drop in eine andere Domäne in der Agent-Hierarchie verschieben.

5. So verschieben Sie Agents auf einen anderen OfficeScan Server:
   - Wählen Sie **Ausgewählte(n) Agent(s) auf einen anderen OfficeScan Server verschieben** aus.
   - Geben Sie den Servernamen oder die IPv4/IPv6-Adressen und die HTTP- oder SSL-Portnummer (443) ein.

Hinweis

Wenn Sie OfficeScan Agents in eine OfficeScan Cloud-Konsole verschieben, können Sie die OfficeScan Cloud-Konsolenserverinformationen über die Control Manager-Konsole abrufen. Navigieren Sie zu **Administration** > **Verwaltete Server** und wählen Sie im Listenfeld **Servervariante** den Eintrag **OfficeScan** aus.

6. Klicken Sie auf **Verschieben**.

Kapitel 3

Erste Schritte mit Datenschutz

In diesem Kapitel wird erläutert, wie Sie das Datenschutzmodul installieren und aktivieren.

Es werden folgende Themen behandelt:

- *Datenschutzinstallation auf Seite 3-2*
- *Datenschutzlizenz auf Seite 3-4*
- *Datenschutz auf OfficeScan Agenten verteilen auf Seite 3-6*
- *Ordner der forensischen Daten und DLP-Datenbank auf Seite 3-9*
- *Den Datenschutz deinstallieren auf Seite 3-15*

Datenschutzinstallation

Das Datenschutzmodul verfügt über folgende Funktionen:

- **Funktion "Prävention vor Datenverlust" (DLP)**: Verhindert die unerlaubte Übertragung digitaler Assets
- **Gerätesteuerung**: Reguliert den Zugriff auf externe Geräte

Hinweis

OfficeScan verfügt standardmäßig über eine Gerätesteuerungsfunktion, die den Zugriff auf häufig verwendete Geräte, wie etwa USB-Speicher, steuert. Die Gerätesteuerung erweitert als Teil des Datenschutzmoduls den Bereich der überwachten Geräte. Eine Liste aller überwachten Geräte finden Sie unter *Gerätesteuerung auf Seite 10-2*.

Die Funktion "Prävention vor Datenverlust" und die Gerätesteuerung sind native OfficeScan Funktionen, die aber separat lizenziert werden. Nach der Installation des OfficeScan Servers sind diese Funktionen zwar vorhanden, aber sie sind nicht funktionsfähig und können nicht auf die agents verteilt werden. Zur Installation des Datenschutzes muss eine Datei vom ActiveUpdate Server oder, falls vorhanden, von einer benutzerdefinierten Update-Adresse heruntergeladen werden. Sobald diese Datei in den OfficeScan Server integriert ist, können Sie die Datenschutzlizenz aktivieren, um alle Funktionen zu nutzen. Installation und Aktivierung werden vom **Plug-in Manager** durchgeführt.

Wichtig

Das Datenschutzmodul muss nicht installiert werden, wenn die Software "Trend Micro Prävention vor Datenverlust" bereits installiert ist und auf den Endpunkten ausgeführt wird.

Datenschutz installieren

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.

2. Navigieren Sie im Fenster **Plug-in Manager** zum Abschnitt **OfficeScan Datenschutz**, und klicken Sie auf **Herunterladen**.

   Die Größe der Download-Datei wird neben der Schaltfläche **Download** angezeigt.

   Der Plug-in Manager speichert die heruntergeladene Datei unter <*Installationsordner des Servers*>\PCCSRV\Download\Product.

   Hinweis

   Wenn der Plug-in Manager die Datei nicht herunterladen kann, wiederholt er den Versuch automatisch nach 24 Stunden. Um den Download manuell zu starten, muss der OfficeScan Plug-in Manager Dienst über die Microsoft Management Console neu gestartet werden.

3. Verfolgen Sie den Download-Fortschritt.

   Sie können während des Downloads zu anderen Fenstern navigieren.

   Treten beim Download der Datei Probleme auf, überprüfen Sie die Server-Update-Protokolle auf der OfficeScan Webkonsole. Klicken Sie im Hauptmenü auf **Protokolle** > **Server-Update**.

   Nachdem der Plug-in Manager die Datei heruntergeladen hat, wird der OfficeScan Datenschutz in einem neuen Fenster angezeigt.

   Hinweis

   Wenn OfficeScan Datenschutz nicht angezeigt wird, finden Sie unter *Fehlersuche in Plug-in Manager auf Seite 17-13* mögliche Ursachen und Lösungen.

4. Um OfficeScan Datenschutz sofort zu installieren, klicken Sie auf **Jetzt installieren**, oder führen Sie Folgendes aus, um die Installation zu einem späteren Zeitpunkt durchzuführen:

   a. Klicken Sie auf **Später installieren**.

   b. Öffnen Sie das Fenster **Plug-in Manager**.

   c. Gehen Sie zum Abschnitt **OfficeScan Datenschutz** , und klicken Sie auf **Installieren**.

5. Lesen Sie die Lizenzvereinbarung und akzeptieren Sie die Bedingungen, indem Sie auf **Stimme zu** klicken.

   Die Installation wird gestartet.

6. Überwachen Sie den Installationsfortschritt. Nach der Installation wird die Version des OfficeScan Datenschutzes angezeigt.

Datenschutzlizenz

Verwenden Sie Plug-in-Manager, um die Datenschutzlizenz anzuzeigen, zu aktivieren und zu verlängern.

Fordern Sie von Trend Micro einen Aktivierungscode an, um damit die Lizenz zu aktivieren.

Plug-in-Programme Lizenz aktivieren

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
2. Navigieren Sie im Fenster **Plug-in Manager** zum Abschnitt für Plug-in-Programme und klicken Sie auf **Programm verwalten**.

   Das Fenster **Produktlizenz – Neuer Aktivierungscode** wird angezeigt.
3. Geben Sie den Aktivierungscode in die Textfelder ein, oder kopieren Sie den Aktivierungscode und fügen ihn in die Textfelder ein.
4. Klicken Sie auf **Speichern**.

   Die Plug-in-Konsole wird angezeigt.

Lizenzdaten anzeigen und Lizenzen verlängern

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
2. Navigieren Sie im Fenster **Plug-in Manager** zum Abschnitt für Plug-in-Programme und klicken Sie auf **Programm verwalten**.
3. Klicken Sie auf **Lizenzdaten anzeigen**, um Informationen zur aktuellen Lizenz auf der Trend Micro-Website anzuzeigen.
4. Ein Fenster mit den folgenden Informationen zur Lizenz wird geöffnet.

Option	Bezeichnung
Status	Wird entweder als "Aktiviert", "Nicht aktiviert" oder "Abgelaufen" angezeigt
Version	Wird entweder als "Vollversion" oder "Testversion" angezeigt **Hinweis** Die Aktivierung sowohl der Vollversion als auch der Testversion wird als "Vollversion" angezeigt.
Arbeitsplätze	Zeigt an, wie viele Endpunkte vom Plug-in-Programm verwaltet werden können.
Lizenz läuft ab am	Wenn es für das Plug-in-Programm mehrere Lizenzen gibt, wird das am weitesten in der Zukunft liegende Ablaufdatum angezeigt. Laufen die Lizenzen beispielsweise am 31.12.2011 und am 30.06.2011 ab, wird das Datum 31.12.2011 angezeigt.
Aktivierungscode	Zeigt den Aktivierungscode an
Erinnerungen	In Abhängigkeit von der aktuellen Lizenzversion zeigt das Plug-in Erinnerungen zum Datum des Lizenzablaufs an, entweder während der Übergangsfrist (nur Vollversionen) oder wenn die Lizenz abläuft.

Hinweis

Die Dauer der Übergangsfrist ist regional verschieden. Überprüfen Sie die Übergangsfrist eines Plug-in-Programms mit einem Trend Micro Vertriebspartner.

5. Um die aktuellsten Lizenzdaten anzuzeigen, klicken Sie auf **Informationen aktualisieren**.

6. Klicken Sie auf **Neuer Aktivierungscode**, um das Fenster **Produktlizenz – Neuer Aktivierungscode** zu öffnen.

   Weitere Informationen finden Sie unter *Plug-in-Programme Lizenz aktivieren auf Seite 3-4*.

Datenschutz auf OfficeScan Agenten verteilen

Aktivieren Sie die Lizenz für das Datenschutzmodul und verteilen Sie es dann auf die OfficeScan Agents. Nach der Verteilung verwenden die OfficeScan Agents dann die Funktion "Prävention vor Datenverlust" und die Gerätesteuerung.

Wichtig

- Das Modul ist auf Windows Server 2003, Windows Server 2008 und Windows Server 2012 standardmäßig deaktiviert, um Leistungseinbußen auf dem Host-Computer zu vermeiden. Wenn Sie das Modul aktivieren möchten, überwachen Sie ständig die Systemleistung, und führen Sie die notwendigen Aktionen durch, wenn Sie einen Leistungsabfall bemerken.

  Sie können das Modul über die Webkonsole aktivieren oder deaktivieren. Weitere Informationen finden Sie unter *OfficeScan Agent Dienste auf Seite 15-7*.

- Wenn die Software 'Trend Micro Prävention vor Datenverlust' bereits auf dem Endpunkt installiert ist, ersetzt OfficeScan die Software nicht durch das Datenschutzmodul.

- Auf Online-Agents wird das Datenschutzmodul sofort installiert. Offline- und unabhängige Agents installieren das Modul nach der erneuten Verbindungsherstellung mit dem OfficeScan Server.

- Benutzer müssen den Computer neu starten, um die Installation der Treiber der Funktion "Prävention vor Datenverlust" abzuschließen. Informieren Sie die Benutzer rechtzeitig über den Neustart.

- Trend Micro empfiehlt die Aktivierung des Debug-Protokolls, um Probleme bei der Verteilung leichter beheben zu können. Weitere Informationen finden Sie unter *Debug-Protokollierung für das Datenschutzmodul aktivieren auf Seite 11-69*.

Das Datenschutzmodul an OfficeScan Agenten verteilen

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. In der Agent-Hierarchie können Sie:

   - Auf das Root-Domänen-Symbol ( ) klicken, um das Modul auf alle bestehenden und künftigen Agents zu verteilen.
   - Eine bestimmte Domäne auswählen, um das Modul auf alle bestehenden und künftigen Agents in dieser Domäne zu verteilen.
   - Einen bestimmten Agent auswählen, damit das Modul nur auf diesen Agent verteilt wird.

3. Verteilen Sie das Modul auf zwei unterschiedliche Arten:

   - Klicken Sie auf **Einstellungen** > **DLP-Einstellungen**.
   - Klicken Sie auf **Einstellungen** > **Einstellungen der Gerätesteuerung**.

   Hinweis

   Wenn Sie die Verteilung mit Hilfe von **Einstellungen** > **DLP-Einstellungen** vornehmen und das Datenschutzmodul erfolgreich verteilt wurde, werden die Treiber der Funktion "Prävention vor Datenverlust" installiert. Wenn die Treiber erfolgreich installiert wurden, wird eine Meldung angezeigt, in der die Benutzer zum Neustarten der Endpunkte aufgefordert werden, um die Treiberinstallation fertig zu stellen.

   Falls die Meldung nicht angezeigt wird, treten möglicherweise Probleme beim Installieren der Treiber auf. Wenn Sie das Debug-Protokoll aktiviert haben, überprüfen Sie die Protokolle, um Informationen über Probleme bei der Installation der Treiber zu erhalten.

4. Eine Nachricht zeigt an, auf wie vielen Agents das Modul nicht installiert wurde. Klicken Sie auf **Ja**, um die Verteilung zu starten.

   Hinweis

   Wenn Sie auf **Nein** klicken (oder wenn das Modul aus irgendeinem Grund auf einen oder mehrere Agents nicht verteilt wurde), wird die gleiche Nachricht angezeigt, wenn Sie wieder auf **Einstellungen** > **DLP-Einstellungen** oder **Einstellungen** > **Einstellungen der Gerätesteuerung** klicken.

   Die OfficeScan Agents beginnen mit dem Download des Moduls vom Server.

5. Überprüfen Sie, ob das Modul auf die Agents verteilt wurde.

   a. Wählen Sie in der Agent-Hierarchie eine Domäne aus.

   b. Wählen Sie in der Ansicht der Agent-Hierarchie **Datenschutzansicht** oder **Alle anzeigen**.

   c. Überprüfen Sie die Spalte **Datenschutzstatus**. Folgende Verteilungszustände sind möglich:

- **Wird ausgeführt**: Das Modul wurde erfolgreich verteilt und seine Funktionen aktiviert.
- **Neustart erforderlich**: Die Treiber der Funktion "Prävention vor Datenverlust" wurden nicht installiert, weil die Benutzer ihre Computer nicht neu gestartet haben. Wenn die Treiber nicht installiert sind, ist die Funktion "Prävention vor Datenverlust" nicht funktionsfähig.
- **Beendet**: Der Dienst für das Modul wurde nicht gestartet, oder der Zielendpunkt wurde nicht normal heruntergefahren. Navigieren Sie zum Starten des Datenschutzdiensts zu **Agents** > **Agent-Verwaltung** > **Einstellungen** > **Zusätzliche Diensteinstellungen** und aktivieren Sie die Datenschutzdienste.
- **Installation nicht möglich**: Bei der Verteilung des Moduls auf den Agent ist ein Problem aufgetreten. Das Modul muss über die Agent-Hierarchie neu verteilt werden.
- **Installation nicht möglich (die Funktion "Prävention vor Datenverlust" ist bereits vorhanden)**: Die Software "Trend Micro Prävention vor Datenverlust" ist bereits auf dem Endpunkt installiert. OfficeScan ersetzt die Software nicht durch das Datenschutzmodul.
- **Nicht installiert**: Das Modul wurde nicht auf den Agent verteilt. Dieser Status wird angezeigt, wenn Sie das Modul nicht auf dem Agent bereitgestellt haben oder wenn sich der Agent während der Bereitstellung im Offline- oder unabhängigen Status befindet.

Ordner der forensischen Daten und DLP-Datenbank

Nach Auftritt eines Datenverlustpräventionsvorfalls protokolliert OfficeScan dessen Details in einer speziellen forensischen Datenbank. OfficeScan erstellt darüber hinaus eine verschlüsselte Datei mit einer Kopie der sensiblen Daten, die den Vorfall ausgelöst haben, und generiert einen Hashwert zur Überprüfung und zur Wahrung der Integrität der sensiblen Daten. OfficeScan erstellt die verschlüsselten forensischen Dateien auf

demagent-Computer und lädt die Dateien dann auf einen angegebenen Speicherort auf dem Server hoch.

Wichtig

- Da diese höchst sensible Daten enthalten, sollten Administratoren beim Zuweisen der Zugriffsberechtigungen sehr vorsichtig vorgehen.
- OfficeScan wird in Control Manager integriert und bietet Benutzern von Control Manager mit entsprechenden Rollen für die DLP-Vorfallsprüfung und die DLP-Compliance die Möglichkeit, auf die Daten in den verschlüsselten Dateien zuzugreifen. Einzelheiten zu den DLP-Rollen und dem Zugriff auf die forensischen Dateien in Control Manager finden Sie im *Administratorhandbuch für Control Manager 6.0 SP3 Patch 2* oder höher.

Einstellungen für Ordner der forensischen Daten und forensische Datenbank ändern

Administratoren können den Speicherort und den Löschzeitplan des Ordners der forensischen Daten sowie die maximale Größe der von agentss hochgeladenen Dateien ändern. Dies erfolgt in den INI-Dateien von OfficeScan.

Warnung!

Wenn der Speicherort des Ordners der forensischen Daten nach der Protokollierung von Datenverlustpräventions-Vorfällen geändert wird, kann dies zu einer Unterbrechung der Verbindung zwischen den Daten in der Datenbank und dem Speicherort der bestehenden forensischen Daten führen. Trend Micro empfiehlt daher nach einer Änderung des Speicherorts des Ordners der forensischen Daten eine manuelle Migration bestehender forensischer Daten in den neuen Ordner.

Die folgende Tabelle zeigt die Servereinstellungen, die in der INI-Datei unter <*Installationsordner des Servers*>`\PCCSRV\Private\ofcserver.ini` auf dem OfficeScan Server enthalten sind.

TABELLE 3-1. Servereinstellungen für Ordner der forensischen Daten in PCCSRV \Private\ofcserver.ini

ZWECK	INI-EINSTELLUNG	WERTE
Benutzerdefinierten Speicherort für Ordner der forensischen Daten zulassen	[INI_IDLP_SECTION] `EnableUserDefinedUploadFolder`	0: Deaktiviert (Standardeinstellung) 1: Aktivieren
Benutzerdefinierten Speicherort für Ordner der forensischen Daten konfigurieren	[INI_IDLP_SECTION] `UserDefinedUploadFolder` **Hinweis** • Die Einstellung `EnableUserDefinedUploadFolder` muss aktiviert sein, damit diese Einstellung wirksam werden kann. • Der Standardspeicherort des Ordners der forensischen Daten ist: <*Installationsordner des Servers*>`\PCCSRV\Private\DLPForensicData` • Der benutzerdefinierte Ordnerspeicherort muss auf einem physischen Laufwerk (intern oder extern) auf dem Server-Computer liegen. OfficeScan unterstützt die Zuordnung von Netzlaufwerken nicht.	Standardwert: <Ersetzen Sie diesen Wert durch den benutzerdefinierten Ordnerpfad. Beispiel: C:\VolumeData\OfficeScanDlpForensicData> Benutzerdefinierter Wert: Muss ein physischer Speicherort auf einem Laufwerk des Server-Computers sein.
Bereinigen forensischer Datendateien zulassen	[INI_IDLP_SECTION] `ForensicDataPurgeEnable`	0: Deaktiviert 1: Aktiviert (Standardeinstellung)

ZWECK	INI-EINSTELLUNG	WERTE
Zeitintervall der Bereinigungsprüfung für forensische Datendateien konfigurieren	[INI_IDLP_SECTION] `ForensicDataPurgeCheckFrequency` **Hinweis** • Die Einstellung `ForensicDataPurgeEnable` muss aktiviert sein, damit diese Einstellung in OfficeScan wirksam werden kann. • OfficeScan löscht nur Datendateien, die das in der Einstellung `ForensicDataExpiredPeriodInDays` festgelegte Ablaufdatum erreicht haben.	1: Monatlich, am ersten Tag des Monats um 00:00 2: Wöchentlich (Standardeinstellung), sonntags um 00:00 3: Täglich, jeden Tag um 00:00 4: Stündlich, jede Stunde um HH:00
Dauer der Speicherung forensischer Datendateien auf dem Server	[INI_IDLP_SECTION] `ForensicDataExpiredPeriodInDays`	Standardwert (in Tagen): 180 Mindestwert: 1 Höchstwert: 3650
Zeitintervall der Speicherplatzprüfung für forensische Datendateien konfigurieren	[INI_SERVER_DISK_THRESHOLD] `MonitorFrequencyInSecond` **Hinweis** Wenn der verfügbare Festplattenspeicher im Ordner der forensischen Daten unter den in der Einstellung `InformUploadOnDiskFreeSpaceInGb` festgelegten Wert fällt, protokolliert OfficeScan ein Ereignis in der Webkonsole.	Standardwert (in Sekunden): 5

ZWECK	INI-EINSTELLUNG	WERTE
Uploadfrequenz der Speicherplatzprüfung für forensische Datendateien konfigurieren	[INI_SERVER_DISK_THRESHOLD] `IsapiCheckCountInRequest` **Hinweis** Wenn der verfügbare Festplattenspeicher im Ordner der forensischen Daten unter den in der Einstellung `InformUploadOnDiskFreeSpaceInGb` festgelegten Wert fällt, protokolliert OfficeScan ein Ereignis in der Webkonsole.	Standardwert (in Anzahl von Dateien): 200
Mindestspeicherplatz konfigurieren, bei dem eine Benachrichtigung über beschränkten Festplattenspeicher ausgelöst wird	[INI_SERVER_DISK_THRESHOLD] `InformUploadOnDiskFreeSpaceInGb` **Hinweis** Wenn der verfügbare Festplattenspeicher im Ordner der forensischen Daten unter diesen Wert fällt, protokolliert OfficeScan ein Ereignis in der Webkonsole.	Standardwert (in GB): 10
Verfügbaren Mindestspeicherplatz zum Hochladen forensischer Datendateien aus agents konfigurieren	[INI_SERVER_DISK_THRESHOLD] `RejectUploadOnDiskFreeSpaceInGb` **Hinweis** Wenn der verfügbare Festplattenspeicher im Ordner der forensischen Daten unter diesen Wert fällt, laden die OfficeScan-agents keine forensischen Datendateien hoch und OfficeScan protokolliert ein Ereignis in der Webkonsole.	Standardwert (in GB): 1

Die folgende Tabelle zeigt die OfficeScan Agent-Einstellungen, die in der INI-Datei unter <*Installationsordner des Servers*>`\PCCSRV\ofcscan.ini` auf dem OfficeScan Server enthalten sind.

TABELLE 3-2. Agent-Einstellungen für forensische Dateien in `PCCSRV\ofcscan.ini`

ZWECK	INI-EINSTELLUNG	WERTE
Hochladen von forensischen Datendateien auf den Server zulassen	`UploadForensicDataEnable`	0: Disable 1: Enable (default)
Maximale Größe der vom OfficeScan Agent auf den Server hochgeladenen Dateien konfigurieren	`UploadForensicDataSizeLimitInMb` **Hinweis** Der OfficeScan Agent sendet nur Dateien an den Server, die kleiner sind als der hier angegebene Wert.	Standardwert (in MB): 10 Mindestwert: 1 Höchstwert: 2048
Dauer der Speicherung forensischer Datendateien auf dem OfficeScan Agent	`ForensicDataKeepDays` **Hinweis** Jeden Tag um 11:00 Uhr löscht der OfficeScan Agent die forensischen Datendateien, die das festgelegte Ablaufdatum erreicht haben.	Standardwert (in Tagen): 180 Mindestwert: 1 Höchstwert: 3650
Zeitintervall der Serververbindungsprüfung durch den OfficeScan Agent konfigurieren	`ForensicDataDelayUploadFrequenceInMinutes` **Hinweis** Wenn OfficeScan Agents die forensischen Dateien nicht automatisch auf den Server hochladen konnten, versuchen sie, die Dateien anhand dieses Intervalls erneut zu senden.	Standardwert (in Minuten): 5 Mindestwert: 5 Höchstwert: 60

Sicherungskopie forensischer Daten erstellen

Abhängig von der jeweiligen Sicherheitspolitik eines Unternehmens kann der zur Speicherung der forensischen Daten erforderliche Zeitaufwand sehr unterschiedlich ausfallen. Um Festplattenspeicher auf dem Server freizugeben, empfiehlt Trend Micro die manuelle Sicherung des Ordners der forensischen Daten und der forensischen Datenbank.

Prozedur

1. Navigieren Sie auf dem Server zum Speicherort des Ordners der forensischen Daten.
   - Standardspeicherort: <*Installationsordner des Servers*>`\PCCSRV\Private\DLPForensicData`
   - Hinweise zum Auffinden des Ordners der forensischen Daten bei benutzerdefinierter Änderung finden Sie unter *Benutzerdefinierten Speicherort für Ordner der forensischen Daten konfigurieren auf Seite 3-11*.
2. Verschieben Sie den Ordner an einen neuen Speicherort.
3. Um die forensische Datenbank manuell zu sichern, gehen Sie zu <*Installationsordner des Servers*>`\PCCSRV\Private`.
4. Verschieben Sie die Datei `DLPForensicDataTracker.db` an einen neuen Speicherort.

Den Datenschutz deinstallieren

Folgendes ist bei der Deinstallation des Datenschutzmoduls über den Plug-in Manager zu beachten:

- Alle Konfigurationen, Einstellungen und Protokolle der Funktion "Prävention vor Datenverlust" werden vom OfficeScan Server entfernt.
- Alle Konfigurationen und Einstellungen der Gerätesteuerung aus dem Datenschutzmodul werden auf dem Server entfernt.

- Das Datenschutzmodul auf den agents wird entfernt. Agent Endpunkte müssen neu gestartet werden, um den Datenschutz vollständig zu entfernen.
- Die Richtlinien der Funktion "Prävention vor Datenverlust" werden auf den agents nicht mehr durchgesetzt.
- Die Gerätesteuerung überwacht nicht mehr den Zugriff auf folgende Geräte:
  - Bluetooth-Adapter
  - COM- und LPT-Anschlüsse
  - IEEE 1394-Schnittstelle
  - Bildverarbeitungsgeräte
  - Infrarotgeräte
  - Modems
  - PCMCIA-Karte
  - Druck-Taste
  - Wireless-NICs

Sie können das Datenschutzmodul jederzeit neu installieren. Nach der erneuten Installation aktivieren Sie die Lizenz unter Verwendung eines gültigen Aktivierungscodes.

Den Datenschutz über den Plug-in Manager deinstallieren

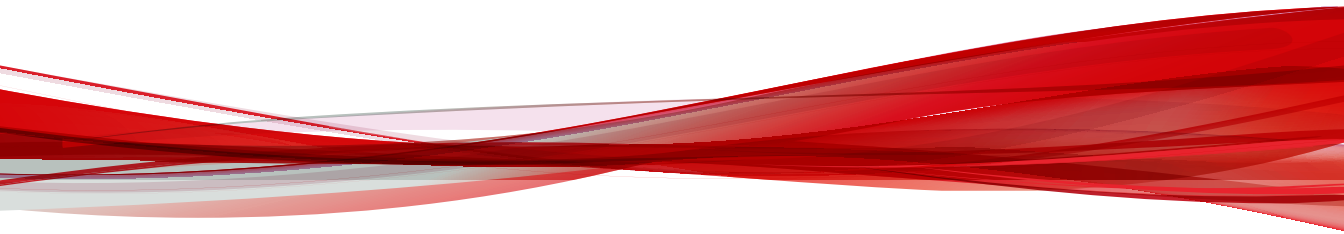
Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
2. Navigieren Sie im Fenster **Plug-in Manager** zum Abschnitt **OfficeScan Datenschutz**, und klicken Sie auf **Deinstallieren**.
3. Verfolgen Sie den Deinstallationsfortschritt. Sie können während der Deinstallation zu anderen Fenstern navigieren.

4. Aktualisieren Sie das Fenster **Plug-in Manager** nach der Deinstallation. Der OfficeScan Datenschutz steht wieder zur Installation bereit.

Teil II

Schützen OfficeScan Agenten



Kapitel 4

Trend Micro Smart Protection verwenden

In diesem Kapitel werden die Trend Micro Smart Protection Lösungen beschrieben. Außerdem wird erläutert, wie Sie die zur Verwendung der Lösungen erforderliche Umgebung einrichten.

Es werden folgende Themen behandelt:

- *Info über Trend Micro Smart Protection auf Seite 4-2*
- *Smart Protection Dienste auf Seite 4-3*
- *Smart Protection Quellen auf Seite 4-6*
- *Pattern-Dateien von Smart Protection auf Seite 4-8*
- *Smart Protection Services einrichten auf Seite 4-13*
- *Smart Protection Services verwenden auf Seite 4-33*

Info über Trend Micro Smart Protection

Trend Micro™ Smart Protection ist eine Content-Sicherheitsinfrastruktur mit Cloud-Client der nächsten Generation, die zum Schutz der Kunden vor Sicherheitsrisiken und Internetbedrohungen dient. Sie umfasst sowohl lokale als auch gehostete Lösungen und bietet umfassenden Schutz im Netzwerk, zu Hause oder unterwegs. Über schlanke agents erhalten die Benutzer Zugriff zu einer einzigartigen Kombination aus E-Mail-, Web- und File-Reputationstechnologien sowie Bedrohungsdatenbanken in der Cloud. Der Schutz der Kunden wird automatisch aktualisiert und weiter gestärkt, indem weitere Produkte, Services und Benutzer auf dieses Netzwerk zugreifen. Dadurch entsteht für die beteiligten Benutzer eine Art "Nachbarschaftsschutz" in Echtzeit.

Durch die Integration von webbasierten Reputationstechniken, Suchvorgängen und Korrelationstechnologien reduzieren die Trend Micro Smart Protection Lösungen die Abhängigkeit von konventionellen Pattern-Datei-Downloads. Die Verzögerungen werden beseitigt, die allgemein mit Desktop-Aktualisierungen in Verbindung gebracht werden.

Die Notwendigkeit einer neuen Lösung

Bei der aktuellen Vorgehensweise gegen dateibasierte Bedrohungen werden die zum Schutz von Endpunkten erforderlichen Pattern (auch "Definitionen" genannt) zeitgesteuert an die Endpunkte ausgeliefert. Pattern werden von Trend Micro in Paketen an die agents übertragen. Nachdem ein neues Update eingegangen ist, lädt die Viren-/Malware-Schutz-Software auf dem agent dieses Definitionspaket für neue Viren/Malware in den Arbeitsspeicher. Wenn ein neues Risiko durch neue Viren/Malware entsteht, muss dieses Pattern auf dem agent erneut vollständig oder teilweise aktualisiert und in den Arbeitsspeicher geladen werden, damit der Schutz aufrechterhalten wird.

Mit der Zeit nimmt der Umfang neu aufkommender Bedrohungen erheblich zu. Man schätzt, dass die Zahl der Bedrohungen in den nächsten Jahren fast exponentiell zunimmt. Dies führt zu einer Wachstumsrate, die die Anzahl der derzeit bekannten Bedrohungen um ein Vielfaches übersteigt. In Zukunft ist allein die immense Anzahl von Sicherheitsrisiken eine neue Art von Sicherheitsrisiko. Die Anzahl von Sicherheitsrisiken kann die Leistung von Servern und Workstations sowie die Netzwerkbandbreite beeinträchtigen. Auch die Dauer bis zur Bereitstellung eines wirksamen Schutzes - auch "Zeit bis zum Schutz" genannt - wird sich verlängern.

Trend Micro ist Vorreiter bei einem neuen Ansatz zur Bewältigung einer hohen Anzahl von Bedrohungen, durch den Trend Micro Kunden immun gegen die starke Zunahme von Viren/Malware werden. Hierzu wird eine Technologie genutzt, bei der Viren-/Malware-Signaturen und -Pattern in die "Cloud", also das Internet, ausgelagert werden. Durch das Auslagern der Viren-/Malware-Signaturen in das Internet ist Trend Micro in der Lage, seine Kunden besser vor den neuen Risiken auf Grund der zukünftigen Anzahl von Bedrohungen zu schützen.

Smart Protection Dienste

Die Smart Protection Services stellen Anti-Malware-Signaturen, Web-Reputation-Daten und Bedrohungsdatenbanken bereit, die im Internet gespeichert sind.

Smart Protection Services beinhaltet:

- **File-Reputation-Dienste**: File-Reputation-Dienste lagern eine Vielzahl von zuvor auf den agent-Computern gespeicherten Anti-Malware-Signaturen auf Smart Protection Quellen aus.

  Weitere Informationen finden Sie unter *File-Reputation-Dienste auf Seite 4-3*.

- **Web-Reputation-Dienste**: Web-Reputation-Dienste ermöglicht es lokalen Smart Protection Quellen, Daten über die Zuverlässigkeit von URLs zu hosten, die früher ausschließlich von Trend Micro gehostet wurden. Beide Technologien beanspruchen weniger Bandbreite, wenn Pattern aktualisiert oder die Gültigkeit einer URL überprüft wird.

  Weitere Informationen finden Sie unter *Web-Reputation-Dienste auf Seite 4-4*.

- **Smart Feedback**: Trend Micro sammelt weiterhin anonym Informationen, die weltweit von Trend Micro Produkten gesendet werden, um jede neue Bedrohung proaktiv zu ermitteln.

  Weitere Informationen finden Sie unter *Smart Feedback auf Seite 4-5*.

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 Cloud-agent-Architektur bietet sofortigen Schutz und verringert den Aufwand der Pattern-Verteilung und die agent-Beeinträchtigung insgesamt erheblich.

Agents müssen sich im intelligenten Suchmodus befinden, damit File-Reputation-Dienste angewendet werden kann. Diese agents werden in diesem Dokument als Smart Scan agents bezeichnet. Agents, die sich nicht im intelligenten Suchmodus befinden, wenden File-Reputation-Dienste nicht an und heißen agents der herkömmlichen Suche. OfficeScan Administratoren können den intelligenten Suchmodus auf allen oder mehreren 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.

OfficeScan Agents, die den Web-Reputation-Richtlinien unterliegen, benutzen Web-Reputation-Dienste. OfficeScan Administratoren können alle oder mehrere agents den Web-Reputation-Richtlinien unterstellen.

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.

Tipp

Sie müssen nicht an Smart Feedback teilnehmen, um Ihre Endpunkte 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/

Smart Protection Quellen

Trend Micro stellt für OfficeScan und Smart Protection Quellen File-Reputation-Dienste und Web-Reputation-Dienste bereit.

Smart Protection Quellen liefern File-Reputation-Dienste durch das Hosten der meisten Viren-/Malware-Patterndefinitionen. OfficeScan Agents hosten alle übrigen Definitionen. Ein agent sendet Suchabfragen an Smart Protection Quellen, wenn seine eigenen Pattern-Definitionen das Risiko der Datei nicht ermitteln können. Die Smart Protection Quellen ermitteln das Risiko mit Hilfe von Identifikationsdaten.

Die Smart Protection Quellen liefern Web-Reputation-Dienste durch das Hosten von Web-Reputation-Daten, die vorher ausschließlich von den von Trend Micro gehosteten Servern zur Verfügung gestellt wurden. Der agent sendet Web-Reputation-Abfragen an die Smart Protection Quellen, um die Zuverlässigkeit von Websites, auf die ein Benutzer zugreifen möchte, zu überprüfen. Der agent gleicht die Zuverlässigkeit einer Website mit der entsprechenden Web-Reputation-Richtlinie, die auf dem Endpunkt angewendet wird, ab, um festzulegen, ob der Zugriff auf die Website zugelassen oder gesperrt wird.

Mit welcher Smart Protection Quelle der agent eine Verbindung aufbaut, hängt vom Standort des agents ab. Agents können entweder eine Verbindung zum Trend Micro Smart Protection Network oder Smart Protection Server herstellen.

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/

Smart Protection Server

Smart Protection Server für Benutzer, die Zugriff auf ihr Unternehmensnetzwerk haben. Lokale Server, um Smart Protection Dienste lokal im Unternehmensnetzwerk auszuführen, um die Effizienz zu optimieren.

Es gibt zwei Arten von Smart Protection Servern:

- **Integrierter Smart Protection Server**: Das OfficeScan Setup-Programm umfasst einen integrierten Smart Protection Server, der auf demselben Endpunkt installiert wird, auf dem bereits der OfficeScan Server installiert ist. Verwalten Sie nach der Installation die Einstellungen für diesen Server von der OfficeScan Webkonsole aus. Der integrierte Server soll dazu verwendet werden, OfficeScan in geringerem Umfang zu verteilen. Bei umfangreicheren Verteilungen ist ein eigenständiger Smart Protection Server erforderlich.
- **Eigenständiger Smart Protection Server**: Ein eigenständiger Smart Protection Server, der auf einem VMware oder Hyper-V Server installiert wurde. Der eigenständige Server verfügt über eine separate Management-Konsole und wird nicht von der OfficeScan Webkonsole verwaltet.

Smart Protection Quellen im Vergleich

Die folgende Tabelle stellt die Unterschiede zwischen Smart Protection Network und Smart Protection Server heraus.

TABELLE 4-1. Smart Protection Quellen im Vergleich

VERGLEICHSGRUNDLAGE	SMART PROTECTION SERVER	TREND MICRO SMART PROTECTION NETWORK
Verfügbarkeit	Verfügbar für interne agents, d. h. für agents, die die Standortkriterien erfüllen, die auf der OfficeScan Webkonsole festgelegt wurden.	Hauptsächlich verfügbar für externe agents, d. h. für agents, die die Standortkriterien nicht erfüllen, die auf der OfficeScan Webkonsole festgelegt wurden.
Zweck	Entwickelt und vorgesehen, um Smart Protection Services lokal in Unternehmensnetzwerken durchzuführen, um die Effizienz zu optimieren	Eine globale, internetbasierte Infrastruktur, die Smart Protection-Dienste für agents bereitstellt, die keinen direkten Zugriff auf ihr Unternehmensnetzwerk haben.
Administration	OfficeScan Administratoren installieren und verwalten diese Smart Protection Quellen	Trend Micro verwaltet diese Quelle
Pattern-Update-Adresse	Trend Micro ActiveUpdate server	Trend Micro ActiveUpdate server
Agent - Verbindungsprotokolle	HTTP und HTTPS	HTTPS

Pattern-Dateien von Smart Protection

Smart Protection Pattern-Dateien werden für File-Reputation-Dienste und Web-Reputation-Dienste verwendet. Trend Micro veröffentlicht diese Pattern-Dateien über den Trend Micro ActiveUpdate Server.

Agent-Pattern der intelligenten Suche

Das Agent-Pattern der intelligenten Suche wird täglich aktualisiert und von der Agent-Update-Adresse der OfficeScan agents (dem OfficeScan Server oder einer benutzerdefinierten Update-Adresse) heruntergeladen. Die Update-Adresse verteilt dann das Pattern auf die agents der intelligenten Suche.

Hinweis

agents der intelligenten Suche sind OfficeScan Agents, die Administratoren konfiguriert haben, um File-Reputation-Dienste zu benutzen. Agents , die File-Reputation-Dienste nicht anwenden, heißen „agents der herkömmlichen Suche“.

agents der intelligenten Suche verwenden beim Durchsuchen nach Sicherheitsrisiken das Agent-Pattern der intelligenten Suche. Wenn das Pattern das Risiko der Datei nicht ermitteln kann, wird ein anderes Pattern, das Pattern der intelligenten Suche heißt, verwendet.

Pattern der intelligenten Suche

Das Pattern der intelligenten Suche wird stündlich aktualisiert und wird von Smart Protection Quellen heruntergeladen. agents der intelligenten Suche laden das Pattern der intelligente Suche nicht herunter. Agents überprüfen potenzielle Bedrohungen mit Hilfe des Patterns der intelligente Suche, indem sie Suchabfragen an die Smart Protection Quellen senden.

Websperrliste

Die Webseiten-Sperrliste wird von Smart Protection Quellen heruntergeladen. OfficeScan Agents , die den Richtlinien der Web Reputation unterliegen, laden keine Websperrlisten herunter.

Hinweis

Administratoren können alle oder mehrere agents den Richtlinien der Web Reputation unterstellen.

Agents Agents, die den Web-Reputation-Richtlinien unterliegen, überprüfen die Zuverlässigkeit einer Website anhand der Websperrliste, indem Web-Reputation-Abfragen an die Smart Protection Quelle gesendet werden. Der agent gleicht die Zuverlässigkeit der von der Smart Protection Quelle erhaltenen Daten mit der Web-Reputation-Richtlinie ab, die auf dem Endpunkt festgelegt wurde. Die jeweilige Richtlinie bestimmt, ob der agent den Zugriff auf eine Website zulässt oder sperrt.

Update-Vorgang für Smart Protection Pattern

Die Smart Protection Pattern Updates stammen ursprünglich vom Trend Micro ActiveUpdate Server.

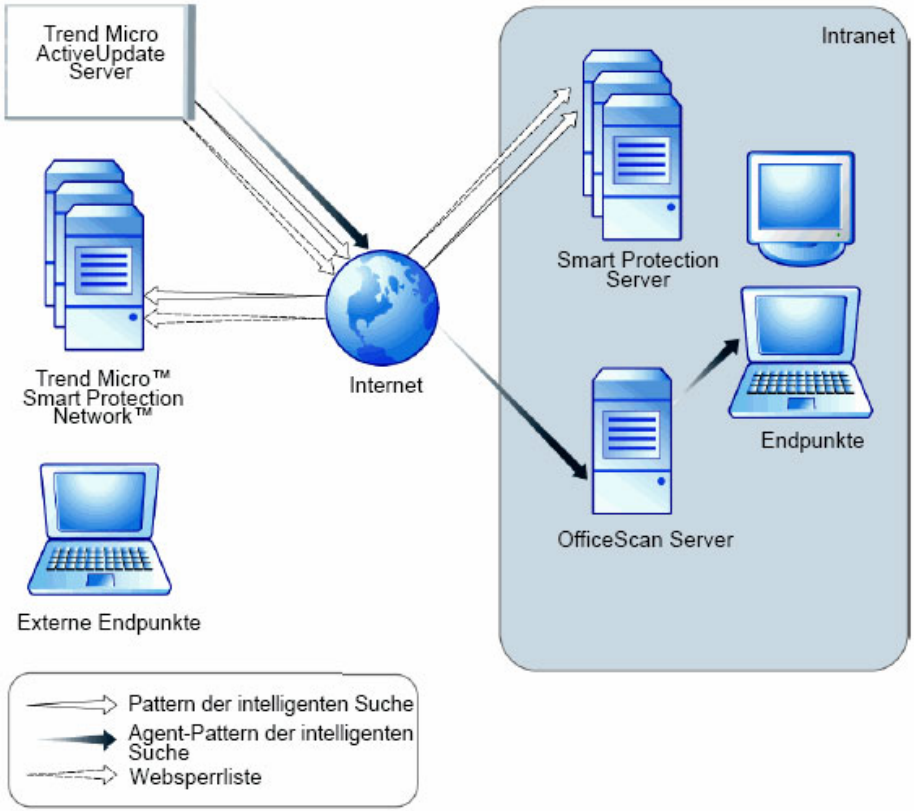


ABBILDUNG 4-1. Pattern-Update-Prozess

Verwendung von Smart Protection Pattern

Ein OfficeScan Agent verwendet das Agent-Pattern der intelligenten Suche, um nach Sicherheitsrisiken zu suchen, und sendet nur dann eine Anfrage an das Pattern der

intelligente Suche, wenn das Smart Scan Agent-Pattern das Risiko der Datei nicht bestimmen kann. Der agent sendet eine Anfrage an die Websperrliste, wenn ein Benutzer versucht, auf eine Website zuzugreifen. Mit der erweiterten Filtertechnologie legt der agent die Abfrageergebnisse in einem "Zwischenspeicher" ab. Dadurch ist es nicht mehr notwendig, ein und dieselbe Anfrage mehrmals zu senden.

Agents , die sich zurzeit in Ihrem Intranet befinden, können sich mit einem Smart Protection Server verbinden, um Anfragen an das Pattern der intelligente Suche oder die Websperrliste zu senden. Eine Netzwerkverbindung ist erforderlich, um eine Verbindung mit dem Smart Protection Server herzustellen. Wurde mehr als ein Smart Protection Server eingerichtet, können Administratoren die Verbindungspriorität festlegen.

Tipp

Sie können mehrere Smart Protection Server installieren, um die Kontinuität des Schutzes sicherzustellen, falls die Verbindung zu einem Smart Protection Server nicht verfügbar ist.

Agents , die sich zurzeit nicht in Ihrem Intranet befinden, können für Abfragen eine Verbindung zum Trend Micro Smart Protection Network herstellen. Eine

Internetverbindung ist erforderlich, um eine Verbindung mit dem Smart Protection Network herzustellen.

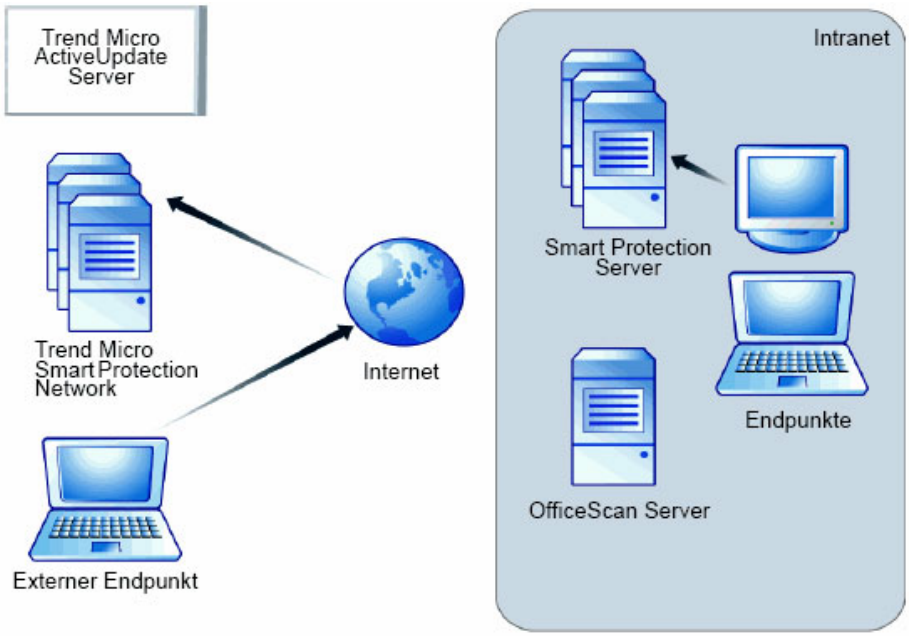


ABBILDUNG 4-2. Abfrageprozess

Agents können auch ohne Netzwerk- oder Internetverbindung vom Schutz profitieren, den das Agent-Pattern der intelligenten Suche und der Zwischenspeicher mit früheren Abfrageergebnissen liefern. Der Schutz ist nur dann geringer, wenn eine neue Abfrage erforderlich ist und der agent nach wiederholten Versuchen keine der Smart Protection Quellen erreichen kann. In diesem Fall markiert der agent die Datei zur weiteren Überprüfung und gewährt vorübergehend Zugriff auf die Datei. Wenn die Verbindung zu einem Smart Protection Server wiederhergestellt ist, werden alle markierten Dateien erneut durchsucht. Anschließend werden die entsprechenden Suchaktionen für alle Dateien ausgeführt, die als Bedrohung erkannt wurden.

Die folgende Tabelle beschreibt den Schutzumfang basierend auf dem Standort des agents.

TABELLE 4-2. Schutzverhalten nach Standort

SPEICHERORT	ARBEITSWEISE DER PATTERN-DATEI UND DER ABFRAGEN
Zugriff auf das	• **Pattern-Datei**: Agents laden die Datei mit dem Agent-Pattern der intelligenten Suche vom OfficeScan Server oder einer benutzerdefinierten Update-Adresse herunter. • **File- und Web-Reputation-Abfragen**: Agents verbinden sich mit dem Smart Protection Server für Abfragen.
Ohne Zugriff auf das Internet, aber mit Verbindung zum Smart Protection Network	• **Pattern-Datei**: Agents laden die neueste Datei mit den Agent-Pattern der intelligenten Suche erst dann herunter, wenn die Verbindung zum OfficeScan Server oder einer benutzerdefinierten Update-Adresse zur Verfügung steht. • **File- und Web-Reputation-Abfragen**: Agents verbinden sich mit dem Smart Protection Network für Abfragen.
Ohne Zugriff auf das Intranet und ohne Verbindung zum Smart Protection Network	• **Pattern-Datei**: Agents laden die neueste Datei mit den Agent-Pattern der intelligenten Suche erst dann herunter, wenn die Verbindung zum OfficeScan Server oder einer benutzerdefinierten Update-Adresse zur Verfügung steht. • **File- und Web-Reputation-Abfragen**: Agents erhalten keine Abfrageergebnisse und müssen sich auf das Agent-Pattern der intelligenten Suche und den Zwischenspeicher, der frühere Abfrageergebnisse enthält, stützen.

Smart Protection Services einrichten

Bevor agents File-Reputation-Dienste und Web-Reputation-Dienste ausführen können, stellen Sie sicher, dass die Smart Protection Umgebung entsprechend eingerichtet worden ist. Prüfen Sie Folgendes:

- *Installation des Smart Protection Server auf Seite 4-14*
- *Verwaltung des integrierten Smart Protection Servers auf Seite 4-19*
- *Liste der Smart Protection Quellen auf Seite 4-23*
- *Proxy-Einstellungen für Agent-Verbindungen auf Seite 4-32*
- *Einstellungen für den Endpunktstandort auf Seite 4-32*
- *Trend Micro Network VirusWall Installationen auf Seite 4-32*

Installation des Smart Protection Server

Sie können den integrierten oder den eigenständigen Smart Protection Server installieren, wenn die Anzahl der mit dem Server verbundenen agents 1.000 oder weniger beträgt. Installieren Sie einen eigenständigen Smart Protection Server, wenn mehr als 1.000 agents vorhanden sind.

Trend Micro empfiehlt die Installation mehrerer Smart Protection Server zur Ausfallsicherung. Agents , die keine Verbindung zu einem bestimmten Server aufbauen können, versuchen eine Verbindung zu den anderen Servern aufzubauen, die Sie eingerichtet haben.

Weil der integrierte Server und der OfficeScan Server auf demselben Endpunkt ausgeführt werden, kann bei sehr großem Datenverkehrsvolumen die Endpunktleistung beider Server signifikant beeinträchtigt werden. Erwägen Sie daher, einen eigenständigen Smart Protection Server als primäre Smart Protection Quelle für die agents zu verwenden und den integrierten Server als Backup.

Installation des eigenständigen Smart Protection Server

Informationen zur Installation und Verwaltung des eigenständigen Smart Protection Server s finden Sie im *Installations- und Upgrade-Handbuch für Smart Protection Server*.

Installation des integrierten Smart Protection Servers

Bei Installation des integrierten Servers während der Installation des OfficeScan Server:

- Aktivieren Sie den integrierten Server und konfigurieren Sie die Servereinstellungen. Weitere Informationen finden Sie unter *Verwaltung des integrierten Smart Protection Servers auf Seite 4-19*.

- Wenn sich der integrierte Server und der OfficeScan Agent auf demselben Servercomputer befinden, sollten Sie die OfficeScan Firewall deaktivieren. Die OfficeScan Firewall ist für den agent-Endpunkt vorgesehen und könnte, wenn sie aktiviert ist, auf Servern die Leistung beeinträchtigen. Anweisungen zum Deaktivieren der Firewall finden Sie unter *Die OfficeScan Firewall aktivieren oder deaktivieren auf Seite 13-6*.

Hinweis

Beachten Sie die Auswirkungen einer deaktivierten Firewall, und stellen Sie sicher, dass Ihre Sicherheitspläne eingehalten werden.

Tipp

Installieren Sie den integrierten Smart Protection Server, nachdem Sie die Installation von OfficeScan abgeschlossen haben, indem Sie das *Tool für integrierten Smart Protection Server auf Seite 4-15* verwenden.

Tool für integrierten Smart Protection Server

Das Trend Micro Tool für einen integrierten Smart Protection Server unterstützt Administratoren dabei, einen integrierten Smart Protection Server nach Abschluss der Installation des OfficeScan Servers zu installieren bzw. zu deinstallieren. Die aktuelle Version von OfficeScan lässt nicht zu, dass Administratoren einen integrierten Smart Protection Server installieren/entfernen, nachdem die Installation des OfficeScan Servers abgeschlossen wurde. Dieses Tool erweitert die Flexibilität der Installationsfunktionen gegenüber den vorherigen Versionen von OfficeScan.

Prozedur

1. Öffnen Sie die Eingabeaufforderung und navigieren Sie zum Verzeichnis <*Installationsordner des Servers*>\PCCSRV\Admin\Utility\ISPSInstaller, in dem sich `ISPSInstaller.exe` befindet.

2. Führen Sie `ISPSInstaller.exe` mit Hilfe eines der folgenden Befehle aus:

TABELLE 4-3. Optionen des Installationsprogramms

BEFEHL	BESCHREIBUNG
`ISPSInstaller.exe /i`	Installiert den integrierten Smart Protection Server anhand der Standard-Porteinstellungen. Details zu den Standard-Porteinstellungen finden Sie in der unten stehenden Tabelle.
`ISPSInstaller.exe /i /f:[Portnummer] /s:[Portnummer] /w:[Portnummer]`	Installiert den integrierten Smart Protection Server anhand der angegebenen Ports. **Hinweis** Sie können die Ports nur bei Verwendung eines Apache Webservers konfigurieren. Wobei gilt: • `/f:[Portnummer]` den HTTP-Port für File Reputation darstellt • `/f:[Portnummer]` den HTTPS-Port für File Reputation darstellt • `/f:[Portnummer]` den Web-Reputation Port darstellt **Hinweis** Einem nicht angegebenen Port wird automatisch der Standardwert zugeordnet.
`ISPSInstaller.exe /u`	Deinstalliert den integrierten Smart Protection Server

TABELLE 4-4. Ports für die Reputation-Dienste des integrierten Smart Protection Servers

WEBSERVER UND EINSTELLUNGEN	PORTS FÜR FILE-REPUTATION-DIENSTE		HTTP-PORT FÜR WEB-REPUTATION-DIENSTE
	HTTP	HTTPS (SSL)	
IIS Standard-Website mit aktiviertem SSL	80	443 (not configurable)	80 (not configurable)
IIS Standard-Website mit deaktiviertem SSL	80	443 (not configurable)	80 (not configurable)
IIS virtuelle Website mit aktiviertem SSL	8080	4343 (configurable)	8080 (configurable)
IIS virtuelle Website mit deaktiviertem SSL	8080	4343 (configurable)	8080 (configurable)

3. Öffnen Sie nach Abschluss der Installation die OfficeScan Webkonsole und verifizieren Sie Folgendes:

   - Öffnen Sie die **Microsoft Management-Konsole** (durch Eingabe von `services.msc` im Menü **Starten**) und überprüfen Sie, ob der Trend Micro Local Web Classification Server und der Trend Micro Smart Scan Server mit dem Status "Gestartet" aufgelistet sind.
   - Öffnen Sie den **Windows Task Manager**. Überprüfen Sie auf der Registerkarte **Prozesse**, ob `iCRCService.exe` und `LWCSService.exe` ausgeführt werden.
   - Stellen Sie in der OfficeScan Webkonsole sicher, dass der Menübefehl **Administration** > **Smart Protection** > **Integrierter Server** angezeigt wird.

Bewährte Methoden im Umgang mit dem Smart Protection Server

Optimieren Sie die Leistung der Smart Protection Server durch Berücksichtigung folgender Punkte:

- Vermeiden Sie es, gleichzeitig manuelle und zeitgesteuerte Suchvorgänge durchzuführen. Staffeln Sie die Suchvorgänge in Gruppen.
- Vermeiden Sie, dass alle agents gleichzeitig die Funktion "Jetzt durchsuchen" verwenden.
- Passen Sie Smart Protection Server an langsamere Netzwerkverbindungen an, zirka 512KBit/s, indem Sie Änderungen in der `ptngrowth.ini`-Datei vornehmen.

Die Datei ptngrowth.ini für den eigenständigen Server anpassen

Prozedur

1. Öffnen Sie die Datei `ptngrowth.ini` in `/var/tmcss/conf/`.
2. Ändern Sie die `ptngrowth.ini`-Datei und verwenden Sie die unten empfohlenen Werte:
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. Speichern Sie die `ptngrowth.ini`-Datei.
4. Geben Sie für den Neustart des `lighttpd`-Service den folgenden Befehl über die Befehlszeilenschnittstelle (CLI) ein:
   - `Neustart lighttpd-Service`

Die Datei ptngrowth.ini für den integrierten Server anpassen

Prozedur

1. Öffnen Sie die Datei `ptngrowth.ini` in <*Installationsordner des Servers*>`\PCCSRV\WSS\`.

2. Ändern Sie die `ptngrowth.ini`-Datei und verwenden Sie die unten empfohlenen Werte:
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. Speichern Sie die `ptngrowth.ini`-Datei.
4. Führen Sie einen Neustart des `Trend Micro Smart Protection Server` Service durch.

Verwaltung des integrierten Smart Protection Servers

Verwalten Sie den integrierten Smart Protection Server, indem Sie folgende Aufgaben durchführen:

- Aktivieren der File-Reputation-Dienste und der Web-Reputation-Dienste des integrierten Servers
- Erfassen der Adressen des integrierten Servers
- Update der Komponenten des integrierten Servers
- Konfigurieren der Liste Zulässige/Gesperrte URLs des integrierten Servers

Weitere Informationen finden Sie unter *Einstellungen eines integrierten Smart Protection Servers konfigurieren auf Seite 4-22*.

Aktivieren der File-Reputation-Dienste und der Web-Reputation-Dienste des integrierten Servers

Damit die agents Suchabfragen und Web-Reputation-Abfragen an den integrierten Server senden können, müssen ihre File-Reputation-Dienste und Web-Reputation-Dienste aktiviert werden. Die Aktivierung dieser Dienste ermöglicht es dem integrierten Server außerdem Komponenten-Updates über den ActiveUpdate Server durchzuführen.

Diese Dienste werden automatisch aktiviert, wenn Sie gewählt haben, den integrierten Server während der Installation von OfficeScan Server zu installieren.

Wenn Sie die Dienste deaktivieren, müssen Sie sicherstellen, dass Sie eigenständige Smart Protection Server installiert haben, an die agents Abfragen senden können.

Weitere Informationen finden Sie unter *Einstellungen eines integrierten Smart Protection Servers konfigurieren auf Seite 4-22*.

Erfassen der Adressen des integrierten Servers

Sie benötigen die Adressen des integrierten Servers, wenn Sie die Liste der Smart Protection Quellen für interne agents konfigurieren. Weitere Informationen zur Liste finden Sie unter *Liste der Smart Protection Quellen auf Seite 4-23*.

Wenn agents Suchabfragen an den integrierten Server senden, identifizieren sie den Server durch eine von zwei File-Reputation-Dienste Adressen – eine HTTP- oder HTTPS-Adresse. Die Verbindung über eine HTTPS-Adresse ist sicherer, während eine HTTP-Verbindung weniger Bandbreite benötigt.

Wenn agents Web-Reputation-Abfragen senden, identifizieren sie den integrierten Server anhand seiner Web-Reputation-Dienste-Adresse.

Tipp

Agents , die von einem anderen OfficeScan Server verwaltet werden, können auch eine Verbindung mit dem integrierten Server aufbauen. Fügen Sie auf der Webkonsole des anderen OfficeScan Servers die Adresse des integrierten Servers zur Liste der Smart Protection Quelle hinzu.

Weitere Informationen finden Sie unter *Einstellungen eines integrierten Smart Protection Servers konfigurieren auf Seite 4-22*.

Update der Komponenten des integrierten Servers

Der integrierte Sever führt ein Update der folgenden Komponenten durch:

- **Pattern der intelligenten Suche**: OfficeScan Agents Agents überprüfen potenzielle Bedrohungen mit Hilfe des Patterns der intelligente Suche, indem sie Suchabfragen an den integrierten Server senden.
- **Websperrliste**: OfficeScan Agents Agents, die den Web-Reputation-Richtlinien unterliegen, überprüfen die Zuverlässigkeit einer Website anhand der Websperrliste, indem Web-Reputation-Abfragen an den integrierten Server gesendet werden.

Sie können diese Komponenten manuell aktualisieren oder einen Update-Zeitplan konfigurieren. Der integrierte Server lädt Komponenten vom ActiveUpdate Server herunter.

Hinweis

Ein reiner IPv6-integrierter Server kann Updates nicht direkt vom Trend Micro ActiveUpdate Server herunterladen. Ein Dual-Stack-Proxy-Server, der IP-Adressen konvertieren kann wie DeleGate, muss ermöglichen, dass der integrierte Server eine Verbindung zum ActiveUpdate Server herstellen kann.

Weitere Informationen finden Sie unter *Einstellungen eines integrierten Smart Protection Servers konfigurieren auf Seite 4-22*.

Konfiguration der Liste "Zulässige/Gesperrte URLs" des integrierten Servers

Agents unterhalten ihre eigene Liste der zulässigen/gesperrten URLs. Die Liste für agents wird konfiguriert, wenn die Web-Reputation-Richtlinien aufgestellt werden (Einzelheiten dazu finden Sie unter *Web-Reputation-Richtlinien auf Seite 12-5*). Jede URL in der agent-Liste wird automatisch zugelassen bzw. gesperrt.

Der integrierte Server hat seine eigene Liste der zulässigen/gesperrten URLs. Ist eine URL nicht in der agent-Liste, sendet der agent eine Web-Reputation-Abfrage an den integrierten Server (wenn der integrierte Server als Smart Protection Quelle festgelegt wurde). Wird die URL in der Liste der zulässigen/gesperrten URLs gefunden, benachrichtigt der integrierte Server den agent, die URL zuzulassen bzw. zu sperren.

Hinweis

Die Liste der gesperrten URLs hat eine höhere Priorität als die Webseiten-Sperrliste.

Um URLs der Liste der zulässigen/gesperrten URLs des integrierten Servers hinzuzufügen, importieren Sie eine Liste vom eigenständigen Smart Protection Server. Es ist nicht möglich, URLs manuell hinzuzufügen.

Weitere Informationen finden Sie unter *Einstellungen eines integrierten Smart Protection Servers konfigurieren auf Seite 4-22*.

Einstellungen eines integrierten Smart Protection Servers konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Smart Protection** > **Integrierter Server**.
2. Wählen Sie **File-Reputation-Dienste aktivieren** aus.
3. Wählen Sie das Protokoll (HTTP oder HTTPS) aus, das agents verwenden, wenn sie die Suchabfrage an den integrierten Server senden.
4. Wählen Sie **Web-Reputation-Dienste aktivieren**.
5. Erfassen Sie die Adressen des integrierten Servers, die in der Spalte **Server-Adresse** angezeigt werden.
6. Update der Komponenten des integrierten Servers:
   - Zeigen Sie die aktuellen Versionen des intelligenten Such-Patterns und der Webseiten-Sperrliste an. Ist ein Update verfügbar, klicken Sie auf **Jetzt aktualisieren**. Das Update-Ergebnis wird oben im Fenster angezeigt.
   - Das Pattern automatisch aktualisieren:
     a. Klicken Sie auf **Zeitgesteuertes Update aktivieren**.
     b. Wählen Sie aus, ob Sie stündlich oder alle 15 Minuten aktualisieren möchten.
     c. Wählen Sie eine Update-Adresse unter **File-Reputation-Dienste** aus. Das intelligente Suchpattern wird von dieser Quelle aus aktualisiert.
     d. Wählen Sie eine Update-Adresse unter **Web-Reputation-Dienste** aus. Die Webseiten-Sperrliste wird von dieser Quelle aus aktualisiert.

Hinweis

- Wenn Sie den ActiveUpdate Server als Update-Adresse nutzen, stellen Sie sicher, dass der 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 *Proxy für Updates von OfficeScan Server auf Seite 6-20*.

- Wenn Sie eine benutzerdefinierte Update-Adresse auswählen, konfigurieren Sie die entsprechende Umgebung und die Update-Ressourcen diese Update-Adresse. Stellen Sie auch sicher, dass der Servercomputer mit dieser Update-Adresse verbunden ist. Sollten Sie beim Einrichten einer Update-Adresse Hilfe benötigen, wenden Sie sich an Ihren Support-Anbieter.

7. Konfigurieren der Liste der Zulässigen/Gesperrten URLs des integrierten Servers:

   a. Klicken Sie auf **Importieren**, um die Liste mit URLs aus einer vorformatierten `.csv`-Datei auszufüllen. Sie erhalten die `.csv`-Datei über den eigenständigen Smart Protection Server.

   b. Wenn Sie über eine bestehende Liste verfügen, klicken Sie auf **Exportieren**, um die Liste in einer `.csv`-Datei zu speichern.

8. Klicken Sie auf **Speichern**.

Liste der Smart Protection Quellen

Agents senden beim Durchsuchen nach Sicherheitsrisiken und Bewerten der Zuverlässigkeit einer Website Anfragen an Smart Protection Quellen.

IPv6-Unterstützung für Smart Protection Quellen

Ein reiner IPv6-agent kann Anfragen nicht direkt an reine IPv4-Quellen senden wie zum Beispiel:

- Smart Protection Server 2.0 (integriert oder standalone)

Hinweis

IPv6-Unterstützung für Smart Protection Server ist ab Version 2.5 verfügbar.

- Trend Micro Smart Protection Network

Entsprechend kann ein reiner IPv4-agent ebenfalls keine Anfragen an reine IPv6 Smart Protection Server senden.

Ein Dual-Stack-Proxy-Server, der IP-Adressen konvertieren kann wie DeleGate, muss ermöglichen, dass agents eine Verbindung zu den Quellen herstellen können.

Smart Protection Quellen und Endpunkt-Standort

Mit welcher Smart Protection Quelle der agent eine Verbindung aufbaut, hängt vom Standort des agent Endpunkts ab.

Weitere Informationen zum Konfigurieren der Einstellungen für den Standort finden Sie unter *Endpunktspeicherort auf Seite 15-2*.

TABELLE 4-5. Smart Protection Quellen nach Standort

SPEICHERORT	SMART PROTECTION QUELLEN
Extern	Externe agents senden Such- und Web-Reputation-Abfragen an das Trend Micro Smart Protection Network.

SPEICHERORT	SMART PROTECTION QUELLEN
Intern	Interne agents senden Such- und Web-Reputation-Abfragen an Smart Protection Server oder an Trend Micro Smart Protection Network. Wenn Sie Smart Protection Server installiert haben, konfigurieren Sie die Liste der Smart Protection Quellen auf der OfficeScan Webkonsole. Ein interner agent wählt einen Server aus der Liste, wenn eine Abfrage ausgeführt werden muss. Wenn ein agent keine Verbindung zum ersten Server aufbauen kann, wird ein anderer Server aus der Liste gewählt. **Tipp** Sie können einen eigenständigen Smart Protection Server als primäre Suchquelle und den integrierten Server als Backup zuordnen. Auf diese Weise wird der Datenverkehr mit dem Endpunkt reduziert, auf dem sich der OfficeScan Server und der integrierte Server befinden. Der eigenständige Server kann außerdem mehr Abfragen verarbeiten. Sie können entweder die Standardliste oder die benutzerdefinierte Liste der Smart Protection Quellen konfigurieren. Die Standardliste wird von allen internen agents verwendet. Eine benutzerdefinierte Liste definiert den Bereich einer IP-Adresse. Befindet sich die IP-Adresse eines internen agent innerhalb dieses Bereichs, benutzt der agent die benutzerdefinierte Liste.

Standardliste der Smart Protection Quellen konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Smart Protection** > **Smart Protection Quellen**.
2. Klicken Sie auf die Registerkarte **Interne Agents**.
3. Wählen Sie **Standardliste verwenden (für alle internen Agents)** aus.
4. Klicken Sie auf den Link **Standardliste**.

   Es öffnet sich ein neues Fenster.

5. Klicken Sie auf **Hinzufügen**.

   Es öffnet sich ein neues Fenster.

6. Geben Sie den Host-Namen des Smart Protection Servers oder die IPv4-/IPv6-Adresse ein. Wenn Sie eine IPv6-Adresse eingeben, setzen Sie die Adresse in Klammern.

   Hinweis

   Geben Sie den Host-Namen ein, wenn es IPv4- oder IPv6-Agents gibt, die sich mit dem Smart Protection Server verbinden.

7. Wählen Sie **File-Reputation-Dienste** aus. Agents können Abfragen per HTTP- oder HTTPS-Protokoll durchführen. HTTPS ermöglicht eine sicherere Verbindung, während HTTP weniger Bandbreite benötigt.

   a. Wenn Agents HTTP verwenden sollen, geben Sie den Server-Listening-Port für HTTP-Anfragen ein. Wenn Agents HTTPS verwenden sollen, wählen Sie "SSL" aus und geben Sie den Server-Listening-Port für HTTPS-Anfragen ein.

   b. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob die Verbindung zum Server aufgebaut werden kann.

   Tipp

   Die Listening Ports sind Teil der Server Adresse. Die Serveradresse ändern:

   Im Falle des integrierten Servers öffnen Sie die OfficeScan Webkonsole und navigieren Sie zu **Administration** > **Smart Protection** > **Integrierter Server**.

   Im Falle des eigenständigen Servers öffnen Sie die Konsole des eigenständigen Servers, und navigieren Sie zum Fenster **Übersicht**.

8. Wählen Sie **Web-Reputation-Dienste** aus. Agents senden Web-Reputation-Abfragen per HTTP-Protokoll. HTTPS wird nicht unterstützt.

   a. Geben Sie den Server-Listening-Port für HTTP-Anfragen ein.

   b. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob die Verbindung zum Server aufgebaut werden kann.

9. Klicken Sie auf **Speichern**.

   Das Fenster wird geschlossen.

10. Fügen Sie mehrere Server hinzu, indem Sie die vorhergehenden Schritte wiederholen.

11. Wählen Sie aus dem Fenster oben **Reihenfolge** oder **Zufällig** aus.

    - **Reihenfolge**: Die Agents wählen die Server in der Reihenfolge aus, in der sie auf der Liste erscheinen. Wenn Sie **Reihenfolge** auswählen, können Sie mit Hilfe der Pfeile unterhalb der Spalte **Reihenfolge** die Server in der Liste nach oben oder unten bewegen.

    - **Zufällig**: Die Agents wählen die Server nach dem Zufallsprinzip aus.

Tipp

Weil der integrierte Smart Protection Server und der OfficeScan Server auf demselben Endpunkt ausgeführt werden können, kann bei sehr hohem Datenaufkommen die Leistung des Endpunkts für beide Server signifikant beeinträchtigt werden. Um den Datenverkehr zum OfficeScan Server-Computer zu reduzieren, ordnen Sie einen eigenständigen Smart Protection Server als primäre Smart Protection Quelle und den integrierten Server als eine Backup-Quelle zu.

12. Verschiedene Aufgaben im angezeigten Fenster durchführen.

    - Wenn Sie eine Liste von einem anderen Server exportiert haben und sie in dieses Fenster importieren möchten, klicken Sie auf **Importieren**, und navigieren Sie zur `.dat`-Datei. Die Liste wird in das Fenster geladen.

    - Um die Liste in eine `.dat`-Datei zu exportieren, klicken Sie auf **Exportieren**, und klicken Sie anschließend auf **Speichern**.

    - Um den Servicestatus der Server zu aktualisieren, klicken Sie auf **Aktualisieren**.

    - Klicken Sie auf den Servernamen, um eine der folgenden Aufgaben auszuführen:

      - Serverinformationen anzeigen oder bearbeiten.

- Die vollständige Serveradresse für Web-Reputation-Dienste oder File-Reputation-Dienste anzeigen.

- Um die Konsole eines Smart Protection Servers zu öffnen, klicken Sie auf **Konsole starten**.

  - Das Serverkonfigurationsfenster für den integrierten Smart Protection Server wird angezeigt.

  - Für eigenständige Smart Protection Server und den integrierten Smart Protection Server eines anderen OfficeScan Servers wird das Anmeldefenster für die Konsole angezeigt.

- Um einen Eintrag zu löschen, aktivieren Sie das Kontrollkästchen für den Server, und klicken Sie auf **Löschen**.

13. Klicken Sie auf **Speichern**.

    Das Fenster wird geschlossen.

14. Klicken Sie auf **Alle Agents benachrichtigen**.

Benutzerdefinierte Listen der Smart Protection Quellen konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Smart Protection** > **Smart Protection Quellen**.

2. Klicken Sie auf die Registerkarte **Interne Agents**.

3. Wählen Sie **Benutzerdefinierte Listen basierend auf der IP-Adresse des Agents verwenden** aus.

4. (Optional) Wählen Sie **Standardliste verwenden, wenn kein Server in den benutzerdefinierten Listen verfügbar ist**, aus.

Tipp

Trend Micro empfiehlt die Aktivierung dieser Funktion, um sicherzustellen, dass Agents eine Verbindung zu einer Smart Protection Quelle herstellen können, wenn die benutzerdefinierten Quellen nicht mehr zur Verfügung stehen.

5. Klicken Sie auf **Hinzufügen**.

   Es öffnet sich ein neues Fenster.

6. Geben Sie im Abschnitt **IP-Bereich** einen IPv4- oder IPv6-Adressbereich ein oder beide.

Hinweis

Agents mit einer IPv4-Adresse können sich mit reinen IPv4- oder mit Dual-Stack-Smart Protection Servern verbinden. Agents mit einer IPv6-Adresse können sich mit reinen IPv6- oder mit Dual-Stack-Smart Protection Servern verbinden. Agents, die sowohl eine IPv4- als auch eine IPv6-Adresse besitzen, können sich mit jedem Smart Protection Server verbinden.

7. Geben Sie im Abschnitt **Proxy-Einstellung** die Proxy-Einstellungen ein, die Agents benutzen, um sich mit den Smart Protection Servern zu verbinden.

   a. Wählen Sie **Für die Kommunikation zwischen Agent und Smart Protection Server einen Proxy-Server verwenden** aus.

   b. Geben Sie den Namen des Proxy-Servers oder eine IPv4-/IPv6-Adresse und eine Portnummer an.

   c. Falls der Proxy-Server eine Authentifizierung verlangt, geben Sie den Benutzernamen und das Kennwort ein.

8. Fügen Sie der **Liste der benutzerdefinierten Smart Protection Server** Smart Protection Server hinzu.

   a. Geben Sie den Host-Namen des Smart Protection Servers oder die IPv4-/IPv6-Adresse ein. Wenn Sie eine IPv6-Adresse eingeben, setzen Sie die Adresse in Klammern.

Hinweis

Geben Sie den Host-Namen ein, wenn es IPv4- oder IPv6-Agents gibt, die sich mit dem Smart Protection Server verbinden.

b. Wählen Sie **File-Reputation-Dienste** aus. Agents können Abfragen per HTTP- oder HTTPS-Protokoll durchführen. HTTPS ermöglicht eine sicherere Verbindung, während HTTP weniger Bandbreite benötigt.

   i. Wenn Agents HTTP verwenden sollen, geben Sie den Server-Listening-Port für HTTP-Anfragen ein. Wenn Agents HTTPS verwenden sollen, wählen Sie **SSL** aus und geben Sie den Server-Listening-Port für HTTPS-Anfragen ein.

   ii. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob die Verbindung zum Server aufgebaut werden kann.

Tipp

Die Listening Ports sind Teil der Server Adresse. Die Serveradresse ändern:

Im Falle des integrierten Servers öffnen Sie die OfficeScan Webkonsole und navigieren Sie zu **Administration** > **Smart Protection** > **Integrierter Server**.

Im Falle des eigenständigen Servers öffnen Sie die Konsole des eigenständigen Servers, und navigieren Sie zum Fenster Übersicht.

c. Wählen Sie **Web-Reputation-Dienste** aus. Agents senden Web-Reputation-Abfragen per HTTP-Protokoll. HTTPS wird nicht unterstützt.

   i. Geben Sie den Server-Listening-Port für HTTP-Anfragen ein.

   ii. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob die Verbindung zum Server aufgebaut werden kann.

d. Klicken Sie **Zur Liste hinzufügen**.

e. Fügen Sie mehrere Server hinzu, indem Sie die vorhergehenden Schritte wiederholen.

f. Wählen Sie **Reihenfolge** oder **Zufällig** aus.

- **Reihenfolge**: Die Agents wählen die Server in der Reihenfolge aus, in der sie auf der Liste erscheinen. Wenn Sie **Reihenfolge** auswählen, können Sie mit Hilfe der Pfeile unterhalb der Spalte **Reihenfolge** die Server in der Liste nach oben oder unten bewegen.
- **Zufällig**: Die Agents wählen die Server nach dem Zufallsprinzip aus.

Tipp

Weil der integrierte Smart Protection Server und der OfficeScan Server auf demselben Computer ausgeführt werden, kann die Computerleistung der beiden Server bei sehr hohem Datenaufkommen signifikant beeinträchtigt werden. Um den Datenverkehr zum OfficeScan Server-Computer zu reduzieren, ordnen Sie einen eigenständigen Smart Protection Server als primäre Smart Protection Quelle und den integrierten Server als eine Backup-Quelle zu.

g. Verschiedene Aufgaben im angezeigten Fenster durchführen.

- Um den Servicestatus der Server zu aktualisieren, klicken Sie auf **Aktualisieren**.
- Um die Konsole eines Smart Protection Servers zu öffnen, klicken Sie auf **Konsole starten**.
  - Das Serverkonfigurationsfenster für den integrierten Smart Protection Server wird angezeigt.
  - Für eigenständige Smart Protection Server und den integrierten Smart Protection Server eines anderen OfficeScan Servers wird das Anmeldefenster für die Konsole angezeigt.
- Um einen Eintrag zu löschen, klicken Sie auf **Löschen** (

).

9. Klicken Sie auf **Speichern**.

Das Fenster wird geschlossen. Die Liste, die Sie gerade hinzugefügt haben, erscheint als Link eines IP-Bereichs unter der Tabelle **IP-Bereich**.

10. Wiederholen Sie Schritt 4 bis Schritt 8, um weitere benutzerdefinierte Listen hinzuzufügen.

11. Verschiedene Aufgaben im angezeigten Fenster durchführen.

    - Um eine Liste zu ändern, klicken Sie auf den Link des IP-Bereichs und ändern Sie dann die Einstellungen in dem Fenster, das sich öffnet.
    - Um die Liste in eine .DAT-Datei zu exportieren, klicken Sie auf **Exportieren**, und klicken Sie anschließend auf **Speichern**.
    - Wenn Sie eine Liste von einem anderen Server exportiert haben und sie in dieses Fenster importieren möchten, klicken Sie auf **Importieren**, und navigieren Sie zur `.dat`-Datei. Die Liste wird in das Fenster geladen.

12. Klicken Sie auf **Alle Agents benachrichtigen**.

Proxy-Einstellungen für Agent-Verbindungen

Wenn zum Verbindungsaufbau mit dem Smart Protection Network eine Proxy-Authentifizierung erforderlich ist, geben Sie zur Authentifizierung die Anmeldedaten ein.

Konfigurieren Sie interne Proxy-Einstellungen, die Agents für Verbindungen mit einem Smart Protection Server verwenden.

Weitere Informationen finden Sie unter *OfficeScan Agent Proxy-Einstellungen auf Seite 15-53*.

Einstellungen für den Endpunktstandort

OfficeScan umfasst die Funktion "Location Awareness", die den Standort des agent-Computers identifiziert und bestimmt, ob der agent eine Verbindung zum Smart Protection Network oder Smart Protection Server aufbaut. Dadurch wird unabhängig vom Standort sichergestellt, dass agents geschützt sind.

Weitere Informationen zum Konfigurieren der Standorteinstellungen finden Sie unter *Endpunktspeicherort auf Seite 15-2*.

Trend Micro Network VirusWall Installationen

Wenn Trend Micro™ Network VirusWall™ Enforcer installiert ist:

- Installieren Sie einen Hotfix (Build 1047 für Network VirusWall Enforcer 2500 und Build 1013 für Network VirusWall Enforcer 1200).
- Aktualisieren Sie die OPSWAT-Engine auf Version 2.5.1017, damit das Produkt die Suchmethode des agents erkennen kann.

Smart Protection Services verwenden

Nachdem die Smart Protection Umgebung entsprechend eingerichtet worden ist, sind die agents bereit, File-Reputation-Dienste und Web-Reputation-Dienste anzuwenden. Sie können auch zuerst die Smart Feedback Einstellungen konfigurieren.

Hinweis

Weitere Informationen über das Einrichten der Smart Protection Umgebung finden Sie unter *Smart Protection Services einrichten auf Seite 4-13*.

Um vom Schutz der File-Reputation-Dienste zu profitieren, müssen agents eine Suchmethode verwenden, die als "Intelligente Suche" bezeichnet wird. Weitere Informationen über die intelligente Suche und deren Aktivierung auf agents finden Sie unter *Suchmethodentypen auf Seite 7-9*.

Um OfficeScan Agents den Einsatz der Web-Reputation-Dienste zu gestatten, konfigurieren Sie die Web-Reputation-Richtlinien. Weitere Informationen finden Sie unter *Web-Reputation-Richtlinien auf Seite 12-5*.

Hinweis

Die Einstellungen für Suchmethoden und Web-Reputation-Richtlinien sind granuläre Einstellungen. Ihren eigenen Anforderungen entsprechend können Sie Einstellungen so konfigurieren, dass sie auf alle agents angewendet werden, oder Sie konfigurieren spezielle Einstellungen für einzelne agents oder agent-Gruppen.

Weitere Informationen zum Konfigurieren von Smart Feedback finden Sie unter *Smart Feedback auf Seite 14-73*.

Kapitel 5

Den OfficeScan Agent installieren

In diesem Kapitel werden die Systemvoraussetzungen für OfficeScan und die Verfahren zur OfficeScan Agent-Installation beschrieben.

Weitere Informationen zum Aktualisieren von OfficeScan Agent finden Sie im *Installations- und Upgrade-Handbuch für OfficeScan*.

Es werden folgende Themen behandelt:

- *OfficeScan Agent Erstinstallationen auf Seite 5-2*
- *überlegungen zur Installation auf Seite 5-2*
- *Überlegungen zur Verteilung auf Seite 5-12*
- *Zu OfficeScan Agent migrieren auf Seite 5-67*
- *Nach der Installation auf Seite 5-71*
- *OfficeScan Agent deinstallieren auf Seite 5-74*

OfficeScan Agent Erstinstallationen

Der OfficeScan Agent kann auf Computern unter folgenden Microsoft Windows Plattformen installiert werden: OfficeScan ist auch mit verschiedenen Produkten von Drittanbietern kompatibel.

Auf der folgenden Website erhalten Sie eine vollständige Liste der Systemvoraussetzungen und kompatibler Produkte von Drittanbietern:

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

überlegungen zur Installation

Beachten Sie vor der Installation der OfficeScan Agents folgende Hinweise:

TABELLE 5-1. überlegungen zur OfficeScan Agent-Installation

ÜBERLEGUNG	BESCHREIBUNG
Unterstützung von Windows-Funktionen	Einige OfficeScan Agent-Funktionen sind auf bestimmten Windows Plattformen nicht verfügbar.
IPv6-Unterstützung	Der OfficeScan Agent kann auf Dual-Stack- oder reinen IPv6-Endpunkten installiert werden. Jedoch: • Einige Windows Betriebssysteme, auf denen der OfficeScan Agent installiert werden kann, unterstützen keine IPv6-Adressierung. • Bei einigen Installationsmethoden gibt es besondere Voraussetzungen für die erfolgreiche Installation des OfficeScan Agents.
OfficeScan Agent-IP-Adressen	Bei OfficeScan Agents mit sowohl IPv4- als auch IPv6-Adressen können Sie wählen, welche IP-Adresse verwendet wird, wenn sich der OfficeScan Agent am Server anmeldet.

ÜBERLEGUNG	BESCHREIBUNG
Ausschlussliste n	Stellen Sie sicher, dass die Ausschlussliste für die folgenden Funktionen richtig konfiguriert wurden: • **Verhaltensüberwachung**:Fügen Sie besonders wichtige Endpunkt-Programme zur Liste "Zulässige Programme" hinzu, um zu verhindern, dass der OfficeScan Agent diese Anwendungen sperrt. Weitere Informationen finden Sie unter *Ausschlussliste für Verhaltensüberwachung auf Seite 9-10*. • **Web Reputation**:Fügen Sie Websites, die Sie als sicher einstufen, zur Liste der zulässigen URLs hinzu, um zu verhindern, dass der OfficeScan Agent den Zugriff auf diese Websites sperrt. Weitere Informationen finden Sie unter *Web-Reputation-Richtlinien auf Seite 12-5*.

OfficeScan Agent Funktionen

Die auf dem Endpunkt verfügbaren OfficeScan Agent-Funktionen richten sich nach dem Betriebssystem.

TABELLE 5-2. OfficeScan Agent-Funktionen auf Server-Plattformen

FUNKTION	WINDOWS BETRIEBSSYSTEM			
	SERVER 2003	SERVER 2008/ SERVER CORE 2008	SERVER 2012/ SERVER CORE 2012	SERVER 2016/ SERVER CORE 2016
Manuelle Suche, Echtzeitsuche und zeitgesteuerte Suche	Ja	Ja	Ja	Ja

Funktion	Windows Betriebssystem			
	Server 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
Komponenten-Update (manuelles und zeitgesteuertes Update)	Ja	Ja	Ja	Ja
Update-Agent	Ja	Ja	Ja	Ja
Web Reputation	Ja, aber standardmäßig bei der Server-Installation deaktiviert	Ja, aber standardmäßig bei der Server-Installation deaktiviert	Ja, aber standardmäßig bei der Server-Installation deaktiviert	Ja, aber standardmäßig bei der Server-Installation deaktiviert
Damage Cleanup Services	Ja	Ja	Ja	Ja
OfficeScan Firewall	Ja, aber standardmäßig bei der Server-Installation deaktiviert	Ja, aber standardmäßig bei der Server-Installation deaktiviert	Ja, aber standardmäßig bei der Server-Installation deaktiviert	Ja, aber standardmäßig bei der Server-Installation deaktiviert
Verhaltensüberwachung	Ja (32 Bit), aber standardmäßig deaktiviert	Ja (32 Bit), aber standardmäßig deaktiviert	Ja (64 Bit), aber standardmäßig deaktiviert	Ja (64 Bit), aber standardmäßig deaktiviert
	Nein (64 Bit)	Ja (64 Bit), aber standardmäßig deaktiviert		

Funktion	Windows Betriebssystem			
	Server 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
Eigenschutz des Agents für: • Registrierungsschlüssel • Prozesse	Ja (32 Bit), aber standardmäßig deaktiviert	Ja (32 Bit), aber standardmäßig deaktiviert	Ja (64 Bit), aber standardmäßig deaktiviert	Ja (64 Bit), aber standardmäßig deaktiviert
	Nein (64 Bit)	Ja (64 Bit), aber standardmäßig deaktiviert		
Eigenschutz des Agents für: • Dienste • Dateischutz	Ja	Ja	Ja	Ja
Gerätesteuerung (Der Trend Micro Unauthorized Change Prevention Service)	Ja (32 Bit), aber standardmäßig deaktiviert	Ja (32 Bit), aber standardmäßig deaktiviert	Ja (64 Bit), aber standardmäßig deaktiviert	Ja (64 Bit), aber standardmäßig deaktiviert
	Nein (64 Bit)	Ja (64 Bit), aber standardmäßig deaktiviert		
Datenschutz (einschließlich Datenschutz für die Gerätesteuerung)	Ja (32 Bit), aber standardmäßig deaktiviert	Ja (32 Bit), aber standardmäßig deaktiviert	Ja (64 Bit), aber standardmäßig deaktiviert	Ja (64 Bit), aber standardmäßig deaktiviert
	Ja (64 Bit), aber standardmäßig deaktiviert	Ja (64 Bit), aber standardmäßig deaktiviert		

Funktion	Windows Betriebssystem			
	Server 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
Verdächtige Verbindungseinstellungen	Ja	Ja	Ja	Ja
Exemplar Zusendung	Ja	Ja	Ja	Ja
POP3 mail scan	Ja	Ja	Ja	Ja
Vorausschauendes Maschinenlernen	Ja	Ja	Ja	Ja
Agent Plug-in Manager	Ja	Ja	Ja	Ja
Unabhängiger Modus	Ja	Ja (Server) Nein (Server-Kern)	Ja	Ja
Smart Feedback	Ja	Ja	Ja	Ja

Tabelle 5-3. OfficeScan Agent-Funktionen auf Desktop-Plattformen

Funktion	Windows Betriebssystem			
	XP	Windows 7	Windows 8/8.1	Windows 10
Manuelle Suche, Echtzeitsuche und zeitgesteuerte Suche	Ja	Ja	Ja	Ja

Funktion	Windows Betriebssystem			
	XP	Windows 7	Windows 8/8.1	Windows 10
Komponenten-Update (manuelles und zeitgesteuertes Update)	Ja	Ja	Ja	Ja
Update-Agent	Ja	Ja	Ja	Ja
Web Reputation	Ja	Ja	Ja, aber nur eingeschränkte Unterstützung des Windows-Benutzeroberflächenmodus	Ja
Damage Cleanup Services	Ja	Ja	Ja	Ja
OfficeScan Firewall	Ja	Ja	Ja	Ja
Verhaltensüberwachung	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit)
	Nein (64 Bit)	Ja (64 Bit)	Ja (64 Bit)	Ja (64 Bit)
Eigenschutz des Agents für: • Registrierungsschlüssel • Prozesse	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit)
	Nein (64 Bit)	Ja (64 Bit)	Ja (64 Bit)	Ja (64 Bit)
Eigenschutz des Agents für: • Dienste • Dateischutz	Ja	Ja	Ja	Ja

Funktion	Windows Betriebssystem			
	XP	Windows 7	Windows 8/8.1	Windows 10
Gerätesteuerung (Der Trend Micro Unauthorized Change Prevention Service)	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit)
	Nein (64 Bit)	Ja (64 Bit)	Ja (64 Bit)	Ja (64 Bit)
Datenschutz (einschließlich Datenschutz für die Gerätesteuerung)	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit)
	Ja (64 Bit)	Ja (64 Bit)	Ja (64 Bit), im Desktop-Modus	Ja (64 Bit)
Verdächtige Verbindungseinstellungen	Ja	Ja	Ja	Ja
Exemplar Zusendung	Ja	Ja	Ja	Ja
POP3 mail scan	Ja	Ja	Ja	Ja
Vorausschauendes Maschinenlernen	Ja	Ja	Ja	Ja
Agent Plug-in Manager	Ja	Ja	Ja	Ja
Unabhängiger Modus	Ja	Ja	Ja	Ja
Smart Feedback	Ja	Ja	Ja	Ja

OfficeScan Agent Installation und IPv6-Unterstützung

Dieses Thema befasst sich mit Fragen zur Installation des OfficeScan Agent auf Dual-Stack- oder reinen IPv6-Endpunkten.

Betriebssystem

Der OfficeScan Agent kann nur unter folgenden Betriebssystemen, die IPv6-Adressierung unterstützen, installiert werden:

- Windows Server 2008 (alle Editionen)
- Windows 7 (alle Editionen)
- Windows Server 2012 (alle Editionen)
- Windows 8/8.1 (alle Editionen)
- Windows 10 (Home, Pro, Education und Enterprise)
- Windows Server 2016 (alle Editionen)

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

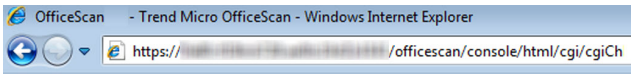
http://docs.trendmicro.com/de-de/enterprise/officescan.aspx

Installationsmethoden

Alle OfficeScan Agent-Installationsmethoden können zur Installation des OfficeScan Agents auf reinen IPv6- oder Dual-Stack-agents verwendet werden. Bei einigen Installationsmethoden gibt es besondere Voraussetzungen für die ordnungsgemäße Installation des OfficeScan Agents.

ServerProtect™ kann nicht mit dem ServerProtect Normal Server Migration Tool auf den OfficeScan Agent migriert werden, da dieses Tool die IPv6-Adressierung nicht unterstützt.

TABELLE 5-4. Installationsmethoden und IPv6-Unterstützung

INSTALLATIONSMETHODE	VORAUSSETZUNGEN/ÜBERLEGUNGEN
Installation über Webseite und Browser	Die URL zur Installationsseite enthält den Host-Namen des OfficeScan Servers oder dessen IP-Adresse.  Die Installation auf einem reinen IPv6-agent 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-agents hängt die im Installationsstatusfenster angezeigte IPv6-Adresse von der im Abschnitt **Bevorzugte IP-Adresse** unter **Agents** > **Globale Agent-Einstellungen** auf der Registerkarte **Netzwerk** ausgewählten Option ab.
Agent Packager	Bei der Ausführung des Packager Tools müssen Sie auswählen, ob Sie dem agent die Berechtigung zum Update Agent zuweisen. Denken Sie daran, dass ein reiner IPv6-Update-Agent nur an reine IPv6- oder Dual-Stack-agents Updates verteilen kann.
Einhaltung von Sicherheitsrichtlinien, Vulnerability Scanner und Remote-Installation	Ein reiner IPv6-Server kann den OfficeScan Agent nicht auf reine IPv4-Endpunkte verteilen. Ebenso kann ein reiner IPv4-Server den OfficeScan Agent nicht auf reine IPv6-Endpunkte verteilen.

Agent IP-Adressen

OfficeScan Server in einer Umgebung, die IPv6-Adressierung unterstützt, können folgende OfficeScan Agents verwalten:

- OfficeScan Server auf reinen IPv6-Host-Rechnern können reine IPv6-agents verwalten.
- OfficeScan Server auf Dual-Stack-Host-Rechnern, denen sowohl IPv4- als auch IPv6-Adressen zugewiesen wurden, können reine IPv6-, Dual-Stack- und reine IPv4-agents verwalten.

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

- Reine IPv6-agents registrieren sich mit ihrer IPv6-Adresse.
- Reine IPv4-agents registrieren sich mit ihrer IPv4-Adresse.
- Dual-Stack-agents registrieren sich entweder mit ihrer IPv4- oder mit ihrer IPv6-Adresse. Sie können auswählen, welche IP-Adresse diese agents verwenden sollen.

IP-Adresse konfigurieren, die Dual-Stack-Agents zur Registrierung beim Server verwenden

Diese Einstellung ist nur auf OfficeScan Dual-Stack-Servern verfügbar und wird nur von Dual-Stack-agents angewendet.

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Klicken Sie auf die Registerkarte **Netzwerk**.
3. Gehen Sie zum Abschnitt **Bevorzugte IP-Adresse**.
4. Wählen Sie dazu eine der folgenden Optionen aus:
   - **Nur IPv4**: Agents verwenden ihre IPv4-Adresse.
   - **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 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.

5. Klicken Sie auf **Speichern**.

Überlegungen zur Verteilung

In diesem Abschnitt finden Sie eine Zusammenfassung der verschiedenen OfficeScan Agent Installationsmethoden für eine Neuinstallation von OfficeScan Agent. Für alle Installationsmethoden sind lokale Administratorrechte auf den Zielcomputern erforderlich.

Wenn Sie bei der Installation der agents die IPv6-Unterstützung aktivieren wollen, lesen Sie die Richtlinien unter *OfficeScan Agent Installation und IPv6-Unterstützung auf Seite 5-9*.

TABELLE 5-5. Überlegungen zur Verteilung für die Installation

INSTALLATIONSMETHODE/ BETRIEBSSYSTEM UNTERSTÜTZUNG	ÜBERLEGUNGEN ZUR VERTEILUNG					
	WAN-VERTEILUNG	ZENTRALE VERWALTUNG	ERFORDERT EINGREIFEN DURCH DEN BENUTZER	ERFORDERT IT-RESSOURCE	VERTEILUNG IN HOHER ANZAHL	VERBRAUCHTE BANDBREITE
Web-Installationsseite Nicht unterstützt auf Windows Server Core-Plattformen	Nein	Nein	Ja	Nein	Nein	Hoch
E-Mail-Link-Installation Nicht unterstützt auf Windows Server Core-Plattformen	Nein	Nein	Ja	Ja	Nein	Hoch, wenn die Installationen gleichzeitig gestartet werden

Installationsmethode/ Betriebssystem unterstützung	Überlegungen zur Verteilung					
	WAN-Verteilung	Zentrale Verwaltung	Erfordert Eingreifen durch den Benutzer	Erfordert IT-Ressource	Verteilung in hoher Anzahl	Verbrauchte Bandbreite
UNC-basierte Installationen Wird unter allen Betriebssystemen unterstützt	Nein	Nein	Ja	Ja	Nein	Hoch, wenn die Installationen gleichzeitig gestartet werden
Remote-Installationen Wird auf allen Betriebssystemen unterstützt, außer: • Windows XP Home • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 (Basic-Versionen) • Windows 10 Home	Nein	Ja	Nein	Ja	Nein	Hoch

Installationsmethode/ Betriebssystem unterstützung	Überlegungen zur Verteilung					
	WAN-Verteilung	Zentrale Verwaltung	Erfordert Eingreifen durch den Benutzer	Erfordert IT-Ressource	Verteilung in hoher Anzahl	Verbrauchte Bandbreite
Anmeldeskript-Setup Wird unter allen Betriebssystemen unterstützt	Nein	Nein	Ja	Ja	Nein	Hoch, wenn die Installationen gleichzeitig gestartet werden
Agent Packager Wird unter allen Betriebssystemen unterstützt	Nein	Nein	Ja	Ja	Nein	Gering, wenn zeitgesteuert
Agent Packager (MSI-Paket, das durch Microsoft SMS verteilt wurde) Wird unter allen Betriebssystemen unterstützt	Ja	Ja	Ja/Nein	Ja	Ja	Gering, wenn zeitgesteuert
Agent Packager (MSI-Paket, das durch Active Directory verteilt wurde) Wird unter allen Betriebssystemen unterstützt	Ja	Ja	Ja/Nein	Ja	Ja	Hoch, wenn die Installationen gleichzeitig gestartet werden

Installationsmethode/ Betriebssystem unterstützung	Überlegungen zur Verteilung					
	WAN-Verteilung	Zentrale Verwaltung	Erfordert Eingreifen durch den Benutzer	Erfordert IT-Ressource	Verteilung in hoher Anzahl	Verbrauchte Bandbreite
Agent-Disk-Image Wird unter allen Betriebssystemen unterstützt	Nein	Nein	Nein	Ja	Nein	Niedrig
Trend Micro Vulnerability Scanner (TMVS) Wird auf allen Betriebssystemen unterstützt außer: • Windows XP Home • Windows 8/8.1 (Basic-Versionen) • Windows 10 Home	Nein	Ja	Nein	Ja	Nein	Hoch

Installationsmethode/ Betriebssystem unterstützung	Überlegungen zur Verteilung					
	WAN-Verteilung	Zentrale Verwaltung	Erfordert Eingreifen durch den Benutzer	Erfordert IT-Ressource	Verteilung in hoher Anzahl	Verbrauchte Bandbreite
Installationen für die Einhaltung von Sicherheitsrichtlinien Wird auf allen Betriebssystemen unterstützt, außer: • Windows XP Home • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 (Basic-Versionen) • Windows 10 Home	Nein	Ja	Nein	Ja	Nein	Hoch

Installation über die Web-Installationsseite

Prozedur

1. Öffnen Sie ein Fenster mit einem unterstützten Webbrowser und geben Sie Folgendes ein:

   ```
   https://<OfficeScan server name>:<port>/officescan
   ```

2. Klicken Sie auf der Anmeldeseite auf den **Installer**-Link, um das 32-Bit- oder 64-Bit-MSI-Paket herunterzuladen (abhängig von Ihrem Betriebssystem).

3. Nach Abschluss der Installation wird das OfficeScan Agent-Symbol in der Windows-Taskleiste angezeigt.

Hinweis

Eine Liste der Symbole in der Taskleiste finden Sie unter *OfficeScan Agent Symbole auf Seite 15-29*.

E-Mail-Link-Installation

Richten Sie eine E-Mail-Nachricht ein, in der die Benutzer eines Netzwerks angewiesen werden, den OfficeScan Agent zu installieren. Um die Installation zu starten, klicken die Benutzer auf den OfficeScan Agent-Installer-Link in der E-Mail.

Vor der Installation der OfficeScan Agents:

- überprüfen Sie die Voraussetzungen zur Installation des OfficeScan Agents.
- überprüfen Sie, welche Computer im Netzwerk zurzeit keinen Schutz vor Sicherheitsrisiken aufweisen. Führen Sie folgende Aufgaben durch:
  - Rufen Sie den Trend Micro Vulnerability Scanner auf. Mit diesem Tool werden die Endpunkte innerhalb eines angegebenen IP-Adressbereichs auf vorhandene Antiviren-Software untersucht.

    Weitere Informationen finden Sie unter *Nutzung des Vulnerability Scanners auf Seite 5-38*.
  - überprüfen Sie die Einhaltung der Sicherheitsrichtlinien.

    Weitere Informationen finden Sie unter *Einhaltung der Sicherheitsrichtlinien für nicht verwaltete Endpunkte auf Seite 15-78*.

E-Mail-Link senden

Die Installation auf einem reinen IPv6-agent 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-Agents hängt die im Installationsstatusfenster angezeigte IPv6-Adresse von der im Abschnitt **Bevorzugte IP-Adresse** unter **Agents** > **Globale Agent-Einstellungen** auf der Registerkarte **Netzwerk** ausgewählten Option ab.

Weitere Informationen finden Sie unter *Agent IP-Adressen auf Seite 5-10*.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Installation** > **Browserbasiert**.
2. ändern Sie gegebenenfalls die Betreffzeile der E-Mail.
3. Klicken Sie auf **E-Mail erstellen.**

   Das Standard-E-Mail-Programm wird geöffnet.
4. Senden Sie die E-Mail an alle beabsichtigten Empfänger.

UNC-basierte Installation durchführen

`AutoPcc.exe` ist ein eigenständiges Programm, das OfficeScan Agent auf nicht geschützten Endpunkten installiert und Programmdateien und Komponenten aktualisiert. Endpunkte müssen zur Domäne gehören, um AutoPcc mit Hilfe eines UNC-Pfads (Uniform Naming Convention) zu nutzen.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Installation** > **UNC-basiert**.
   - So installieren Sie OfficeScan Agent mit Hilfe von `AutoPcc.exe` auf einem ungeschützten Endpunkt:
     a. Stellen Sie eine Verbindung zum Servercomputer her. Navigieren Sie zum UNC-Pfad:

```
\\<Name des Server-Computers>\ofcscan
```

b. Klicken Sie mit der rechten Maustaste auf `AutoPcc.exe`, und wählen Sie **Als Administrator ausführen** aus.

- Remote-Desktop-Installation über `AutoPcc.exe`:

  a. Öffnen Sie eine Remotedesktopverbindung (Mstsc.exe) im Konsolenmodus. Dadurch wird die Installation von `AutoPcc.exe` in Sitzung 0 ausgeführt.

  b. Navigieren Sie zum Verzeichnis `\\<Name des Server-Computers>\ofcscan`, und führen Sie `AutoPcc.exe` aus.

Remote-Installation über die OfficeScan Webkonsole

Auf Netzwerkcomputern kann der OfficeScan Agent auf einem oder mehreren Computern gleichzeitig remote installiert werden. Stellen Sie sicher, dass Sie über Administratorrechte für die Ziel-Endpunkte verfügen, um die Remote-Installation durchzuführen. Bei der Remote-Installation wird der OfficeScan Agent nicht auf Endpunkten installiert, auf denen bereits der OfficeScan Server ausgeführt wird.

Hinweis

Diese Installationsmethode steht für Endpunkte unter Windows XP Home, Windows 7 Home Basic und Home Premium (32-Bit- und 64-Bit-Versionen) und Windows 8/8.1 (32-Bit- und 64-Bit-Basic-Versionen) sowie Windows 10 Home nicht zur Verfügung. Ein reiner IPv6-Server kann den OfficeScan Agent nicht auf reine IPv4-Agents verteilen. Ebenso kann ein reiner IPv4-Server den OfficeScan Agent nicht auf reine IPv6-Agents verteilen.

Prozedur

1. Führen Sie die folgenden Schritte zur Vorbereitung der Installation für Ihre Windows Version durch.

   - Bei Ausführung von Windows XP:

     a. Aktivieren Sie ein integriertes Domänenadministratorkonto und richten Sie das Kennwort für das Konto ein.

b. Navigieren Sie auf dem Endpunkt zur Registerkarte **Arbeitsplatz** > **Tools** > **Ordneroptionen** > **Ansicht** und deaktivieren Sie die Option **Einfache Dateifreigabe verwenden**.

c. Navigieren Sie zur Registerkarte **Start** > **Programme** > **Windows Firewall** > **Ausnahmen** und aktivieren Sie die Option **Datei- und Druckerfreigabe**.

d. Öffnen Sie die Microsoft Management-Konsole (klicken Sie auf **Start** > **Ausführen** und geben Sie `services.msc` ein) und starten Sie die Dienste **Remote-Registrierung** und **Remote-Prozessaufruf**. Installieren Sie den OfficeScan Agent mit dem integrierten Administratorkonto und -kennwort.

- Bei Ausführung von Windows 7, Windows 8 (Pro, Enterprise), Windows 8.1, Windows 10 (Pro, Education, Enterprise) oder Windows Server 2012/2016:

  a. Aktivieren Sie ein integriertes Domänenadministratorkonto und richten Sie das Kennwort für das Konto ein.

  b. Navigieren Sie zu **Start** > **Programme** > **Verwaltung** > **Windows-Firewall mit erweiterter Sicherheit**.

  c. Aktivieren Sie je nach Netzwerkumgebung **Datei- und Druckerfreigabe**-Regeln für „Domäne“, „Privat“ bzw. „Öffentlich“.

  d. Öffnen Sie die Microsoft Management-Konsole (klicken Sie auf **Start** > **Ausführen** und geben Sie `services.msc` ein) und starten Sie die Dienste **Remote-Registrierung** und **Remote-Prozessaufruf**. Installieren Sie den OfficeScan Agent mit dem integrierten Administratorkonto und -kennwort.

2. Navigieren Sie auf der Webkonsole zu **Agents** > **Agent-Installation** > **Remote**.

3. Wählen Sie die Ziel-Endpunkte aus.

   - In der Liste **Domänen und Endpunkte** werden alle Windows Domänen im Netzwerk angezeigt. Doppelklicken Sie auf einen Domänennamen, um die Endpunkte einer bestimmten Domäne anzuzeigen. Wählen Sie einen Endpunkt, und klicken Sie anschließend auf **Hinzufügen**.

- Geben Sie den Endpunktnamen in das Feld **Nach Endpunkten suchen** oben auf der Seite ein, und drücken Sie die EINGABETASTE, um nach einem bestimmten Endpunktnamen zu suchen.

OfficeScan fordert Sie auf, für den Zielendpunkt einen Benutzernamen und ein Kennwort einzugeben. Verwenden Sie den Benutzernamen und das Kennwort eines Administratorkontos, um den Vorgang fortzusetzen.

4. Geben Sie Ihren Benutzernamen und das Kennwort ein, und klicken Sie dann auf **Anmelden**.

   Der Zielendpunkt wird in der Tabelle **Ausgewählte Endpunkte** angezeigt.

5. Wiederholen Sie die Schritte 3 und 4, um weitere Endpunkte hinzuzufügen.

6. Klicken Sie auf **Installieren**, wenn Sie alle Einstellungen zur Installation des OfficeScan Agents auf den Ziel-Endpunkten vorgenommen haben.

   Ein Bestätigungsfenster wird angezeigt.

7. Klicken Sie auf **Ja**, um die OfficeScan Agent-Installation auf den Ziel-Endpunkten zu bestätigen.

   Während die Programmdateien auf die jeweiligen Zielendpunkte kopiert werden, wird ein Fortschrittsfenster angezeigt.

Wenn OfficeScan die Installation auf einem Zielendpunkt abgeschlossen hat, wird der Name des Endpunkts aus der Liste **Ausgewählte Endpunkte** entfernt und in der Liste **Domänen und Endpunkte** mit einem roten Häkchen angezeigt.

Wenn alle Ziel-Endpunkte in der Liste **Domänen und Endpunkte** mit einem roten Häkchen versehen sind, ist die Remote-Installation abgeschlossen.

Hinweis

Wenn Sie die Installation auf mehreren Endpunkten durchführen, wird im Falle eines fehlgeschlagenen Installationsvorgangs ein Protokolleintrag von OfficeScan erstellt (weitere Informationen hierzu finden Sie unter *Erstinstallations-Protokolle auf Seite 18-16*). Die Installation auf den übrigen Computern bleibt davon unbeeinflusst. Die Installation wird durch Klicken auf **Installieren** gestartet und anschließend vollständig automatisch ausgeführt. Überprüfen Sie die Protokolle zu einem späteren Zeitpunkt, um das Ergebnis der Installation einzusehen.

Mit Anmeldeskript-Setup installieren

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

`AutoPcc.exe` installiert den OfficeScan Agent auf nicht verwalteten Endpunkten und aktualisiert Programmdateien und Komponenten. Endpunkte muss Teil der Domäne sein, um AutoPcc über das Anmeldeskript verwenden zu können.

OfficeScan Agent-Installation

`AutoPcc.exe` installiert den OfficeScan Agent automatisch auf einem ungeschützten Endpunkt unter Windows Server 2003, wenn sich der Endpunkt an dem Server anmeldet, dessen Anmeldeskripts von Ihnen geändert wurden. `AutoPcc.exe` installiert den OfficeScan Agent auf Computern unter Windows 7, 8, 8.1, 10, Server 2008, Server 2012 und Server 2016 jedoch nicht automatisch. Die Benutzer müssen eine Verbindung zum Server-Computer herstellen, dann zum Verzeichnis `\\<Name des Server-Computers>\ofcscan` wechseln, mit der rechten Maustaste auf `AutoPcc.exe` klicken und anschließend **Als Administrator ausführen** wählen.

Remote-Desktop-Installation über `AutoPcc.exe`:

- Der Endpunkt muss im Modus `Mstsc.exe /console` ausgeführt werden. Dadurch wird die Installation von `AutoPcc.exe` in Sitzung 0 ausgeführt.

- Ordnen Sie dem Ordner "ofcscan" ein Laufwerk zu, und führen Sie `AutoPcc.exe` von dort aus.

Programm- und Komponenten-Updates

`AutoPcc.exe` aktualisiert die Programmdateien und die Komponenten des Virenschutzes, der Anti-Spyware und der Damage Cleanup Services.

Windows Server-Skripte

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

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

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

Wobei gilt:

- `<Server_name>` ist der Name des Endpunkts oder die IP-Adresse des OfficeScan Servers.
- "`ofcscan`" ist der Name des Freigabeordners von OfficeScan auf dem Server.
- "`autopcc`" ist der Link zur ausführbaren Datei "autopcc", die den OfficeScan Agent installiert.

Speicherort des Anmeldeskripts (durch ein über die Netzwerkanmeldung freigegebenes Verzeichnis):

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

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

Die Datei "Autopcc.exe" mit Hilfe des Anmeldeskript-Setups zum Anmeldeskript hinzufügen

Prozedur

1. Klicken Sie auf dem Endpunkt, auf dem die Server-Installation ausgeführt wurde, im Windows Start-Menü auf **Programme** > **Trend Micro OfficeScan Server <Servername>** > **Anmeldeskript-Setup**.

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

2. 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.

3. Geben Sie den Benutzernamen und das Kennwort ein. Klicken Sie zum Fortfahren auf **OK**.

   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.

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

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

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

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

8. 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.

9. Klicken Sie auf **OK**.

   Das Eingangsfenster des Anmeldeskript-Setups wird wieder angezeigt.

10. Wiederholen Sie die Schritte 2 bis 4, um das Anmeldeskript anderer Server zu ändern.

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

Installation mit Agent Packager

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

Agent Packager ist besonders nützlich bei der Verteilung des OfficeScan Agent oder von Komponenten auf Endpunkte in externen Büros mit geringer Bandbreite. OfficeScan Agents, die mit Agent Packager installiert werden, berichten an den Server, auf dem das Setup-Paket erstellt wurde.

Agent Packager benötigt Folgendes:

- 800MB verfügbaren Festplattenspeicher
- Windows Installer 2.0 (zur Ausführung eines MSI-Pakets)

Richtlinien für die Paketverteilung

1. Senden Sie das Paket an die Benutzer, und fordern Sie sie auf, das OfficeScan Agent-Paket mit einem Doppelklick auf die `EXE`- oder `MSI`-Datei auf ihren Endpunkten auszuführen.

Hinweis

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

2. Fordern Sie Benutzer, die das `EXE`-Paket auf Endpunkten unter Windows Server 2008, 7, 8, 8.1, 10, Server 2012 oder Server 2016 installieren möchten, dazu auf, mit der rechten Maustaste auf die `EXE`-Datei zu klicken und **Als Administrator ausführen** auszuwählen.

3. Wenn Sie eine `MSI`-Datei erstellt haben, verteilen Sie das Paket, indem Sie die folgenden Aufgaben durchführen:

   - Verwenden Sie Active Directory oder Microsoft SMS.

     Weitere Informationen finden Sie unter *Ein MSI-Paket über Active Directory verteilen auf Seite 5-31* oder *Ein MSI-Paket über Microsoft SMS verteilen auf Seite 5-33*.

4. Starten Sie das MSI-Paket über die Eingabeaufforderung, um den OfficeScan Agent unbeaufsichtigt auf einem Remote-Endpunkt unter Windows XP, Server 2008, 7, 8, 8.1, 10, Server 2012 oder Server 2016 zu installieren.

Suchmethodenrichtlinien für Agent Pakete

Wählen Sie für das Paket die Suchmethode aus. Weitere Informationen finden Sie unter *Suchmethodentypen auf Seite 7-9*.

Welche Komponenten im Paket enthalten sind, hängt von der ausgewählten Suchmethode ab. Weitere Informationen über Komponenten, die für jede einzelne Suchmethode zur Verfügung stehen, finden Sie unter *OfficeScan Agent-Updates auf Seite 6-29*.

Lesen Sie vor der Auswahl der Suchmethode die folgenden Richtlinien, die Ihnen bei der effizienten Verteilung des Pakets helfen sollen:

- Wenn Sie mit dem Paket den agent auf diese OfficeScan Version aktualisieren, überprüfen Sie auf der Webkonsole die Suchmethode auf Domänenebene. Navigieren Sie auf der Konsole zur **Agents** > **Agent-Verwaltung**, wählen Sie die Domäne der agent-Hierarchie, zu der der agent gehört, und klicken Sie auf

Einstellungen > **Sucheinstellungen** > **Suchmethoden**. Die Suchmethode auf Domänenebene sollte der Suchmethode für das Paket entsprechen.

- Wenn Sie mit dem Paket eine Neuinstallation des OfficeScan Agent durchführen möchten, aktivieren Sie die Einstellung für die agent-Gruppierung. Navigieren Sie auf der Webkonsole zu **Agents** > **Agent-Gruppierung**.
- Wenn für die agent-Gruppierung NetBIOS, Active Directory oder eine DNS-Domäne verwendet wird, prüfen Sie die Domäne, zu der der Ziel-Endpunkt gehört. Wenn die Domäne vorhanden ist, aktivieren Sie die Suchmethode, die für die Domäne konfiguriert ist. Wenn die Domäne nicht vorhanden ist, überprüfen Sie die Suchmethode auf Root-Ebene (wählen Sie das Root-Domänen-Symbol ( ) in der agent-Hierarchie, und klicken Sie auf **Einstellungen** > **Sucheinstellungen** > **Suchmethoden**). Die Suchmethode auf Domänen-Stammebene sollte der Suchmethode für das Paket entsprechen.
- Wenn die agent-Gruppierung durch benutzerdefinierte agent-Gruppen realisiert wurde, prüfen Sie die **Priorität für die Gruppierung** und die **Quelle**.

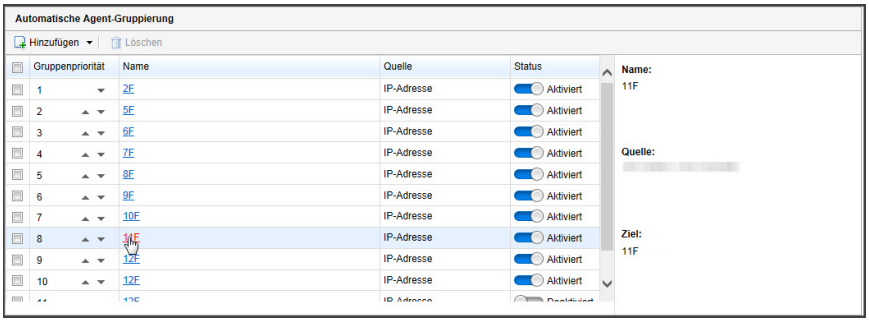


ABBILDUNG 5-1. Fensterbereich "Vorschau" für die automatische Agent-Gruppierung

Wenn der Ziel-Endpunkt zu einer bestimmten Quelle gehört, überprüfen Sie das entsprechende **Ziel**. Beim Ziel handelt es sich um den Domänennamen, der in der agent-Hierarchie angezeigt wird. Nach der Installation wendet der agent die Suchmethode für diese Domäne an.

- Wenn Sie mit dem Paket Komponenten auf dem agent aktualisieren, die diese OfficeScan Version verwenden, aktivieren Sie die Suchmethode, die für die

Domäne in der agent-Hierarchie konfiguriert ist, zu der der agent gehört. Die Suchmethode auf Domänenebene sollte der Suchmethode für das Paket entsprechen.

Ein Installationspaket mit Agent Packager erstellen

Prozedur

1. Navigieren Sie auf dem OfficeScan Server-Computer zu <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\ClientPackager`.
2. Doppelklicken Sie auf die Datei `ClnPack.exe`, um das Tool auszuführen.

   Die **Agent Packager** Konsole wird geöffnet.
3. Wählen Sie aus, welche Art von Paket Sie erstellen möchten.

TABELLE 5-6. Agent-Paketarten

PACKETTYP	BESCHREIBUNG
Setup	Wählen Sie **Setup** , um das Paket als ausführbare Datei zu erstellen. Das Paket installiert das OfficeScan Agent-Programm mit den Komponenten, die gegenwärtig auf dem Server verfügbar sind. Wenn auf dem Ziel-Endpunkt bereits eine frühere Version des agents installiert ist, können Sie den agent mit Hilfe der ausführbaren Datei aktualisieren.
Update	Wählen Sie **Update**, um ein Paket zu erstellen, das die Komponenten enthält, die gegenwärtig auf dem Server verfügbar sind. Das Paket wird anschließend als ausführbare Datei erstellt. Verwenden Sie dieses Paket, wenn bei der Aktualisierung von Komponenten auf einem agent-Endpunkt Probleme auftreten.
MSI	Wählen Sie **MSI**, um ein Paket zu erstellen, das dem Paketformat von Microsoft Installer entspricht. Das Paket installiert auch das OfficeScan Agent-Programm mit den Komponenten, die gegenwärtig auf dem Server verfügbar sind. Wenn auf dem Ziel-Endpunkt bereits eine frühere Version des agents installiert ist, können Sie den agent mit Hilfe der MSI-Datei aktualisieren.

4. Wählen Sie das Betriebssystem, für das Sie das Paket erstellen möchten. Verteilen Sie das Paket nur auf Endpunkte mit dem richtigen Betriebssystem. Erstellen Sie ein anderes Paket, um es an ein anderes Betriebssystem zu verteilen.

5. Wählen Sie die Suchmethode aus, mit der das agent-Paket verteilt wird.

   Richtlinien zur Auswahl einer Suchmethode finden Sie unter *Suchmethodenrichtlinien für Agent Pakete auf Seite 5-26*.

6. Wählen Sie unter **Domäne** eine der folgenden Optionen:

   - **Agent kann seine Domäne automatisch melden**: Nach der Installation des OfficeScan Agents führt der agent eine Abfrage der OfficeScan Server-Datenbank durch und meldet die Domäneneinstellungen an den Server.
   - Beliebige Domäne in der Liste: Agent Packager wird mit dem OfficeScan Server synchronisiert und listet die aktuell verwendeten Domänen in der agent-Hierarchie auf.

7. Wählen Sie unter **Optionen** eine der folgenden Optionen:

OPTION	BEZEICHNUNG
Unbeaufsichtigter Modus	Diese Option erstellt ein Paket, das auf dem agent Endpunkt im Hintergrund, für den agent nicht sichtbar und ohne Anzeige des Installationsfortschritts, angezeigt wird. Aktivieren Sie diese Option, wenn Sie planen, das Paket remote auf den Ziel-Endpunkt zu verteilen.
Überschreiben mit neuester Version erzwingen	Diese Option überschreibt die Komponentenversionen auf dem agent mit den Versionen, die gegenwärtig auf dem Server verfügbar sind. Aktivieren Sie diese Option, um sicherzustellen, dass die Komponenten auf dem Server und agent synchron sind.
Virensuche vor der Installation deaktivieren (nur bei Neuinstallationen)	Wenn auf dem Ziel-Endpunkt kein OfficeScan Agent installiert ist, durchsucht das Paket zunächst den Endpunkt nach Sicherheitsrisiken, bevor der OfficeScan Agent installiert wird. Wenn Sie sicher sind, dass der Ziel-Endpunkt nicht mit Sicherheitsrisiken infiziert ist, deaktivieren Sie die Virensuche vor der Installation.

OPTION	BEZEICHNUNG
	Wenn die Virensuche vor der Installation aktiviert ist, führt Setup eine Suche nach Viren/Malware in den anfälligsten Bereichen des Endpunkts durch, wie beispielsweise: • Boot-Bereich und das Boot-Verzeichnis (Suche nach Boot-Viren) • Windows Ordner • Ordner "Programme"

8. Wählen Sie unter **Update-Agent-Funktionen** die Funktionen aus, die vom Update-Agent verteilt werden können.

9. Wählen Sie unter **Komponenten** die Komponenten und Funktionen für das Paket aus.

   - Weitere Informationen zu Komponenten finden Sie unter *OfficeScan Komponenten und Programme auf Seite 6-2*.
   - Das Datenschutzmodul ist nur verfügbar, wenn Sie den Datenschutz installieren und aktivieren. Weitere Informationen zum Datenschutz finden Sie unter *Erste Schritte mit Datenschutz auf Seite 3-1*.

10. Stellen Sie im Feld neben **Quelldatei** sicher, dass der Speicherort der Datei `ofcscan.ini` richtig angegeben wurde. Klicken Sie auf (...), um zur Datei `ofcscan.ini` zu navigieren und den Pfad zu ändern.

    Standardmäßig befindet sich diese Datei unter `<Installationsordner des Servers>\PCCSRV` auf dem OfficeScan Server.

11. Klicken Sie unter **Ausgabedatei** auf (...), um anzugeben, wo das OfficeScan Agent-Paket erstellt werden soll, und geben Sie den Namen der Paketdatei an (z. B. `AgentSetup.exe`).

12. 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.

13. Verteilen Sie das Paket.

Ein MSI-Paket über Active Directory verteilen

Sie können mit Hilfe von Active Directory das MSI-Paket gleichzeitig auf mehrere agent-Endpunkte verteilen.

Informationen über die Erstellung einer MSI-Datei finden Sie unter *Installation mit Agent Packager auf Seite 5-25*.

Prozedur

1. Führen Sie Folgendes aus:
   - Für Windows Server 2003 und frühere Versionen:
     a. Öffnen Sie die Active Directory Konsole.
     b. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, in der Sie das MSI-Paket installieren möchten, und klicken Sie dann auf **Eigenschaften**.
     c. Klicken Sie auf der Registerkarte **Gruppenrichtlinie** auf **Neu**.
   - Bei Windows Server 2008 und Windows Server 2008 R2:
     a. Öffnen Sie die **Gruppenrichtlinien-Verwaltungskonsole**. Klicken Sie auf **Start** > **Systemsteuerung** > **Verwaltung** > **Gruppenrichtlinienverwaltung**.
     b. Erweitern Sie in der Konsolenstruktur **Gruppenrichtlinienobjekte** in der Gesamtstruktur und der Domäne mit dem GPO, das bearbeitet werden soll.
     c. Klicken Sie mit der rechten Maustaste auf das GPO, die bearbeitet werden soll, und klicken Sie anschließend auf **Bearbeiten**. Daraufhin wird der **Gruppenrichtlinienobjekt-Editor** geöffnet.
   - Für Windows Server 2012 und Windows Server 2016:

a. Öffnen Sie die **Gruppenrichtlinien-Verwaltungskonsole**. Klicken Sie auf **Serververwaltung** > **Tools** > **Gruppenrichtlinienverwaltung**.

b. Erweitern Sie in der Konsolenstruktur **Gruppenrichtlinienobjekte** in der Gesamtstruktur und der Domäne mit dem GPO, das bearbeitet werden soll.

c. Klicken Sie mit der rechten Maustaste auf das GPO, die bearbeitet werden soll, und klicken Sie anschließend auf **Bearbeiten**. Daraufhin wird der **Gruppenrichtlinienobjekt-Editor** geöffnet.

2. Wählen Sie zwischen **Computer-Konfiguration** und **Benutzerkonfiguration**, und öffnen Sie darunter **Softwareeinstellungen**.

Tipp

Trend Micro empfiehlt, **Computer-Konfiguration** und nicht **Benutzerkonfiguration** zu verwenden, damit das MSI-Paket unabhängig von dem am Endpunkt angemeldeten Benutzer ordnungsgemäß installiert wird.

3. Klicken Sie unter **Softwareeinstellungen** mit der rechten Maustaste auf **Softwareinstallation**, und wählen Sie dann **Neu** und **Paket** aus.

4. Wählen Sie das MSI-Paket aus.

5. Wählen Sie eine Installationsmethode aus, und klicken Sie auf **OK**.

- **Zugewiesen**: Das MSI-Paket wird automatisch installiert, wenn sich ein Benutzer das nächste Mal am Endpunkt anmeldet (bei Auswahl von Benutzerkonfiguration) oder wenn der Endpunkt neu gestartet wird (bei Auswahl von Computer-Konfiguration). Bei dieser Methode ist kein Eingreifen des Benutzers erforderlich.

- **Veröffentlicht**: Weisen Sie die Benutzer an, in der Systemsteuerung die Option "Software" und anschließend die Option, mit der Programme im Netzwerk installiert/hinzugefügt werden, auszuwählen, um das MSI-Paket zu installieren. Wenn das MSI-Paket des OfficeScan Agent Agents angezeigt wird, kann die Installation des OfficeScan Agent fortgesetzt werden.

Ein MSI-Paket über Microsoft SMS verteilen

Sie können das MSI-Paket mit Hilfe von Microsoft System Management Server (SMS) verteilen, wenn Microsoft BackOffice SMS auf dem Server installiert ist.

Informationen über die Erstellung einer MSI-Datei finden Sie unter *Installation mit Agent Packager auf Seite 5-25*.

Der SMS Server muss die MSI-Datei vom OfficeScan Server erhalten, bevor das Paket auf den Ziel-Endpunkten verteilt werden kann.

- Lokal: Der SMS Server und der OfficeScan Server befinden sich auf demselben Endpunkt.
- Remote: Der SMS Server und der OfficeScan Server befinden sich auf verschiedenen Endpunkten.

Bekannte Probleme bei der Installation mit Microsoft SMS:

- In der Spalte **Laufzeit** der SMS Konsole wird „Unbekannt“ angezeigt.
- Falls die Installation fehlschlägt, wird der Installationsstatus im SMS Programmmonitor unter Umständen weiterhin als abgeschlossen angezeigt.

  Hinweise zur Überprüfung, ob eine Installation erfolgreich war, finden Sie unter *Nach der Installation auf Seite 5-71*.

Beachten Sie die folgenden Anweisungen bei der Verwendung von Microsoft SMS 2.0 und 2003.

Das Paket lokal erhalten

Prozedur

1. Öffnen Sie die **SMS Administrator**-Konsole.
2. Klicken Sie auf der Registerkarte **Struktur** auf **Pakete**.
3. Klicken Sie im Menü **Aktion** auf **Neu** > **Paket aus einer Definition**.

   Das **Begrüßungsfenster** des **Assistenten für die Erstellung eines Pakets aus einer Definition** wird angezeigt.

4. Klicken Sie auf **Weiter**.

   Das Fenster **Paketdefinition** wird angezeigt.

5. Klicken Sie auf **Durchsuchen**.

   Das Fenster **Öffnen** wird angezeigt.

6. Wählen Sie die von Agent Packager erstellte MSI-Paketdatei aus, und klicken Sie dann auf **Öffnen**.

   Der Name des MSI-Pakets wird im Fenster **Paketdefinition** angezeigt. Im Paketnamen ist neben "OfficeScan Agent" auch die Programmversion angegeben.

7. Klicken Sie auf **Weiter**.

   Das Fenster **Quelldateien** wird angezeigt.

8. Klicken Sie auf **Dateien immer aus einem Quellverzeichnis abrufen**, und klicken Sie dann auf **Weiter**.

   Das Fenster **Quellverzeichnis** wird angezeigt. Es enthält den Namen des zu erstellenden Pakets und das Quellverzeichnis.

9. Klicken Sie auf **Lokales Laufwerk auf Standort-Server**.

10. Klicken Sie auf **Durchsuchen**, und wählen Sie das Quellverzeichnis, in dem sich die MSI-Datei befindet.

11. Klicken Sie auf **Weiter**.

    Der Assistent erstellt das Paket. Nach Abschluss des Vorgangs wird der Name des Pakets auf der **SMS Administrator**-Konsole angezeigt.

Das Paket remote erhalten

Prozedur

1. Verwenden Sie auf dem OfficeScan Server Agent Packager, um ein Setup-Paket mit einer `EXE`-Erweiterung zu erstellen (ein `MSI`-Paket kann nicht erstellt werden). Weitere Informationen finden Sie unter *Installation mit Agent Packager auf Seite 5-25*.

2. Erstellen Sie einen Freigabeordner auf dem Endpunkt, auf dem die Quelle gespeichert werden soll.

3. Öffnen Sie die SMS Administratorkonsole.

4. Klicken Sie auf der Registerkarte **Struktur** auf **Pakete**.

5. Klicken Sie im Menü **Aktion** auf **Neu** > **Paket aus einer Definition**.

   Das **Begrüßungsfenster** des **Assistenten für die Erstellung eines Pakets aus einer Definition** wird angezeigt.

6. Klicken Sie auf **Weiter**.

   Das Fenster **Paketdefinition** wird angezeigt.

7. Klicken Sie auf **Durchsuchen**.

   Das Fenster **Öffnen** wird angezeigt.

8. Suchen Sie nach der MSI-Paketdatei. Die Datei befindet sich in dem von Ihnen erstellten Freigabeordner.

9. Klicken Sie auf **Weiter**.

   Das Fenster **Quelldateien** wird angezeigt.

10. Klicken Sie auf **Dateien immer aus einem Quellverzeichnis abrufen**, und klicken Sie dann auf **Weiter**.

    Das Fenster **Quellverzeichnis** wird angezeigt.

11. Klicken Sie auf **Netzwerkpfad (UNC-Name)**.

12. Klicken Sie auf **Durchsuchen**, und wählen Sie das Quellverzeichnis, in dem sich die MSI-Datei befindet (der von Ihnen erstellte Freigabeordner).

13. Klicken Sie auf **Weiter**.

    Der Assistent erstellt das Paket. Nach Abschluss des Vorgangs wird der Name des Pakets auf der **SMS Administrator**-Konsole angezeigt.

Das Paket an die Ziel-Endpunkte verteilen

Prozedur

1. Klicken Sie auf der Registerkarte **Struktur** auf **Ankündigungen**.
2. Klicken Sie im Menü **Aktion** auf **Alle Tasks** > **Software verteilen**.

   Das Fenster **Willkommen** des **Assistenten für die Softwareverteilung** wird geöffnet.
3. Klicken Sie auf **Weiter**.

   Das Fenster **Paket** wird angezeigt.
4. Klicken Sie auf **Vorhandenes Paket verteilen** und dann auf den Namen des von Ihnen erstellten Setup-Pakets.
5. Klicken Sie auf **Weiter**.

   Das Fenster **Verteilungspunkte** wird angezeigt.
6. Wählen Sie einen Verteilungspunkt, an den das Paket kopiert werden soll, und klicken Sie dann auf **Weiter**.

   Das Fenster **Programm ankündigen** wird angezeigt.
7. Klicken Sie auf **Ja**, um das OfficeScan Agent-Installationspaket anzukündigen, und klicken Sie dann auf **Weiter**.

   Das Fenster **Ankündigungsziel** wird angezeigt.
8. Klicken Sie auf **Durchsuchen**, um die Ziel-Endpunkte auszuwählen.

   Das Fenster **Sammlung durchsuchen** wird angezeigt.
9. Klicken Sie auf **Alle Windows NT Systeme**.
10. Klicken Sie auf **OK**.

    Das Fenster **Ankündigungsziel** wird erneut angezeigt.
11. Klicken Sie auf **Weiter**.

    Das Fenster **Ankündigungsname** wird angezeigt.

12. Geben Sie eine Bezeichnung für die Ankündigung und Anmerkungen in die entsprechenden Felder ein, und klicken Sie dann auf **Weiter**.

    Das Fenster **Untersammlungen ankündigen** wird angezeigt.

13. Wählen Sie aus, ob das Paket an Untersammlungen angekündigt werden soll. Sie können das Programm nur Mitgliedern der angegebenen Sammlung ankündigen oder das Programm auch den Mitgliedern von Untersammlungen ankündigen.

14. Klicken Sie auf **Weiter**.

    Das Fenster **Ankündigungszeitplan** wird angezeigt.

15. Geben Sie an, wann das OfficeScan Agent-Installationspaket angekündigt werden soll, indem Sie das Datum und die Uhrzeit eingeben bzw. auswählen.

    Hinweis

    Wenn Microsoft SMS das Paket nur bis zu einem bestimmten Tag ankündigen soll, klicken Sie auf **Ja** , und geben Sie nach Ablauf der Ankündigung das Datum und die Uhrzeit in das Feld **Ablaufdatum und -zeitpunkt** ein.

16. Klicken Sie auf **Weiter**.

    Das Fenster **Programm zuordnen** wird angezeigt.

17. Klicken Sie auf **Programm zuordnen** und anschließend auf **Weiter**.

    Microsoft SMS erstellt die Ankündigung und zeigt sie auf der SMS-Administratorkonsole an.

18. Wenn Microsoft SMS das angekündigte Programm, d. h. den OfficeScan Agent, auf die Ziel-Endpunkte verteilt, wird auf jedem Ziel-Endpunkt ein Fenster angezeigt. Weisen Sie die Benutzer an, auf **Ja** zu klicken und den Anweisungen des Assistenten für die Installation des OfficeScan Agent auf ihren Endpunkten zu folgen.

Installation mit Hilfe von Agent-Disk-Images

Mit der Disk-Image-Technologie können Sie ein Image des OfficeScan Agents erstellen und damit die Agent-Software auf anderen Computern im Netzwerk installieren.

Für jede OfficeScan Agent-Installation ist eine GUID (Globally Unique Identifier) erforderlich, damit der Server die agents eindeutig identifizieren kann. Verwenden Sie das OfficeScan Programm `ImgSetup.exe`, um für jeden Klon eine eigene GUID-Nummer zu erstellen.

Ein Disk-Image des OfficeScan Agent erstellen

Prozedur

1. Installieren Sie den OfficeScan Agent auf dem Endpunkt.
2. Kopieren Sie `ImgSetup.exe` von <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\ImgSetup` auf diesen Endpunkt.
3. Starten Sie `ImgSetup.exe` auf diesem Endpunkt.

   Hiermit wird der Registrierungsschlüssel `RUN` unter `HKEY_LOCAL_MACHINE` erstellt.
4. Erstellen Sie mit Hilfe der Imaging-Software ein Image des OfficeScan Agents.
5. Starten Sie den Klon neu.

   `ImgSetup.exe` wird automatisch gestartet. Dabei wird neuer GUID-Wert erstellt. Der OfficeScan Agent meldet den neuen GUID an den Server, und der Server erstellt einen neuen Eintrag für den neuen OfficeScan Agent.

Warnung!

Um zu vermeiden, dass in der OfficeScan Datenbank zwei Computer mit demselben Namen gespeichert sind, müssen Sie den Endpunkt- oder Domänennamen des geklonten OfficeScan Agents manuell ändern.

Nutzung des Vulnerability Scanners

Der Vulnerability Scanner erkennt installierte Antiviren-Programme, sucht nach ungeschützten Computern im Netzwerk und installiert OfficeScan Agents auf diesen Computern.

überlegungen zur Verwendung des Vulnerability Scanners

Um Ihnen bei der Entscheidung zu helfen, ob Sie den Vulnerability Scanner verwenden sollten, bedenken Sie das Folgende:

- *Netzwerkadministration auf Seite 5-39*
- *Netzwerktopologie und -architektur auf Seite 5-40*
- *Software/Hardware-Spezifikationen auf Seite 5-40*
- *Domänenstruktur auf Seite 5-41*
- *Netzwerkdatenverkehr auf Seite 5-41*
- *Netzwerkgröße auf Seite 5-42*

Netzwerkadministration

TABELLE 5-7. Netzwerkadministration

SETUP	EFFEKTIVITÄT DES VULNERABILITY SCANNERS
Administration mit strengen Sicherheitsrichtlinien	Sehr effektiv. Der Vulnerability Scanner meldet, ob auf allen Computern eine Antiviren-Software installiert ist.
Administrative Verantwortung wird auf verschiedene Standorte verteilt	Moderat effektiv
Zentralisierte Administration	Moderat effektiv
Ausgelagerte Dienstleistungen	Moderat effektiv
Benutzer verwalten ihre eigenen Computer	Nicht effektiv. Weil der Vulnerability Scanner im Netzwerk überprüft, ob eine Antiviren-Installation vorhanden ist, ist es nicht machbar, dass Benutzer ihre eigenen Computer durchsuchen.

Netzwerktopologie und -architektur

TABELLE 5-8. Netzwerktopologie und -architektur

SETUP	EFFEKTIVITÄT DES VULNERABILITY SCANNERS
Einzelner Standort	Sehr effektiv. Mit dem Vulnerability Scanner können Sie ein gesamtes IP-Segment durchsuchen und den OfficeScan Agent problemlos im LAN installieren.
Mehrere Standorte mit Hochgeschwindigkeitsverbindung	Moderat effektiv
Mehrere Standorte mit einer langsamen Datenverbindung	Nicht effektiv. Sie müssen den Vulnerability Scanner an jedem Standort ausführen und die OfficeScan Agent-Installation muss an einen lokalen OfficeScan Server geleitet werden.
Remote- und isolierte Computer	Moderat effektiv

Software/Hardware-Spezifikationen

TABELLE 5-9. Software/Hardware-Spezifikationen

SETUP	EFFEKTIVITÄT DES VULNERABILITY SCANNERS
Windows NT-basierte Betriebssysteme	Sehr effektiv. Der Vulnerability Scanner kann ohne großen Aufwand den OfficeScan Agent remote auf Computern installieren, auf denen ein Windows NT-basiertes Betriebssystem ausgeführt wird.
Gemischte Betriebssysteme	Moderat effektiv Der Vulnerability Scanner kann nur auf Computern installiert werden, auf denen ein Windows NT-basiertes Betriebssystem ausgeführt wird.
Desktop-Management-Software	Nicht effektiv. Der Vulnerability Scanner kann nicht zusammen mit Desktop-Management-Software verwendet werden. Diese Software kann jedoch dazu beitragen, den Fortschritt der OfficeScan Agent-Installation zu verfolgen.

Domänenstruktur

TABELLE 5-10. Domänenstruktur

SETUP	EFFEKTIVITÄT DES VULNERABILITY SCANNERS
Microsoft Active Directory	Sehr effektiv. Durch die Angabe des Kontos für den Domänenadministrator im Vulnerability Scanner können Sie die Remote-Installation des OfficeScan Agents zulassen.
Workgroup	Nicht effektiv. Vulnerability Scanner kann Schwierigkeiten bei der Installation auf Computern haben, wenn verschiedene Administratorkonten und Kennwörter verwendet werden.
Novell™ Directory Service	Nicht effektiv. Der Vulnerability Scanner setzt ein Windows Domänenkonto für die Installation des OfficeScan Agents voraus.
Peer-to-peer	Nicht effektiv. Vulnerability Scanner kann Schwierigkeiten bei der Installation auf Computern haben, wenn verschiedene Administratorkonten und Kennwörter verwendet werden.

Netzwerkdatenverkehr

TABELLE 5-11. Netzwerkdatenverkehr

SETUP	EFFEKTIVITÄT DES VULNERABILITY SCANNERS
LAN-Verbindung	Sehr effektiv
512 KBit/s	Moderat effektiv
T1-Verbindung und höher	Moderat effektiv
Einwählverbindung	Nicht effektiv. Es dauert sehr lange, bis die Installation von OfficeScan Agent abgeschlossen ist.

Netzwerkgröße

TABELLE 5-12. Netzwerkgröße

SETUP	EFFEKTIVITÄT DES VULNERABILITY SCANNERS
Sehr großes Unternehmen	Sehr effektiv. Je größer das Netzwerk ist, desto notwendiger ist Vulnerability Scanner, um die OfficeScan Agent-Installationen zu überprüfen.
Kleine und mittlere Unternehmen	Moderat effektiv Bei kleinen Netzwerken kann der Vulnerability Scanner eine Möglichkeit zur Installation von OfficeScan Agent sein. Andere OfficeScan Agent-Installationsmethoden können unter Umständen leichter implementiert werden.

Richtlinien für die Installation des OfficeScan Agents mit Hilfe von Vulnerability Scanner

Vulnerability Scanner installiert den OfficeScan Agent nicht, wenn:

- Der OfficeScan Server oder eine andere Sicherheitssoftware auf dem Zielrechner installiert ist.
- Auf dem Remote-Endpunkt wird Windows XP Home, Windows 7 Home Basic, Windows 7 Home Premium, Windows 8 (Basisversionen), Windows 8.1 (Basisversionen) oder Windows 10 Home ausgeführt.

Hinweis

Sie können den OfficeScan Agent auf dem Ziel-Host-Rechner mit anderen Installationsmethoden installieren. Diese werden unter *Überlegungen zur Verteilung auf Seite 5-12* erläutert.

Führen Sie vor der Installation des OfficeScan Agents mit Vulnerability Scanner folgende Schritte durch:

- Für Windows 7 (Professional, Enterprise, Ultimate Edition), Windows 8 (Pro, Enterprise), Windows 8.1 (Pro, Enterprise), Windows 10 (Pro, Education, Enterprise), Windows Server 2012 (alle Editionen) oder Windows Server 2016 (alle Editionen):

1. Aktivieren Sie ein integriertes Administratorkonto, und richten Sie das Kennwort für das Konto ein.
2. Klicken Sie auf **Starten** > **Programme** > **Administrator-Tools** > **Windows-Firewall mit erweiterter Sicherheit**.
3. Setzen Sie den Status der Firewall für Domänenprofil, Privates Profil und öffentliches Profil auf "Aus".
4. öffnen Sie die Microsoft Management-Konsole (klicken Sie auf **Starten** > **Ausführen**, und geben Sie `services.msc` ein), und starten Sie den **Remote-Registrierungsdienst**. Installieren Sie den OfficeScan Agent mit dem integrierten Administratorkonto und -kennwort.

- Unter Windows XP Professional (32-Bit- oder 64-Bit-Version):
  1. öffnen Sie Windows Explorer, und klicken Sie auf **Extras** > **Ordneroptionen**.
  2. Klicken Sie auf die Registerkarte **Ansicht**, und deaktivieren Sie **Einfache Dateifreigabe verwenden (empfohlen)**.

Methoden der Schwachstellensuche

Vulnerability Scanner überprüft, ob auf den Host-Rechnern Sicherheitssoftware installiert ist, und kann den OfficeScan Agent auf ungeschützten Rechnern installieren.

Die Schwachstellensuche kann auf verschiedene Art durchgeführt werden.

TABELLE 5-13. Methoden der Schwachstellensuche

METHODE	DETAILS
Manuelle Suche nach Schwachstellen	Administratoren können die Schwachstellensuche nach Anforderung ausführen.

METHODE	DETAILS
DHCP-Suche	Administratoren können Schwachstellensuchen auf Host-Rechnern durchführen, 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 Host-Rechner entdeckt, läuft die Schwachstellensuche auf dem Rechner. **Hinweis** Vulnerability Scanner kann keine DHCP-Anforderungen entdecken, wenn er auf Windows Server 2008, Windows 7, Windows 8, Windows 8.1, Windows 10 oder Windows Server 2012 gestartet wird.
Zeitgesteuerte Suche nach Schwachstellen	Schwachstellensuchen werden automatisch nach dem Zeitplan des Administrators ausgeführt.

Wenn Vulnerability Scanner ausgeführt wird, wird der Status des OfficeScan Agent auf den Ziel-Host-Rechnern angezeigt. Folgende Zustände sind möglich:

- **Normal**: Der OfficeScan Agent läuft und arbeitet ordnungsgemäß.
- **Ungewöhnlich**: Die OfficeScan Agent-Dienste laufen nicht oder der agent verfügt nicht über Echtzeitschutz.
- **Nicht installiert**: Der TMListen-Dienst fehlt oder der OfficeScan Agent ist nicht installiert.
- **Nicht erreichbar**: Vulnerability Scanner konnte keine Verbindung zum Host-Rechner aufbauen und den Status des OfficeScan Agents nicht ermitteln. OfficeScan Agent

Eine manuelle Schwachstellensuche ausführen

Prozedur

1. Um die Schwachstellensuche auf dem OfficeScan Server-Computer auszuführen, navigieren Sie zu <Installationsordner des Servers>\PCCSRV\Admin\Utility\TMVS, und doppelklicken Sie auf TMVS.exe. Die **Trend Micro Vulnerability Scanner** Konsole wird angezeigt. So führen Sie eine Schwachstellensuche auf einem anderen Endpunkt unter Windows Server 2003, Server 2008, 7, 8, 8.1, 10 oder Server2012/2016 aus:

   a. Navigieren Sie auf dem OfficeScan Server-Computer zu <Installationsordner des Servers >\PCCSRV\Admin\Utility.

   b. Kopieren Sie den Ordner TMVS auf den anderen Endpunkt.

   c. öffnen Sie auf dem anderen Endpunkt den Ordner TMVS, und doppelklicken Sie auf TMVS.exe.

      Die **Trend Micro Vulnerability Scanner** Konsole wird angezeigt.

   Hinweis

   Das Tool kann nicht über den Terminal Server gestartet werden.

2. Gehen Sie zum Abschnitt **Manuelle Suche**.

3. Geben Sie den IP-Adressbereich der Endpunkte 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 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 ausgeführt wird.

4. Klicken Sie auf **Einstellungen**.

   Das Fenster **Einstellungen** wird angezeigt.

5. Konfigurieren Sie die folgenden Einstellungen:

OPTION	BEZEICHNUNG
Ping-Einstellungen	Vulnerability Scanner kann die IP-Adressen "anpingen", die im vorhergehenden Schritt festgelegt wurden, um zu überprüfen, ob sie zurzeit verwendet werden. Wenn ein Host-Zielcomputer eine IP-Adresse verwendet, kann Vulnerability Scanner das Betriebssystem des Host-Computers ermitteln. Weitere Informationen finden Sie unter *Ping-Einstellungen auf Seite 5-62*.
Methode zum Abrufen von Computerbeschreibungen	Von Host-Rechnern, die auf den "Ping"-Befehl antworten, kann Vulnerability Scanner zusätzliche Informationen abfragen. Weitere Informationen finden Sie unter *Methode zum Abrufen von Endpunkt-Beschreibungen auf Seite 5-59*.
Produktabfrage:	Vulnerability Scanner kann feststellen, ob auf den Endpunkten Sicherheitssoftware vorhanden ist. Weitere Informationen finden Sie unter *Produktabfrage auf Seite 5-55*.
OfficScan Servereinstellungen	Konfigurieren Sie diese Einstellungen, wenn Vulnerability Scanner den OfficeScan Agent automatisch auf ungeschützten Host-Rechnern installieren soll. über diese Einstellungen können der übergeordnete Server des OfficeScan Agents und die Anmeldedaten des Administrators auf den Host-Rechnern ermittelt werden.

OPTION	BEZEICHNUNG
	Weitere Informationen finden Sie unter *Einstellungen des OfficeScan Servers auf Seite 5-63*. **Hinweis** Bestimmte Bedingungen können die Installation des OfficeScan Agents auf die Ziel-Host-Rechner verhindern. Weitere Informationen finden Sie unter *Richtlinien für die Installation des OfficeScan Agents mit Hilfe von Vulnerability Scanner auf Seite 5-42*.
Benachrichtigungen	Vulnerability Scanner kann die Ergebnisse der Schwachstellensuche an die OfficeScan Administratoren senden. Er kann auch Benachrichtigungen auf ungeschützten Host-Rechnern anzeigen. Weitere Informationen finden Sie unter *Benachrichtigungen auf Seite 5-59*.
Ergebnisse speichern	Zusätzlich zum Versenden der Ergebnisse der Schwachstellensuche an die Administratoren kann Vulnerability Scanner die Ergebnisse in einer `.csv`-Datei speichern. Weitere Informationen finden Sie unter *Ergebnisse der Suche nach Schwachstellen auf Seite 5-61*.

6. Klicken Sie auf **OK**.

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 Endpunkt Windows Server 2008 oder Windows Server 2012 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

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 5-14. 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 8.
DhcpDelayScan=x	Dabei handelt es sich um die Verzögerung in Sekunden, bevor überprüft wird, ob auf dem anfragenden Endpunkt bereits eine Antiviren-Software installiert ist. Der Minimalwert ist 0 (keine Wartezeit) und der Maximalwert ist 600. Der Standardwert ist 30.
LogReport=x	0 deaktiviert die Protokollierung, 1 aktiviert die Protokollierung. Vulnerability Scanner versendet die Ergebnisse der Suche an den OfficeScan Server. Protokolle werden im Fenster **Systemereignisprotokolle** der Webkonsole angezeigt.
OsceServer=x	Das ist die IP-Adresse oder der DNS-Name des OfficeScan Servers.
OsceServerPort=x	Das ist der Webserver-Port auf dem OfficeScan Server.

2. Um die Schwachstellensuche auf dem OfficeScan Server-Computer auszuführen, navigieren Sie zu <Installationsordner des Servers>`\PCCSRV\Admin\Utility`

\TMVS, und doppelklicken Sie auf TMVS.exe. Die **Trend Micro Vulnerability Scanner** Konsole wird angezeigt. So führen Sie eine Schwachstellensuche auf einem anderen Endpunkt unter Windows Server 2003, Server 2008, 7, 8, 8.1, 10 oder Server2012/2016 aus:

a. Navigieren Sie auf dem OfficeScan Server-Computer zu <Installationsordner des Servers >\PCCSRV\Admin\Utility.

b. Kopieren Sie den Ordner TMVS auf den anderen Endpunkt.

c. öffnen Sie auf dem anderen Endpunkt den Ordner TMVS, und doppelklicken Sie auf TMVS.exe.

   Die **Trend Micro Vulnerability Scanner** Konsole wird angezeigt.

Hinweis

Das Tool kann nicht über den Terminal Server gestartet werden.

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

   Das Fenster **Einstellungen** wird angezeigt.

4. Konfigurieren Sie die folgenden Einstellungen:

OPTION	BEZEICHNUNG
Produktabfrage:	Vulnerability Scanner kann feststellen, ob auf den Endpunkten Sicherheitssoftware vorhanden ist. Weitere Informationen finden Sie unter *Produktabfrage auf Seite 5-55*.
OfficScan Servereinstellungen	Konfigurieren Sie diese Einstellungen, wenn Vulnerability Scanner den OfficeScan Agent automatisch auf ungeschützten Host-Rechnern installieren soll. über diese Einstellungen können der übergeordnete Server des OfficeScan Agents und die Anmeldedaten des Administrators auf den Host-Rechnern ermittelt werden. Weitere Informationen finden Sie unter *Einstellungen des OfficeScan Servers auf Seite 5-63*.

OPTION	BEZEICHNUNG
	Hinweis Bestimmte Bedingungen können die Installation des OfficeScan Agents auf die Ziel-Host-Rechner verhindern. Weitere Informationen finden Sie unter *Richtlinien für die Installation des OfficeScan Agents mit Hilfe von Vulnerability Scanner auf Seite 5-42*.
Benachrichtigungen	Vulnerability Scanner kann die Ergebnisse der Schwachstellensuche an die OfficeScan Administratoren senden. Er kann auch Benachrichtigungen auf ungeschützten Host-Rechnern anzeigen. Weitere Informationen finden Sie unter *Benachrichtigungen auf Seite 5-59*.
Ergebnisse speichern	Zusätzlich zum Versenden der Ergebnisse der Schwachstellensuche an die Administratoren kann Vulnerability Scanner die Ergebnisse in einer `.csv`-Datei speichern. Weitere Informationen finden Sie unter *Ergebnisse der Suche nach Schwachstellen auf Seite 5-61*.

5. Klicken Sie auf **OK**.

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

Hinweis

Die Registerkarte **DHCP-Suche** ist auf Computern unter Windows Server 2008, Windows 7, Windows 8, Windows 8.1, Windows 10 und Windows Server 2012 nicht verfügbar.

7. Klicken Sie auf **Start**.

   Der Vulnerability Scanner wartet nun auf DHCP-Anfragen und untersucht dann alle Computer, 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

Prozedur

1. Um die Schwachstellensuche auf dem OfficeScan Server-Computer auszuführen, navigieren Sie zu <Installationsordner des Servers>`\PCCSRV\Admin\Utility\TMVS`, und doppelklicken Sie auf `TMVS.exe`. Die **Trend Micro Vulnerability Scanner** Konsole wird angezeigt. So führen Sie eine Schwachstellensuche auf einem anderen Endpunkt unter Windows Server 2003, Server 2008, 7, 8, 8.1, 10 oder Server2012/2016 aus:

   a. Navigieren Sie auf dem OfficeScan Server-Computer zu `<Installationsordner des Servers >\PCCSRV\Admin\Utility`.

   b. Kopieren Sie den Ordner `TMVS` auf den anderen Endpunkt.

   c. öffnen Sie auf dem anderen Endpunkt den Ordner `TMVS`, und doppelklicken Sie auf `TMVS.exe`.

      Die **Trend Micro Vulnerability Scanner** Konsole wird angezeigt.

   Hinweis

   Das Tool kann nicht über den Terminal Server gestartet werden.

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 Endpunkte 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 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 ausgeführt wird.

6. Geben Sie die Startzeit für den **Zeitplan** 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, welche Reihe von Einstellungen der Schwachstellensuche verwendet werden soll.

   a. 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 5-45*.

   b. 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.

   c. Konfigurieren Sie die folgenden Einstellungen:

Ping-Einstellungen	Vulnerability Scanner kann die IP-Adressen "anpingen", die im vorhergehenden Schritt festgelegt wurden, um zu überprüfen, ob sie zurzeit verwendet werden. Wenn ein Host-Zielcomputer eine IP-Adresse verwendet, kann Vulnerability Scanner das Betriebssystem des Host-Computers ermitteln. Weitere Informationen finden Sie unter *Ping-Einstellungen auf Seite 5-62*.
Methode zum Abrufen von Computerbeschreibungen	Von Host-Rechnern, die auf den "Ping"-Befehl antworten, kann Vulnerability Scanner zusätzliche Informationen abfragen. Weitere Informationen finden Sie unter *Methode zum Abrufen von Endpunkt-Beschreibungen auf Seite 5-59*.
Produktabfrage:	Vulnerability Scanner kann feststellen, ob auf den Endpunkten Sicherheitssoftware vorhanden ist. Weitere Informationen finden Sie unter *Produktabfrage auf Seite 5-55*.
OfficScan Servereinstellungen	Konfigurieren Sie diese Einstellungen, wenn Vulnerability Scanner den OfficeScan Agent automatisch auf ungeschützten Host-Rechnern installieren soll. über diese Einstellungen können der übergeordnete Server des OfficeScan Agents und die Anmeldedaten des Administrators auf den Host-Rechnern ermittelt werden. Weitere Informationen finden Sie unter *Einstellungen des OfficeScan Servers auf Seite 5-63*. **Hinweis** Bestimmte Bedingungen können die Installation des OfficeScan Agents auf die Ziel-Host-Rechner verhindern. Weitere Informationen finden Sie unter *Richtlinien für die Installation des OfficeScan Agents mit Hilfe von Vulnerability Scanner auf Seite 5-42*.

Benachrichtigungen	Vulnerability Scanner kann die Ergebnisse der Schwachstellensuche an die OfficeScan Administratoren senden. Er kann auch Benachrichtigungen auf ungeschützten Host-Rechnern anzeigen. Weitere Informationen finden Sie unter *Benachrichtigungen auf Seite 5-59*.
Ergebnisse speichern	Zusätzlich zum Versenden der Ergebnisse der Schwachstellensuche an die Administratoren kann Vulnerability Scanner die Ergebnisse in einer `.csv`-Datei speichern. Weitere Informationen finden Sie unter *Ergebnisse der Suche nach Schwachstellen auf Seite 5-61*.

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 Endpunkt Windows Server 2008 oder Windows Server 2012 ausgeführt wird, werden in der Tabelle **Ergebnisse** keine Informationen über die MAC-Adresse angezeigt.

10. 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**.

Einstellungen für die Suche nach Schwachstellen

Einstellungen für die Suche nach Schwachstellen werden direkt im Trend Micro Vulnerability Scanner (`TMVS.exe`) oder in der Datei `TMVS.ini` vorgenommen.

Hinweis

Weitere Informationen dazu, wie Debug-Protokolle für Vulnerability Scanner erfasst werden, finden Sie unter *Server-Debug-Protokolle unter Verwendung von LogServer.exe auf Seite 18-3*.

Produktabfrage

Vulnerability Scanner kann feststellen, ob auf den agents Sicherheitssoftware vorhanden ist. Die folgende Tabelle erläutert, wie Vulnerability Scanner die Sicherheitsprodukte überprüft:

TABELLE 5-15. Sicherheitsprodukte, die von Vulnerability Scanner überprüft werden

PRODUCT	BESCHREIBUNG
ServerProtect für Windows	Der Vulnerability Scanner verwendet den RPC-Endpunkt, um zu überprüfen, ob `SPNTSVC.exe` ausgeführt wird. Die zurückgegebenen Informationen beinhalten Betriebssystem und Viren-Scan-Engine sowie Viren-Pattern- und Produktversion. Der Vulnerability Scanner kann den ServerProtect Information Server oder die ServerProtect Management-Konsole nicht erkennen.
ServerProtect für Linux	Wenn auf dem Ziel-Endpunkt kein Windows Betriebssystem ausgeführt wird, überprüft der Vulnerability Scanner, ob ServerProtect für Linux installiert ist. Dazu wird versucht, eine Verbindung mit Port 14942 aufzubauen.

PRODUCT	BESCHREIBUNG
OfficeScan Agent	Vulnerability Scanner überprüft mit Hilfe des OfficeScan Agent Ports, ob der OfficeScan Agent installiert ist. Es wird außerdem überprüft, ob der `TmListen.exe`-Prozess ausgeführt wird. Die Portnummern werden automatisch abgerufen, wenn das Programm vom Standardspeicherort ausgeführt wird. Wenn Sie Vulnerability Scanner auf einem anderen Endpunkt als dem OfficeScan Server gestartet haben, führen Sie eine Überprüfung durch, und verwenden Sie anschließend den Kommunikationsport des anderen Endpunkts.
PortalProtect™	Vulnerability Scanner lädt die Webseite `http://localhost:port/PortalProtect/index.html`, um zu überprüfen, ob das Produkt installiert ist.
ScanMail™ for Microsoft Exchange™	Der Vulnerability Scanner lädt die Webseite `http://ipaddress:port/scanmail.html`, um zu überprüfen, ob eine ScanMail Installation vorliegt. Standardmäßig verwendet ScanMail Port 16372. Wenn ScanMail eine andere Portnummer verwendet, geben Sie diese Portnummer an. Andernfalls kann ScanMail von Vulnerability Scanner nicht erkannt werden.
InterScan™ Produktreihe	Vulnerability Scanner lädt die Webseite für unterschiedliche Produkte, um zu überprüfen, ob die Produkte installiert sind. • InterScan Messaging Security Suite 5.x: `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan eManager 3.x: `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan VirusWall™ 3.x: `http://localhost:port/InterScan/cgi-bin/interscan.dll`
Trend Micro Internet Security™ (PC-cillin)	Der Vulnerability Scanner verwendet Port 40116, um zu überprüfen, ob Trend Micro Internet Security installiert ist.

PRODUCT	BESCHREIBUNG
McAfee VirusScan ePolicy Orchestrator	Der Vulnerability Scanner sendet ein spezielles Token an den TCP-Port 8081, den Standardport von ePolicy Orchestrator für die Verbindung zwischen Server und agent. Der Endpunkt mit diesem Antivirus-Produkt verwendet einen speziellen Token-Typ. Der Vulnerability Scanner kann den eigenständigen McAfee VirusScan nicht erkennen.
Norton Antivirus™ Corporate Edition	Der Vulnerability Scanner sendet ein spezielles Token an den UDP-Port 2967, dem Standardport von Norton Antivirus Corporate Edition RTVScan. Der Endpunkt mit diesem Antivirus-Produkt verwendet einen speziellen Token-Typ. Da Norton Antivirus Corporate Edition über UDP kommuniziert, ist die Genauigkeit nicht garantiert. Des Weiteren kann der Netzwerkdatenverkehr die UDP-Wartezeit beeinflussen.

Der Vulnerability Scanner erkennt Produkte und Computer, die die folgenden Protokolle verwenden:

- **RPC**: Erkennt ServerProtect for NT
- **UDP**: Erkennt Norton AntiVirus Corporate Edition-Clients
- **TCP**: Erkennt McAfee VirusScan ePolicy Orchestrator
- **ICMP**: Erkennt Computer durch das Versenden von ICMP-Paketen
- **HTTP**: Erkennt OfficeScan Agents
- **DHCP**: Wird eine DHCP-Anfrage erkannt, prüft der Vulnerability Scanner, ob auf dem anfragenden Endpunkt bereits eine Antiviren-Software installiert ist.

Einstellungen zur Überprüfung von Produkten konfigurieren

Die Einstellungen zur Überprüfung der Produkte sind eine Unterkategorie der Einstellungen für die Suche nach Schwachstellen. Weitere Informationen zur Suche nach Schwachstellen finden Sie unter *Methoden der Schwachstellensuche auf Seite 5-43*.

Prozedur

1. Einstellungen zur Überprüfung von Produkten in Vulnerability Scanner (`TMVS.exe`) vornehmen:

a. Starten Sie die Datei `TMVS.exe`.

b. Klicken Sie auf **Einstellungen**.

   Das Fenster **Einstellungen** wird angezeigt.

c. Gehen Sie zum Abschnitt **Product query**.

d. Wählen Sie die Produkte, die überprüft werden sollen.

e. Klicken Sie neben dem Produktnamen auf **Einstellungen** und geben Sie dann die Port-Nummer an, die Vulnerability Scanner überprüfen soll.

f. Klicken Sie auf **OK**.

   Das Fenster **Einstellungen** wird geschlossen.

2. Die Anzahl der Computer festlegen, auf denen Vulnerability Scanner gleichzeitig nach Sicherheitssoftware sucht:

a. Navigieren Sie zu <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\TMVS`, und öffnen Sie `TMVS.ini` mit Hilfe eines Texteditors, z. B. Notepad.

b. Um die Anzahl der Computer festzulegen, die bei der Suche nach Schwachstellen überprüft werden, ändern Sie den Wert für `ThreadNumManual`. Geben Sie einen Wert zwischen 8 und 64 an.

   Geben Sie zum Beispiel `ThreadNumManual=60` ein, wenn Vulnerability Scanner 60 Computer gleichzeitig überprüfen soll.

c. Um die Anzahl der Computer festzulegen, die bei der zeitgesteuerten Suche nach Schwachstellen überprüft werden, ändern Sie den Wert für `ThreadNumSchedule`. Geben Sie einen Wert zwischen 8 und 64 an.

   Geben Sie zum Beispiel `ThreadNumSchedule=50` ein, wenn Vulnerability Scanner 50 Computer gleichzeitig überprüfen soll.

d. Speichern Sie die Datei `TMVS.ini`.

Methode zum Abrufen von Endpunkt-Beschreibungen

Wenn Vulnerability Scanner die Host-Rechner "anpingen" kann, kann er zusätzliche Informationen über die Host-Rechner abfragen. Es gibt zwei Methoden zur Abfrage von Informationen:

- **Schnellabfrage**: Bei der Schnellabfrage wird nur der Endpunkt-Name abgefragt.
- **Normale Abfrage**: Fragt Informationen über die Domäne und den Endpunkt ab.

Abfrageeinstellungen konfigurieren

Die Abfrageeinstellungen sind eine Unterkategorie der Einstellungen für die Suche nach Schwachstellen. Weitere Informationen zur Suche nach Schwachstellen finden Sie unter *Methoden der Schwachstellensuche auf Seite 5-43*.

Prozedur

1. Starten Sie die Datei `TMVS.exe`.
2. Klicken Sie auf **Einstellungen**.

   Das Fenster **Einstellungen** wird angezeigt.
3. Gehen Sie zum Abschnitt **Method for retrieving computer descriptions**.
4. Wählen Sie **Normal** oder **Quick**.
5. Wenn Sie **Normal** ausgewählt haben, wählen Sie **Computerbeschreibungen bei Verfügbarkeit abrufen**.
6. Klicken Sie auf **OK**.

   Das Fenster **Einstellungen** wird geschlossen.

Benachrichtigungen

Vulnerability Scanner kann die Ergebnisse der Schwachstellensuche an die OfficeScan Administratoren senden. Er kann auch Benachrichtigungen auf ungeschützten Host-Rechnern anzeigen.

Einstellungen für die Benachrichtigungen konfigurieren

Die Benachrichtigungseinstellungen sind eine Unterkategorie der Einstellungen für die Suche nach Schwachstellen. Weitere Informationen zur Suche nach Schwachstellen finden Sie unter *Methoden der Schwachstellensuche auf Seite 5-43*.

Prozedur

1. Starten Sie die Datei `TMVS.exe`.
2. Klicken Sie auf **Einstellungen**.

   Das Fenster **Einstellungen** wird angezeigt.
3. Gehen Sie zum Abschnitt **Notifications**.
4. Die Ergebnisse der Schwachstellensuche automatisch an Sie selbst oder an andere Administratoren in Ihrem Unternehmen senden:

   a. Wählen Sie **Email results to the system administrator**.

   b. Klicken Sie auf **Konfigurieren**, um die E-Mail-Einstellungen festzulegen.

   c. Geben Sie in das Feld **An** die E-Mail-Adresse des Empfängers ein.

   d. Geben Sie in das Feld **Von** die E-Mail-Adresse des Absenders ein.

   e. 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.

   f. Geben Sie unter **Subject** einen Betreff für die Nachricht ein, oder übernehmen Sie den Standardbetreff.

   g. Klicken Sie auf **OK**.
5. Die Benutzer darüber informieren, dass auf ihren Computern keine Sicherheitssoftware installiert ist:

   a. Wählen Sie **Display a notification on unprotected computers**.

   b. Klicken Sie auf **Anpassen**, um die Benachrichtigung zu konfigurieren.

c. Geben Sie im Fenster **Benachrichtigung** eine eigene Meldung ein, oder verwenden Sie den Standardtext.

d. Klicken Sie auf **OK**.

6. Klicken Sie auf **OK**.

   Das Fenster **Einstellungen** wird geschlossen.

Ergebnisse der Suche nach Schwachstellen

Sie können die Ergebnisse der Schwachstellensuche in einer komma-separierten Datei (CSV) speichern.

Suchergebnisse konfigurieren

Die Einstellungen zur Speicherung der Ergebnisse der Schwachstellensuche sind eine Unterkategorie der Einstellungen der Schwachstellensuche. Weitere Informationen zur Suche nach Schwachstellen finden Sie unter *Methoden der Schwachstellensuche auf Seite 5-43*.

Prozedur

1. Starten Sie die Datei `TMVS.exe`.
2. Klicken Sie auf **Einstellungen**.

   Das Fenster **Einstellungen** wird angezeigt.
3. Gehen Sie zum Abschnitt **Save results**.
4. Wählen Sie **Automatically save the results to a CSV file**.
5. Den Standardspeicherordner für die `CSV`-Datei ändern:

   a. Klicken Sie auf **Durchsuchen**.

   b. Wählen Sie einen Zielordner auf dem Endpunkt oder im Netzwerk aus.

   c. Klicken Sie auf **OK**.
6. Klicken Sie auf **OK**.

Das Fenster **Einstellungen** wird geschlossen.

Ping-Einstellungen

Verwenden Sie die "Ping"-Einstellungen, um das Vorhandensein eines Zielrechners zu überprüfen und dessen Betriebssystem festzustellen. Wenn diese Einstellungen deaktiviert sind, durchsucht Vulnerability Scanner alle IP-Adressen innerhalb des vorgegebenen IP-Adressbereichs – sogar solche, die auf keinem Host-Rechner verwendet werden –, und macht dadurch den Suchvorgang länger als er sein sollte.

Ping-Einstellungen konfigurieren

Die Ping-Einstellungen sind eine Unterkategorie der Einstellungen der Schwachstellensuche. Weitere Informationen zur Suche nach Schwachstellen finden Sie unter *Methoden der Schwachstellensuche auf Seite 5-43*.

Prozedur

1. Ping-Einstellungen in Vulnerability Scanner (`TMVS.exe`) vornehmen:

   a. Starten Sie die Datei `TMVS.exe`.

   b. Klicken Sie auf **Einstellungen**.

      Das Fenster **Einstellungen** wird angezeigt.

   c. Gehen Sie zum Abschnitt **Ping**-Einstellungen.

   d. Wählen Sie **Allow Vulnerability Scanner to ping computers on your network to check their status**.

   e. Übernehmen oder ändern Sie die Standardwerte in den Feldern **Packet size** und **Timeout**.

   f. Wählen Sie **Detect the type of operating system using ICMP OS fingerprinting**.

      Wenn Sie diese Option wählen, bestimmt Vulnerability Scanner, ob auf einem Host-Rechner Windows oder ein anderes Betriebssystem läuft. Bei Host-Rechnern mit Windows kann Vulnerability Scanner die Version von Windows feststellen.

g. Klicken Sie auf **OK**.

Das Fenster **Einstellungen** wird geschlossen.

2. Legen Sie die Anzahl der Computer fest, an die Vulnerability Scanner gleichzeitig Pings sendet:

a. Navigieren Sie zu <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\TMVS`, und öffnen Sie `TMVS.ini` mit Hilfe eines Texteditors, z. B. Notepad.

b. 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 Computer gleichzeitig senden soll.

c. Speichern Sie die Datei `TMVS.ini`.

Einstellungen des OfficeScan Servers

OfficeScan Server-Einstellungen werden verwendet, wenn:

- Vulnerability Scanner installiert den OfficeScan Agent auf ungeschützten Zielrechnern. Über die Server-Einstellungen kann Vulnerability Scanner den übergeordneten Server des OfficeScan Agents und die Administratordaten zur Anmeldung auf den Zielrechnern ermitteln.

Hinweis

Bestimmte Bedingungen können die Installation des OfficeScan Agents auf die Ziel-Host-Rechner verhindern.

Weitere Informationen finden Sie unter *Richtlinien für die Installation des OfficeScan Agents mit Hilfe von Vulnerability Scanner auf Seite 5-42*.

- Vulnerability Scanner versendet agent-Installationsprotokolle an den OfficeScan Server.

Einstellungen des OfficeScan Servers konfigurieren

Die OfficeScan Server-Einstellungen sind eine Unterkategorie der Einstellungen für die Suche nach Schwachstellen. Weitere Informationen zur Suche nach Schwachstellen finden Sie unter *Methoden der Schwachstellensuche auf Seite 5-43*.

Prozedur

1. Starten Sie die Datei `TMVS.exe`.
2. Klicken Sie auf **Einstellungen**.

   Das Fenster **Einstellungen** wird angezeigt.
3. Gehen Sie zum Abschnitt **OfficeScan server Einstellungen**.
4. Geben Sie den Namen und die Portnummer des OfficeScan Servers ein.
5. Wählen Sie **OfficeScan Agent automatisch auf ungeschützten Computern installieren** aus.
6. Die Anmeldedaten zur Administration konfigurieren:
   a. Klicken Sie auf **Install to Account**.
   b. Geben Sie im Fenster **Kontoinformationen** einen Benutzernamen und ein Kennwort ein.
   c. Klicken Sie auf **OK**.
7. Wählen Sie **Send logs to the OfficeScan server**.
8. Klicken Sie auf **OK**.

   Das Fenster **Einstellungen** wird geschlossen.

Installation bei Einhaltung von Sicherheitsrichtlinien

Installieren Sie OfficeScan Agents auf Computern innerhalb der Netzwerkdomänen oder installieren Sie den OfficeScan Agent mit Hilfe der IP-Adresse auf einem Zielendpunkt.

Bevor Sie den OfficeScan Agent installieren, beachten Sie das Folgende:

Prozedur

1. Notieren Sie die Anmeldedaten für jeden Endpunkt. OfficeScan fordert Sie während der Installation auf, die Anmeldedaten einzugeben.

2. Der OfficeScan Agent wird unter folgenden Voraussetzungen nicht auf dem Endpunkt installiert:

   - Der OfficeScan Server ist auf dem Endpunkt installiert.
   - Auf dem Endpunkt wird Windows XP Home, Windows 7™ Starter, Windows 7 Home Basic, Windows 7 Home Premium, Windows 8 (Basisversionen), Windows 8.1 (Basisversionen) und Windows 10 Home ausgeführt. Bei Endpunkten, die auf diesen Plattformen ausgeführt werden, wählen Sie eine andere Installationsmethode aus. Weitere Informationen finden Sie unter *Überlegungen zur Verteilung auf Seite 5-12*.

3. Wenn auf dem Zielendpunkt Windows 7 (Professional, Enterprise, oder Ultimate Edition), Windows 8 (Pro, Enterprise), Windows 8.1 (Pro, Enterprise), Windows 10 (Pro, Education, Enterprise), Windows Server 2012 (Standard) oder Windows Server 2016 (alle Editionen) ausgeführt wird, führen Sie die folgenden Schritte auf dem Endpunkt durch:

   a. Aktivieren Sie ein integriertes Administratorkonto, und richten Sie das Kennwort für das Konto ein.

   b. Deaktivieren Sie die Windows Firewall.

   c. Klicken Sie auf **Starten** > **Programme** > **Administrator-Tools** > **Windows-Firewall mit erweiterter Sicherheit**.

   d. Setzen Sie den Status der Firewall für Domänenprofil, Privates Profil und öffentliches Profil auf "Aus".

   e. öffnen Sie die Microsoft Management-Konsole (klicken Sie auf **Start** > **Ausführen**, und geben Sie `services.msc` ein), und starten Sie den **Remote-Registrierungsdienst**. Installieren Sie den OfficeScan Agent mit dem integrierten Administratorkonto und -kennwort.

4. Wenn sich auf dem Endpunkt Sicherheitsprogramme für Endpunkte von Trend Micro befinden, überprüfen Sie, ob OfficeScan die Software automatisch deinstallieren und durch den OfficeScan Agent ersetzen kann. Um eine Liste der Agent-Sicherheitssoftware anzuzeigen, die OfficeScan automatisch deinstalliert, öffnen Sie die folgenden Dateien unter <*Installationsordner des Servers*>`\PCCSRV\Admin`. Sie können diese Dateien mit Hilfe eines Texteditors wie beispielsweise Notepad öffnen.

   - `tmuninst.ptn`
   - `tmuninst_as.ptn`

   Wenn die auf dem Zielendpunkt installierte Software nicht in der Liste enthalten ist, müssen Sie sie zuerst deinstallieren. Je nach Deinstallationsverfahren muss der Endpunkt nach der Deinstallation unter Umständen neu gestartet werden.

Den OfficeScan Agent installieren

Prozedur

1. Navigieren Sie zu **Bewertung** > **Nicht verwaltete Endpunkte**.
2. Klicken Sie oben in der Agent-Hierarchie auf **Installieren**.
   - Wenn eine frühere Version von OfficeScan Agent bereits auf dem Endpunkt installiert ist und Sie auf **Installieren** klicken, überspringt OfficeScan die Installation und führt kein Upgrade des Endpunkts auf diese Version durch. Um das Upgrade des Endpunkts durchzuführen, müssen Sie unbedingt die folgende Einstellung konfigurieren.
     a. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
     b. Klicken Sie auf die Registerkarte **Einstellungen** > **Berechtigungen und andere Einstellungen** > **Andere Einstellungen**.
     c. Gehen Sie zum Abschnitt **Update-Einstellungen**.
     d. Wählen Sie im Listenfeld **OfficeScan Agents aktualisieren nur die folgenden Komponenten** die Option **Alle Komponenten (einschließlich Hotfixes und Agent-Programm)** aus.

e. Klicken Sie auf **Auf alle Agents anwenden**.

3. Geben Sie für jeden Endpunkt das Anmeldekonto für den Administrator an und klicken Sie auf **Anmelden**. OfficeScan startet die Installation des Agents auf dem Zielendpunkt.

4. Zeigen Sie den Installationstatus an.

Zu OfficeScan Agent migrieren

Ersetzen Sie agent Sicherheitssoftware, die auf dem Ziel-Endpunkt installiert ist, durch den OfficeScan Agent.

Migration von einer anderen Endpunkt-Sicherheitssoftware

Bei der Installation des OfficeScan Agent überprüft das Installationsprogramm, ob auf dem Ziel-Endpunkt Endpunkt-Sicherheitssoftware von Trend Micro oder Fremdherstellern installiert ist. Das Installationsprogramm kann die Software automatisch deinstallieren und sie durch den OfficeScan Agent ersetzen.

Um eine Liste der Endpoint Security-Software anzuzeigen, die OfficeScan automatisch deinstalliert, öffnen Sie die folgenden Dateien unter <*Installationsordner des Servers*>`\PCCSRV\Admin`. Öffnen Sie diese Dateien mit Hilfe eines Texteditors, z. B. Notepad.

- `tmuninst.ptn`
- `tmuninst_as.ptn`

Wenn die auf dem Ziel-Endpunkt installierte Software nicht in der Liste enthalten ist, müssen Sie sie zuerst deinstallieren. Je nach Deinstallationsverfahren muss der Endpunkt nach der Deinstallation unter Umständen neu gestartet werden.

OfficeScan Agent Probleme bei der Migration des

- Starten Sie den Endpunkt neu, falls der agent zwar automatisch migriert wurde, bei den Benutzern jedoch unmittelbar nach der Installation Probleme mit dem OfficeScan Agent auftreten.
- Wenn das OfficeScan Installationsprogramm die Installation fortsetzt, der OfficeScan Agent jedoch nicht in der Lage war, die Sicherheitssoftware zu deinstallieren, kommt es zu Konflikten zwischen den beiden Programmen. Deinstallieren Sie die beiden Programme, und installieren Sie anschließend den OfficeScan Agent mit Hilfe einer der Installationsmethoden, die unter *Überlegungen zur Verteilung auf Seite 5-12* beschrieben werden.

Migration von ServerProtect Normal Servern

Mit dem ServerProtect™ Normal Server Migration Tool können Sie Computer, auf denen Trend Micro ServerProtect Normal Server ausgeführt wird, zu OfficeScan Agent migrieren.

Für das ServerProtect Normal Server Migration Tool gelten die gleichen Hardware- und Software-Voraussetzungen wie für den OfficeScan Server. Führen Sie das Tool auf Computern mit Windows Server 2003 oder Windows Server 2008 aus.

Nach der Deinstallation des ServerProtect Normal Servers installiert das Tool automatisch den OfficeScan Agent. Dabei werden ebenfalls die Einstellungen für die Ausschlussliste der Suche (für alle Suchtypen) auf den OfficeScan Agent migriert.

Bei der Installation des OfficeScan Agent kommt es in manchen Fällen zu einer Zeitüberschreitung des agent-Installationsprogramms für das Migration Tool, und Sie erhalten eine Benachrichtigung, dass die Installation erfolglos verlaufen ist. Der OfficeScan Agent kann aber dennoch erfolgreich installiert worden sein. Überprüfen Sie die Installation auf dem agent-Endpunkt über die OfficeScan Webkonsole.

Unter den folgenden Umständen ist keine Migration möglich:

- Der Remote-agent hat nur eine IPv6-Adresse. Das Migration Tool unterstützt keine IPv6-Adressierung.
- Der Remote-agent kann das NetBIOS-Protokoll nicht verwenden.

- Die Ports 455, 337 und 339 sind gesperrt.
- Der Remote-agent kann das RPC-Protokoll nicht verwenden.
- Der Remote-Registrierungsdienst wird beendet.

Hinweis

Das ServerProtect Normal Server Migration Tool deinstalliert den Control Manager™ Agent für ServerProtect nicht. Weitere Informationen über die Deinstallation des Agents finden Sie in der ServerProtect Dokumentation und/oder der Control Manager Dokumentation.

Das ServerProtect Normal Server Migration Tool verwenden

Prozedur

1. Öffnen Sie auf dem OfficeScan Server-Computer den Ordner <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\SPNSXfr`, und kopieren Sie die Dateien `SPNSXfr.exe` und `SPNSX.ini` in den Ordner `<Installationsordner des Servers>\PCCSRV\Admin`.
2. Doppelklicken Sie auf die Datei `SPNSXfr.exe`, um das Tool auszuführen.

   Die Konsole des **Server Protect Normal Server Migration Tools** wird geöffnet.
3. Wählen Sie den OfficeScan Server aus. Der Pfad des OfficeScan Servers wird unter "OfficeScan Server-Pfad" angezeigt. Ist der Pfad falsch, klicken Sie auf **Browse** und wählen den Ordner `PCCSRV` in dem Verzeichnis, in dem Sie OfficeScan installiert haben. Damit der OfficeScan Server beim nächsten Öffnen des Tools automatisch gesucht wird, aktivieren Sie das Kontrollkästchen **Pfad des Auto Find Servers** (voreingestellt).
4. Wählen Sie die Computer aus, auf denen ServerProtect Normal Server ausgeführt wird und auf denen Sie die Migration durchführen wollen, indem Sie unter **Zielendpunkt** auf eine der folgenden Optionen klicken:
   - **Windows Netzwerkhierarchie**: Zeigt eine Hierarchie aller Domänen im Netzwerk an. Um Computer mit dieser Methode auszuwählen, klicken Sie auf die Domänen, in denen nach agent-Computern gesucht werden soll.

- **Name Informations-Server**: Suche über den Namen des Information Servers. Zur Auswahl der Computer mit dieser Methode geben Sie den Namen eines Information Servers im Netzwerk in das Textfeld ein. Bei der Suche nach mehreren Information Servern trennen Sie die einzelnen Servernamen jeweils durch einen Strichpunkt ;.
- **Bestimmter Name des Normal Servers**: Die Suche erfolgt über den Namen des Normal Servers. Zur Auswahl der Computer mit dieser Methode geben Sie den Namen eines Normal Servers im Netzwerk in das Textfeld ein. Trennen Sie für die Suche nach mehreren Normal Servern die jeweiligen Servernamen durch Strichpunkt ";".
- **Suche im IP-Bereich**: Suche über einen Bereich von IP-Adressen. Zur Auswahl der Computer mit dieser Methode geben Sie unter IP range einen Bereich von IP-Adressen der Klasse B ein.

Hinweis

Wenn ein DNS-Server im Netzwerk bei der Suche nach agents nicht antwortet, wird der Suchvorgang unterbrochen. Warten Sie, bis die Zeitüberschreitung erreicht ist.

5. Aktivieren Sie **Nach der Installation neu starten**, um die Zielcomputer nach der Migration automatisch neu zu starten.

   Ein Neustart ist erforderlich, damit die Migration erfolgreich abgeschlossen werden kann. Wenn Sie das Kontrollkästchen nicht aktivieren, müssen Sie die Computer nach der Migration manuell neu starten.

6. Klicken Sie auf **Suchen**.

   Die Suchergebnisse werden unter **ServerProtect Normal Servers** angezeigt.

7. Klicken Sie auf die Computer, auf denen die Migration durchgeführt werden soll.

   a. Um alle Computer auszuwählen, klicken Sie auf **Select all**.

   b. Um die Auswahl für alle Computer aufzuheben, klicken Sie **Auswahl für alle aufheben**.

   c. Um die Liste als komma-separierte Datei im CSV-Format zu exportieren, klicken Sie auf **In CSV-Datei exportieren**.

8. Falls zur Anmeldung an den Zielcomputern ein Benutzername und ein Kennwort benötigt werden, gehen Sie folgendermaßen vor:

   a. Aktivieren Sie das Kontrollkästchen **Use group account/password**.

   b. Klicken Sie auf **Set User Logon Account**.

      Das Fenster "Enter Administration Information" wird angezeigt.

   c. Geben Sie den Benutzernamen und das Kennwort ein.

      Hinweis

      Melden Sie sich mit dem lokalen oder Domänenadministratorkonto am Zielendpunkt Endpunkt an. Wenn Sie sich ohne ausreichende Berechtigungen, z. B. als "Gast" oder "Normaler Benutzer" anmelden, können Sie die Installation nicht durchführen.

   d. Klicken Sie auf **OK**.

   e. Klicken Sie auf **Ask again if logon is unsuccessful**, damit der Benutzername und das Kennwort während der Migration erneut eingegeben werden können, falls die Anmeldung fehl schlägt.

9. Klicken Sie auf **Migrate**.

10. Wenn Sie das Kontrollkästchen **Nach der Installation neu starten** nicht aktiviert haben, starten Sie die Zielcomputer neu, um die Migration abzuschließen.

Nach der Installation

Überprüfen Sie nach Abschluss der Installation das Folgende:

- *OfficeScan Agent Verknüpfung auf Seite 5-72*
- *Programmliste auf Seite 5-72*
- *OfficeScan Agent-Dienste auf Seite 5-72*
- *OfficeScan Agent -Installationsprotokolle auf Seite 5-73*

OfficeScan Agent Verknüpfung

Die OfficeScan Agent-Verknüpfungen werden im Windows Start-Menü auf dem Agent-Endpunkt angezeigt.

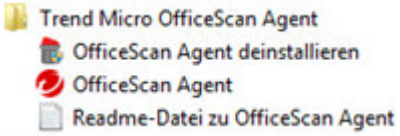


ABBILDUNG 5-2. OfficeScan Agent Verknüpfung

Hinweis

Nicht verfügbar unter Windows 8/8.1/10 oder Windows Server 2012/2012 R2/2016.

Programmliste

Trend Micro OfficeScan Agent ist auf der Liste **Programme hinzufügen/entfernen** in der Systemsteuerung des agent-Endpunkts aufgeführt.

OfficeScan Agent-Dienste

Die folgenden OfficeScan Agent-Dienste werden in der **Microsoft Management-Konsole** aufgeführt:

- OfficeScan NT Listener (`TmListen.exe`)
- OfficeScan NT RealTime Scan (`NTRtScan.exe`)
- OfficeScan NT Proxy-Dienst (`TmProxy.exe`)

Hinweis

Der OfficeScan NT Proxy-Dienst ist auf Windows 7-/8-/8.1-/10- oder Windows Server 2008 R2-/2012-/2016-Plattformen nicht vorhanden.

- OfficeScan NT Firewall (`TmPfw.exe`); falls die Firewall bei der Installation aktiviert wurde
- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)
- Gemeinsames Client Solution Framework für Trend Micro (`TmCCSF.exe`)

OfficeScan Agent -Installationsprotokolle

Das OfficeScan Agent-Installationsprotokoll `OFCNT.LOG` befindet sich an den folgenden Speicherorten:

- `%windir%` für alle Installationsmethoden außer bei MSI-Paket-Installation
- `%temp%` für die Installation mit einem MSI-Paket

Empfohlene Aufgaben nach der Installation

Trend Micro empfiehlt, im Anschluss an die Installation folgende Aufgaben durchzuführen.

Komponenten-Updates

Aktualisieren Sie die OfficeScan Agent-Komponenten, damit die agents über den neuesten Schutz vor Sicherheitsrisiken verfügen. Sie können die agent manuell über die Webkonsole aktualisieren oder die Benutzer auffordern, den Befehl "Jetzt installieren" auf ihren Computern auszuführen.

Die Suche mit dem EICAR-Testskript testen

EICAR, das europäische Institut für Computervirenforschung, hat das EICAR-Testskript zur gefahrlosen Überprüfung der Installation und Konfiguration Ihrer Antiviren-Software entwickelt. Weitere Informationen finden Sie auf der EICAR-Website:

http://www.eicar.org

Das EICAR-Testskript ist eine inaktive Textdatei mit der Erweiterung `.com`. Dieses Skript ist kein Virus und enthält auch keinen Virencode. Die meisten Antiviren-

Programme reagieren jedoch auf dieses Skript wie auf einen Virus. Sie können mit dem Skript einen Virenvorfall simulieren und sicherstellen, dass die E-Mail-Benachrichtigungen und die Virenprotokolle einwandfrei funktionieren.

Warnung!

Testen Sie Ihre Antiviren-Software niemals mit echten Viren.

Eine Testsuche durchführen

Prozedur

1. Aktivieren Sie die Echtzeitsuche auf dem agent.
2. Kopieren Sie die folgende Zeichenfolge, und fügen Sie sie in WordPad oder einen anderen Texteditor ein: `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
3. Speichern Sie die Datei unter dem Namen `EICAR.com` in einem temporären Verzeichnis. OfficeScan erkennt die Datei sofort.
4. Um weitere Computer im Netzwerk zu testen, senden Sie die Datei EICAR.com per E-Mail an die betreffenden Computer.

Tipp

Trend Micro empfiehlt, dass Sie die EICAR-Datei mit einer Komprimierungssoftware (wie z. B. WinZip) komprimieren und anschließend eine weitere Testsuche durchführen.

OfficeScan Agent deinstallieren

Es gibt zwei Möglichkeiten, den OfficeScan Agent von einem Computer zu deinstallieren:

- *Den OfficeScan Agent von der Webkonsole aus deinstallieren auf Seite 5-75*

- *Das Programm zur Deinstallation des OfficeScan Agents ausführen auf Seite 5-77*

Wenn der OfficeScan Agent nicht mit Hilfe der oben erwählten Methode deinstalliert werden kann, deinstallieren Sie den OfficeScan Agent manuell. Weitere Informationen finden Sie unter *Den OfficeScan Agent manuell deinstallieren auf Seite 5-77*.

Den OfficeScan Agent von der Webkonsole aus deinstallieren

Deinstallieren Sie das OfficeScan Agent-Programm von der Webkonsole aus. Führen Sie die Deinstallation nur aus, wenn es zu Problemen mit dem Programm kommt. Führen Sie anschließend sofort eine Neuinstallation durch, um den Endpunkt vor Sicherheitsrisiken zu schützen.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Aufgaben** > **Agent deinstallieren**.
4. Klicken Sie im Fenster **Agent deinstallieren** auf **Deinstallation starten**.
5. Überprüfen Sie den Benachrichtigungsstatus und ob alle agents benachrichtigt wurden.
   a. Klicken Sie auf **Nicht benachrichtigte Endpunkte auswählen** und anschließend auf **Deinstallation starten**, um die Benachrichtigung erneut an noch nicht benachrichtigte agents zu senden.
   b. Klicken Sie auf **Deinstallation beenden**, damit OfficeScan die Benachrichtigung an agents abbricht. Agents Bereits benachrichtigte Agents und Agents, die aktuell deinstalliert werden, ignorieren diesen Befehl.

Das Programm zur Deinstallation des OfficeScan Agent

Benutzer, die Sie zur Deinstallation des OfficeScan Agent-Programms berechtigen, können angewiesen werden, das agent-Deinstallationsprogramm auf ihren Computern auszuführen.

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.

Gewähren der Berechtigung zum Deinstallieren von OfficeScan Agent

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Gehen Sie auf der Registerkarte **Berechtigungen** zum Abschnitt **Deinstallation**.
5. Um die Deinstallation ohne Kennwort zu erlauben, wählen Sie **Der Benutzer darf den OfficeScan Agent deinstallieren**. Ist ein Kennwort erforderlich, wählen Sie **Der Benutzer muss zur Deinstallation des OfficeScan Agents ein Kennwort eingeben**, geben Sie dann das Kennwort ein und bestätigen es.
6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Das Programm zur Deinstallation des OfficeScan Agents ausführen

Prozedur

1. Klicken Sie im Windows Menü **Start** auf **Programme** > **Trend Micro OfficeScan Agent** > **OfficeScan Agent deinstallieren**.

   Sie können auch die folgenden Schritte ausführen:

   a. Klicken Sie auf **Systemsteuerung** > **Software**.

   b. Suchen Sie **Trend Micro OfficeScan Agent**, und klicken Sie auf **Ändern**.

   c. Folgen Sie den Hinweisen auf dem Bildschirm.

2. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort für die Deinstallation ein. OfficeScan informiert den Benutzer über den Verlauf und Abschluss des Deinstallationsvorgangs. Der Benutzer muss zum Abschluss der Deinstallation den agent-Endpunkt nicht neu starten.

Den OfficeScan Agent manuell deinstallieren

Führen Sie die manuelle Deinstallation nur aus, wenn beim Deinstallieren des OfficeScan Agents über die Webkonsole oder nach dem Ausführen des Deinstallationsprogramms Probleme auftreten.

Prozedur

1. Melden Sie sich am Agent-Endpunkt mit einem Konto mit Administratorrechten an.

2. Klicken Sie mit der rechten Maustaste in der Taskleiste auf das Symbol für den OfficeScan Agent und wählen Sie **OfficeScan beenden** aus. Wenn Sie aufgefordert werden, ein Kennwort einzugeben, geben Sie das Kennwort zum Beenden des Programms an, und klicken Sie anschließend auf **OK**.

Hinweis

- Wechseln Sie für Windows 8, 8.1, 10, Windows Server 2012 und Windows Server 2016 in den Desktopmodus, um den OfficeScan Agent zu beenden.
- Deaktivieren Sie das Kennwort auf Computern, auf denen der OfficeScan Agent beendet wird.

  Weitere Informationen finden Sie unter *Agent-Berechtigungen und weitere Einstellungen konfigurieren auf Seite 15-101*.

---

3. Wenn das Kennwort zum Beenden des Programms nicht angegeben wurde, beenden Sie die folgenden Dienste über die Microsoft Management-Konsole:
   - OfficeScan NT Listener
   - OfficeScan NT Proxy-Dienst (für Windows Server 2008)
   - OfficeScan NT Echtzeitsuche
   - Gemeinsames Client Solution Framework für Trend Micro
4. Entfernen Sie die Verknüpfung des OfficeScan Agent aus dem Start-Menü.
   - Unter Windows 8, 8.1, 10, Windows Server 2012 und Windows Server 2016:
     a. Wechseln Sie in den Desktopmodus.
     b. Bewegen Sie den Mauszeiger in die untere rechte Ecke des Bildschirms, und klicken Sie in dem erscheinenden Menü auf **Starten**.

        Der Startbildschirm wird angezeigt.
     c. Klicken Sie mit der rechten Maustaste auf **Trend Micro OfficeScan**.
     d. Klicken Sie auf **Von „Start“ lösen**.
   - Auf allen anderen Windows-Plattformen:

Klicken Sie auf **Start** > **Programme**, klicken Sie mit der rechten Maustaste auf **Trend Micro OfficeScan Agent**, und klicken Sie auf **Löschen**.

5. Öffnen Sie den Windows Registrierungseditor (`regedit.exe`).

Warnung!

Die nächsten Schritte erfordern, dass Sie Registrierungsschlüssel löschen. Unsachgemäße Änderungen an der Registrierung können zu ernsthaften Systemproblemen führen. Erstellen Sie immer eine Sicherungskopie, bevor Sie Änderungen an der Registrierung vornehmen. Weitere Informationen finden Sie in der Hilfe zum Registrierungseditor.

6. Löschen Sie die folgenden Registrierungsschlüssel:

   - Wenn auf dem Endpunkt keine anderen Produkte von Trend Micro installiert sind:
     - Für 32-Bit-Systeme:

       `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`
     - Für 64-Bit-Systeme:

       `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

       `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro`
   - Wenn andere Produkte von Trend Micro auf dem Endpunkt installiert sind, löschen Sie nur die folgenden Schlüssel:
     - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
     - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfcWatchDog`

       Für 32-Bit-Systeme:

       `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfcWatchDog`
     - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp`

       Für 64-Bit-Systeme:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro
\PC-cillinNTCorp
```

7. Löschen Sie die folgenden Registrierungsschlüssel/Werte:
   - Für 32-Bit-Systeme:
     - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Uninstall\OfficeScanNT`
     - OfficeScanNT Monitor (`REG_SZ`) unter `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
   - Für 64-Bit-Systeme:
     - `HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Microsoft \Windows\CurrentVersion\Uninstall\OfficeScanNT`
     - OfficeScanNT Monitor (`REG_SZ`) unter `HKEY_LOCAL_MACHINE \SOFTWARE\ Wow6432Node\Microsoft\Windows \CurrentVersion\Run`
8. Löschen Sie alle Instanzen der folgenden Registrierungsschlüssel an den folgenden Speicherorten:
   - Speicherorte:
     - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`
     - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services`
     - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services`
     - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services`
   - Schlüssel:
     - NTRtScan
     - tmccsf
     - TmFilter
     - TmListen

- TmPreFilter
- TmProxy

Hinweis

TmProxy ist auf Plattformen mit Windows 7/8/8.1/10 oder Windows Server 2008 R2/2012/2012 R2/2016 nicht verfügbar.

- tmtdi

Hinweis

tmtdi ist auf Plattformen mit Windows 7/8/8.1/10 oder Windows Server 2008 R2/2012/2012 R2/2016 nicht verfügbar.

- VSApiNt
- tmlwf (für Computer unter Windows Server 2008/7/8/8.1/10/Server 2012/2016)
- tmwfp (für Computer unter Windows Server 2008/7/8/8.1/10/Server 2012/2016)
- tmevtmgr
- tmeevw (für Computer unter Windows 7/8/8.1/10/Server 2008 R2/ Server 2012/2012 R2/2016)
- tmusa (für Computer unter Windows 7/8/8.1/10/Server 2008 R2/ Server 2012/2012 R2/2016)

9. Schließen Sie den Registrierungseditor.
10. Löschen Sie Trend Micro Treiber und Dienste manuell mit einem Befehlszeilen-Editor (nur Windows 8/8.1/10/Server 2012) unter Verwendung der folgenden Befehle:

    - `sc delete tmeevw`

      Für Windows 7/8/8.1/10 und Windows Server 2008 R2/2012/2012 R2/2016

- `sc delete tmusa`

  Für Windows 7/8/8.1/10 und Windows Server 2008 R2/2012/2012 R2/2016

- `sc delete tmccsf`
- `sc delete tmproxy`

  Für Windows Server 2008

- `sc delete tmtdi`

  Für Windows Server 2008

Hinweis

Führen Sie den Befehlszeilen-Editor mit Administratorrechten aus (z. B., indem Sie mit der rechten Maustaste auf `cmd.exe` und dann mit der linken Maustaste auf **Als Administrator ausführen** klicken), um sicherzustellen, dass die Befehle erfolgreich ausgeführt werden.

11. Starten Sie den Agent-Endpunkt neu.
12. Wenn keine anderen Produkte von Trend Micro auf dem Endpunkt installiert sind, löschen Sie den `Trend Micro` Installationsordner (in der Regel `C:\Programme\Trend Micro`). Auf 64-Bit-Computern befindet sich der Installationsordner unter `C:\Programme (x86)\Trend Micro`.
13. Wenn andere Produkte von Trend Micro installiert sind, löschen Sie die folgenden Ordner:

    - <Installationsordner des Agents>
    - Den Ordner `BM` im Installationsordner von `Trend Micro` (normalerweise `C:\Programme\Trend Micro\BM` (bei 32-Bit-Systemen) und `C:\Programme (x86)\Trend Micro\BM` (bei 64-Bit-Systemen))

Kapitel 6

Schutzfunktionen aktuell halten

In diesem Kapitel werden die Komponenten und Update-Verfahren von OfficeScan beschrieben.

Es werden folgende Themen behandelt:

- *OfficeScan Komponenten und Programme auf Seite 6-2*
- *Update-Übersicht auf Seite 6-12*
- *OfficeScan Server-Updates auf Seite 6-16*
- *Updates für den integrierten Smart Protection Server auf Seite 6-29*
- *OfficeScan Agent-Updates auf Seite 6-29*
- *Update-Agents auf Seite 6-59*
- *Komponenten-Update - Zusammenfassung auf Seite 6-68*

OfficeScan Komponenten und Programme

OfficeScan verwendet Komponenten und Programme, mit denen agent-Computer vor den neuesten Sicherheitsrisiken geschützt sind. Halten Sie diese Komponenten und Programme mit manuellen oder zeitgesteuerten Updates auf dem neuesten Stand.

Zusätzlich zu den Komponenten erhalten OfficeScan agents aktualisierte Konfigurationsdateien vom OfficeScan Server. Agents benötigen die Konfigurationsdateien, um neue Einstellungen anzuwenden. Bei jeder änderung der OfficeScan Einstellungen über die Webkonsole ändern sich auch die Konfigurationsdateien.

Die Komponenten sind wie folgt gruppiert:

- *Antiviren-Komponenten auf Seite 6-3*
- *Anti-Spyware-Komponenten auf Seite 6-7*
- *Damage Cleanup Services-Komponenten auf Seite 6-7*
- *Firewall-Komponenten auf Seite 6-8*
- *Komponenten der Verhaltensüberwachung auf Seite 6-8*
- *Komponenten des Diensts für verdächtige Verbindungen auf Seite 6-10*
- *Lösung für Browser-Schwachstellen auf Seite 6-10*
- *Programme auf Seite 6-10*
- *Web-Reputation-Komponenten auf Seite 6-12*

Antiviren-Komponenten

KOMPONENTE	BESCHREIBUNG
Viren-Scan-Engine (32/64 Bit)	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
Viren-Pattern	Das Viren-Pattern enthält Informationen, die OfficeScan 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.
Virensuchtreiber	Der Virensuchtreiber überwacht die Aktionen, die Benutzer an Dateien durchführen. Diese Aktionen können das Öffnen und Schließen einer Datei sowie die Ausführung einer Anwendung sein. Es gibt zwei Versionen dieses Treibers. Hierbei handelt es sich um `TmXPFlt.sys` und `TmPreFlt.sys`. `TmXPFlt.sys` wird für die Echtzeitkonfiguration der Viren-Scan-Engine und `TmPreFlt.sys` zur Überwachung von Benutzeraktionen verwendet. **Hinweis** Diese Komponente wird nicht in der Konsole angezeigt. Um die Version dieser Komponente zu überprüfen, wechseln Sie zum Verzeichnis <*Installationsordner des Servers*>`\PCCSRV\Pccnt\Drv`. Klicken Sie mit der rechten Maustaste auf die `.sys`-Datei, wählen Sie **Eigenschaften**, und navigieren Sie zur Registerkarte **Version**.

KOMPONENTE	BESCHREIBUNG
Pattern der intelligenten Suche	Im intelligenten Suchmodus verwenden OfficeScan 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 **Pattern der intelligenten Suche**. Das **Smart Scan Agent Pattern** enthält alle anderen Pattern, die sich nicht im Pattern der intelligenten Suche befinden. Der OfficeScan Agent sucht mit Hilfe des **Agent-Pattern der intelligenten Suche** nach Sicherheitsbedrohungen. OfficeScan 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 OfficeScan server gehosteten Dienst. Der Suchserver überprüft das Risiko mit dem**Pattern der intelligenten Suche**. Der OfficeScan Agent legt das vom Scan Server gelieferte Suchabfrageergebnis zur Verbesserung der Suchleistung in einem Zwischenspeicher ab.
Smart Scan Agent Pattern	
IntelliTrap Pattern	Das IntelliTrap Pattern erkennt in Echtzeit komprimierte Dateien, die als ausführbare Dateien gepackt sind. Weitere Informationen finden Sie unter *IntelliTrap auf Seite E-7*.
IntelliTrap Ausnahme-Pattern	Das IntelliTrap Ausnahme-Pattern enthält eine Liste „zulässiger“ komprimierter Dateien.

KOMPONENTE	BESCHREIBUNG
Speicher-Inspektions-Pattern	Die Echtzeitsuche wertet mit Hilfe des Patterns der Arbeitsspeicherprüfung ausführbare komprimierte Dateien aus, die durch die Verhaltensüberwachung identifiziert werden. Die Echtzeitsuche führt die folgenden Aktionen für ausführbare komprimierte Dateien aus: 1. Eine Zuordnungsdatei wird im Arbeitsspeicher erstellt, nachdem der Prozess-Image-Pfad überprüft wurde. **Hinweis** Die Suchausschlussliste hat Vorrang vor dem Durchsuchen der Dateien. 2. Die Prozess-ID wird an den erweiterten Schutzdienst gesendet, der dann folgende Aktionen ausführt: a. Mit Hilfe der Viren-Scan-Engine wird der Arbeitsspeicher überprüft. b. Der Prozess wird über allgemein zulässige Listen für Windows-Systemdateien, für digital signierte Dateien aus zuverlässigen Quellen und für mit Trend Micro getestete Dateien gefiltert. Nachdem überprüft wurde, dass eine Datei sicher ist, führt OfficeScan keine Aktionen für die Datei aus. 3. Nach der Verarbeitung der Arbeitsspeichersuche sendet der erweiterte Schutzdienst die Ergebnisse an die Echtzeitsuche. 4. Die Echtzeitsuche stellt dann entdeckte Malware-Bedrohungen unter Quarantäne und beendet den Prozess.
Maschine für Kontextbezogene Intelligenz 32/64-Bit	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 vorrausschaunde Maschinenlernen gesendet werden.
Muster für kontextbezogene Intelligenz	Das Muster für kontextbezogene Intelligenz enthält eine Liste "geduldeter" Verhaltensweisen, die für bekannte Bedrohungen nicht relevant sind.

KOMPONENTE	BESCHREIBUNG
Abfragehandhabung für kontextbezogene Intelligenz 32/64-Bit	Der Abfragehandhabung für kontextbezogene Intelligenz verarbeitet von der Maschine für Kontextbezogene Intelligenz erkanntes Verhalten und sendet den Bericht an das Modul für vorrausschaunde Maschinenlernen.
Fortgeschrittenes Bedrohungssuchmaschine 32/64-Bit	Die Fortgeschrittenes Bedrohungssuchmaschine extrahiert Dateifunktionen aus selten vorkommenden Dateien und sendet die Daten an das Modul für vorrausschaunde Maschinenlernen.
Fortgeschrittenes Bedrohungskorrelationsmuster	Das Fortgeschrittenes Bedrohungskorrelationsmuster enthält eine Liste mit Dateifunktionen, die für bekannte Bedrohungen nicht relevant sind.

Die Scan Engine aktualisieren

Da die zeitkritischsten Informationen über Viren/Malware im Viren-Pattern gespeichert sind, kann Trend Micro die Anzahl der Scan-Engine-Updates auf ein Mindestmaß reduzieren und gleichzeitig ein hohes Schutzniveau beibehalten. Dennoch stellt Trend Micro in regelmäßigen Abständen neue Versionen der Scan Engine zur Verfügung, Trend Micro und zwar in den folgenden Fällen:

- Neue Technologien zur Suche und Entdeckung von Viren werden in die Software integriert
- Neue, potenziell gefährliche Viren/Malware wurden entdeckt, auf welche die Scan Engine nicht reagieren kann.
- Die Suchleistung wurde verbessert.
- Neue Dateiformate, Skriptsprachen, Kodierungen und/oder Komprimierungsformate werden hinzugefügt.

Anti-Spyware-Komponenten

Komponente	Beschreibung
Spyware/Grayware-Pattern	Das Spyware-/Grayware-Pattern erkennt Spyware/Grayware in Dateien und Programmen, Speichermodulen, der Windows Registrierung und in URL-Verknüpfungen.
Spyware/Grayware Scan Engine (32/64 Bit)	Die Spyware/Grayware Scan Engine sucht anhand der entsprechenden Suchaktionen nach Spyware/Grayware.
Spyware-Aktivmonitor-Pattern	Das Spyware-Aktivmonitor-Pattern wird für die Echtzeitsuche nach Spyware/Grayware verwendet. Nur agents der herkömmlichen Suche verwenden dieses Pattern. agents der intelligenten Suche verwenden das Agent-Pattern der intelligenten Suche für die Echtzeitsuche nach Spyware/Grayware. Agents senden Suchabfragen an eine Smart Protection Quelle, wenn das Risiko des Suchziels während der Suche nicht bestimmt werden kann.

Damage Cleanup Services-Komponenten

Komponente	Beschreibung
Damage-Cleanup Engine 32/64 Bit	Die Damage Cleanup Engine sucht und entfernt Trojaner und Trojaner-Prozesse.
Damage Cleanup Template	Damage Cleanup Template: Die Damage Cleanup Engine verwendet dieses Template, um z. B. Trojaner-Dateien oder -Prozesse zu erkennen und zu beseitigen.
Early Boot Cleanup Driver 32-/64-Bit	Der Trend Micro Early Boot Cleanup Driver lädt vor den Betriebssystemtreibern, was das Erkennen und Sperren von Boot-Rootkits ermöglicht. Nachdem der OfficeScan Agent geladen wurde, werden vom Trend Micro Early Boot Cleanup Driver die Damage Cleanup Services zum Säubern des Rootkits aufgerufen.

Firewall-Komponenten

KOMPONENTE	BESCHREIBUNG
Allgemeiner Firewall-Treiber 32-/64-Bit	Der Treiber für die allgemeine Firewall wird mit dem Pattern der allgemeinen Firewall verwendet, um nach Netzwerkviren auf agent-Endpunkten zu suchen. Dieser Treiber unterstützt 32-Bit- und 64-Bit-Plattformen.
Pattern der allgemeinen Firewall	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.

Komponenten der Verhaltensüberwachung

KOMPONENTE	BESCHREIBUNG
Erkennungs-Pattern der Verhaltensüberwachung (32/64 Bit)	Dieses Pattern enthält die Regeln für die Erkennung von verdächtigem Bedrohungsverhalten.
Kerntreiber der Verhaltensüberwachung 32/64 Bit	Dieser Treiber im Kernelmodus überwacht Systemereignisse und leitet sie an den Kerndienst der Verhaltensüberwachung zwecks Durchsetzung von Sicherheitsrichtlinien weiter.
Kerndienst der Verhaltensüberwachung 32/64 Bit	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	Der Treiber der Verhaltensüberwachung verwendet dieses Pattern, um normale Systemereignisse zu erkennen und diese bei der Durchsetzung von Sicherheitsrichtlinien auszuschließen.

KOMPONENTE	BESCHREIBUNG
Pattern für digitale Signaturen	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	Der Kerndienst der Verhaltensüberwachung überprüft Systemereignisse hinsichtlich der Richtlinien in diesem Pattern.
Auslöse-Pattern zum Durchsuchen des Speichers (32/64 Bit)	Die Verhaltensüberwachung identifiziert mit dem Pattern zum Auslösen der Arbeitsspeichersuche potenzielle Bedrohungen durch die Erkennung der folgenden Vorgänge: • Dateischreibvorgänge • Registrierungsschreibvorgänge • Erstellung neuer Prozesse Wenn einer dieser Vorgänge identifiziert wurde, ruft die Verhaltensüberwachung das Pattern der Arbeitsspeicherprüfung der Echtzeitsuche auf, um nach Sicherheitsrisiken zu suchen. Weitere Informationen zu Echtzeitsuchvorgängen finden Sie unter *Pattern der Arbeitsspeicherprüfung auf Seite 6-5*.
Schadensbehebungsmuster	Das Schadensbehebungsmuster enthält Richtlinien, die zur Überwachung von verdächtigem Bedrohungsverhalten verwendet werden.
Muster der Programmsinspektionsüberwachung	Das Muster der Programmsinspektionsüberwachung überwacht und speichert Prüfpunkte, die zur Verhaltensüberwachung verwendet werden.

Komponenten des Diensts für verdächtige Verbindungen

Komponente	Beschreibung
Allgemeine C&C-IP-Liste	Die allgemeine C&C-IP-Liste wird zusammen mit der Network Content Inspection Engine (NCIE) verwendet, um Netzwerkverbindungen zu bekannten C&C-Servern zu erkennen. NCIE erkennt C&C-Serververbindungen über jeden Netzwerkkanal. OfficeScan protokolliert alle Daten der Verbindungen mit Servern in der globalen C&C-IP-Liste, damit sie ausgewertet werden können.
Pattern-Relevanzregeln	Der Dienst für verdächtige Verbindungen verwendet die Pattern-Relevanzregeln, um eindeutige Signaturen von Malware-Familien in den Kopfzeilen von Netzwerkpaketen zu erkennen.

Lösung für Browser-Schwachstellen

Komponente	Beschreibung
Pattern für die Prävention von Angriffen auf Browser	Dieses Pattern identifiziert die aktuellsten Webbrowserangriffe und verhindert, dass die Angriffe zur Gefährdung des Webbrowsers verwendet werden.
Einheitliches Skriptanalysemuster	Dieses Pattern analysiert die Skripte in Webseiten und identifiziert schädliche Skripte.

Programme

Komponente	Beschreibung
OfficeScan Agent	Das OfficeScan Agent-Programm dient dem Schutz vor Sicherheitsrisiken.

KOMPONENTE	BESCHREIBUNG
Hotfixes, Patches und Service Packs	Nach der Veröffentlichung eines Produkts entwickelt Trend Micro oft Folgendes zur Problembehebung, Leistungsverbesserung oder Funktionserweiterung: • *Hotfix auf Seite E-5* • *Patch auf Seite E-10* • *Sicherheits-Patch auf Seite E-11* • *Service Pack auf Seite E-12* 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.

Hotfix- und Patch-Verlauf

Wenn der OfficeScan Server Hotfixes oder Patch-Dateien an OfficeScan Agents verteilt, zeichnet das OfficeScan Agent-Programm Informationen zum Hotfix oder Patch im Registrierungseditor auf. Sie können diese Informationen für mehrere agents mit Hilfe von Verwaltungssoftware wie Microsoft SMS, LANDesk™ oder BigFix™ abfragen.

Hinweis

Diese Funktion zeichnet keine Hotfixes und Patches auf, die nur an den Server verteilt werden.

Diese Funktion steht ab OfficeScan 8.0 mit Service Pack 1 und Patch 3.1 zur Verfügung.

- Agents, bei denen ein Upgrade von Version 8.0 Service Pack 1 mit Patch 3.1 oder höher durchgeführt wurde, zeichnen installierte Hotfixes und Patches für Version 8.0 und höher auf.

- Agents, bei denen ein Upgrade von früheren Versionen als 8.0 und Service Pack 1 mit Patch 3.1 durchgeführt wurde, zeichnen installierte Hotfixes und Patches für Version 10.0 und höher auf.

Die Informationen werden in den folgenden Schlüsseln gespeichert:

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`
- Für Computer auf einer x64-Plattform:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\ PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`

Prüfen Sie, ob die folgenden Schlüssel vorhanden sind:

- **Schlüssel**: `HotFix_installed`

  Typ: `REG_SZ`

  Wert: `<Hotfix- oder Patch-Name>`
- **Schlüssel**: `HotfixInstalledNum`

  Typ: `DWORD`

  Wert: `<Hotfix- oder Patch-Nummer>`

Web-Reputation-Komponenten

KOMPONENTE	BESCHREIBUNG
URL-Filter-Engine	Die URL-Filter-Engine erleichtert die Kommunikation zwischen OfficeScan und dem Trend Micro URL-Filterdienst, der URLs bewertet und die Ergebnisse an OfficeScan weiterleitet.

Update-Übersicht

Alle Komponenten-Updates stammen ursprünglich vom Trend Micro ActiveUpdate Server. Bei Verfügbarkeit von Updates laden der OfficeScan Server und die Smart

Protection Quellen (Smart Protection Server oder Smart Protection Network) die aktuellen Komponenten herunter. Beim Komponenten-Download gibt es keine Überlappungen zwischen dem OfficeScan Server und der Smart Protection Quelle, da beide unterschiedliche Komponentenpakete herunterladen.

Hinweis

Sie können sowohl den OfficeScan Server als auch den Smart Protection Server so konfigurieren, dass diese vom Trend Micro ActiveUpdate Server oder einer anderen Adresse Updates beziehen. Dazu müssen Sie eine benutzerdefinierte Update-Adresse einrichten. Sollten Sie beim Einrichten dieser Update-Adresse Hilfe benötigen, wenden Sie sich an Ihren Support-Anbieter.

OfficeScan Server- und OfficeScan Agent-Update

Der OfficeScan Server lädt die meisten von den agents benötigten Komponenten herunter. Das Pattern der intelligenten Suche stellt hierbei die einzige Ausnahme dar, und wird von einemSmart Protection Server heruntergeladen.

Wird mit dem OfficeScan Server eine große Anzahl von agents verwaltet, können die Updates einen Großteil der Servercomputer-Ressourcen verbrauchen und somit die Stabilität und Leistung des Servers beeinflussen. Um diesem Problem entgegenzuwirken, hat OfficeScan eine Update-Agent-Funktion, die bestimmten agents ermöglicht, bei der Verteilung von Updates an andere agents mitzuwirken.

In der folgenden Tabelle sind die verschiedenen Optionen aufgeführt, die für das Komponenten-Update bei OfficeScan Servern und agents verfügbar sind, sowie Empfehlungen, wann diese am besten zur Anwendung kommen:

TABELLE 6-1. Update-Optionen für Server und Agent

UPDATE-OPTION	BESCHREIBUNG	EMPFEHLUNG
ActiveUpdate server > **Server** > **Agent**	Der OfficeScan Server empfängt aktualisierte Komponenten vom Trend Micro ActiveUpdate Server (oder einer anderen Update-Adresse) und startet das Komponenten-Update auf agents.	Wenden Sie diese Methode an, wenn es zwischen dem OfficeScan Server und den agents keine Netzwerkabschnitte mit geringer Bandbreite gibt.
ActiveUpdate Server > **Server** > **Update-Agents** > **Agent**	Der OfficeScan Server empfängt aktualisierte Komponenten vom ActiveUpdate Server (oder einer anderen Update-Adresse) und startet das Komponenten-Update auf agents. Agents mit der Funktion eines Update-Agents fordern andere agents dann zum Update der Komponenten auf.	Verwenden Sie diese Methode zum Ausgleich der Netzwerkbelastung, wenn einige der Netzwerkabschnitte zwischen OfficeScan Server und agents eine geringe Bandbreite aufweisen.
ActiveUpdate Server > **Update-Agents** > **Agent**	Die Update-Agents erhalten aktualisierte Komponenten direkt vom ActiveUpdate Server (oder einer anderen Update-Adresse) und senden Benachrichtigungen zum Update der Komponenten an die agents.	Verwenden Sie diese Methode nur, wenn das Update der Update-Agents über den OfficeScan Server oder andere Update-Agents nicht problemlos möglich ist. In den meisten Fällen erhalten Update-Agents die Updates schneller vom OfficeScan Server oder anderen Update-Agents als von einer externen Update-Adresse.

UPDATE-OPTION	BESCHREIBUNG	EMPFEHLUNG
ActiveUpdate server > **Agent**	OfficeScan agents erhalten aktualisierte Komponenten direkt vom ActiveUpdate Server (oder einer anderen Update-Adresse).	Wenden Sie diese Methode nur dann an, wenn die agents nicht über den OfficeScan Server oder Update-Agents aktualisiert werden können. In den meisten Fällen erhalten die agents die Updates schneller über den OfficeScan Server oder über Update-Agents als von einer externen Update-Adresse.

Update der Smart Protection Quelle

Eine Smart Protection Quelle (Smart Protection Server oder Smart Protection Network) lädt das Pattern der intelligenten Suche herunter. agents der intelligenten Suche laden dieses Pattern nicht herunter. Agents verifizieren potenzielle Bedrohungen mit Hilfe des Patterns, indem sie Suchabfragen an die Smart Protection Quelle senden.

Hinweis

Weitere Informationen zu Smart Protection Quellen finden Sie unter *Smart Protection Quellen auf Seite 4-6*.

In der folgenden Tabelle ist die Vorgehensweise beim Update für Smart Protection Quellen beschrieben.

TABELLE 6-2. Update-Prozess der Smart Protection Quelle

UPDATE-VORGANG	BESCHREIBUNG
ActiveUpdate server > **Smart Protection Network**	Das Trend Micro Smart Protection Network erhält Updates vom Trend Micro ActiveUpdate Server. Smart Scan agents, die nicht mit dem Unternehmensnetzwerk verbunden ist, senden Abfragen an das Trend Micro Smart Protection Network.

Update-Vorgang	Beschreibung
ActiveUpdate server > **Smart Protection Server**	Der Smart Protection Server (integriert oder eigenständig) erhält Updates vom Trend Micro ActiveUpdate Server. Smart Protection agents, die mit dem Unternehmensnetzwerk verbunden sind, senden Anfragen an den Smart Protection Server.
Smart Protection Network > **Smart Protection Server**	Ein Smart Protection Server (integriert oder eigenständig) erhält Updates vom Trend Micro Smart Protection Network. Smart Protection agents, die mit dem Unternehmensnetzwerk verbunden sind, senden Anfragen an den Smart Protection Server.

OfficeScan Server-Updates

Der OfficeScan Server lädt die folgenden Komponenten herunter und verteilt sie anschließend an die Agents:

Tabelle 6-3. Vom OfficeScan Server heruntergeladene Komponenten

Komponente	Verteilung	
	Agents der herkömmlichen Suche	Agents der intelligenten Suche
Virenschutz		
Smart Scan Agent Pattern	Nein	Ja
Viren-Pattern	Ja	Nein
IntelliTrap Pattern	Ja	Ja
IntelliTrap Ausnahme-Pattern	Ja	Ja
Viren-Scan-Engine (32/64 Bit)	Ja	Ja
Speicher-Inspektions-Pattern	Ja	Ja

Komponente	Verteilung	
	Agents der herkömmlichen Suche	Agents der intelligenten Suche
Frühstart Anti-Malware Muster 32-/64-Bit	Ja	Ja
Maschine für Kontextbezogene Intelligenz 32/64-Bit	Ja	Ja
Muster für kontextbezogene Intelligenz	Ja	Ja
Abfragehandhabung für kontextbezogene Intelligenz 32/64-Bit	Ja	Ja
Fortgeschrittenes Bedrohungssuchmaschine 32/64-Bit	Ja	Ja
Fortgeschrittenes Bedrohungskorrelationsmuster	Ja	Ja
Anti-spyware		
Spyware/Grayware-Pattern	Ja	Ja
Spyware-Aktivmonitor-Pattern	Ja	Nein
Spyware/Grayware Scan Engine (32/64 Bit)	Ja	Ja
Damage Cleanup Services		
Damage Cleanup Template	Ja	Ja
Damage-Cleanup Engine 32/64 Bit	Ja	Ja
Early Boot Cleanup Driver 32-/64-Bit	Ja	Ja
Firewall		
Pattern der allgemeinen Firewall	Ja	Ja
Komponenten der Verhaltensüberwachung		

Komponente	Verteilung	
	Agents der herkömmlichen Suche	Agents der intelligenten Suche
Erkennungs-Pattern der Verhaltensüberwachung (32/64 Bit)	Ja	Ja
Kerntreiber der Verhaltensüberwachung 32/64 Bit	Ja	Ja
Kerndienst der Verhaltensüberwachung 32/64 Bit	Ja	Ja
Pattern zur Konfiguration der Verhaltensüberwachung	Ja	Ja
Pattern der Richtliniendurchsetzung	Ja	Ja
Pattern für digitale Signaturen	Ja	Ja
Auslöse-Pattern zum Durchsuchen des Speichers (32/64 Bit)	Ja	Ja
Muster der Programmsinspektionsüberwachung	Ja	Ja
Schadensbehebungsmuster	Ja	Ja
Verdächtige Verbindungen		
Allgemeine C&C-IP-Liste	Ja	Ja
Pattern-Relevanzregeln	Ja	Ja
Lösung für Browser-Schwachstellen		
Pattern für die Prävention von Angriffen auf Browser	Ja	Ja
Einheitliches Skriptanalysemuster	Ja	Ja

Update-Hinweise und -Empfehlungen:

- Um dem Server die Verteilung der aktualisierten Komponenten an die Agents zu ermöglichen, aktivieren Sie die Funktion automatisches Agent-Update. Weitere Informationen finden Sie unter *OfficeScan Agent Automatische Updates auf Seite 6-41*. Ist die Funktion automatisches Agent-Update deaktiviert, lädt der Server zwar die Updates herunter, verteilt sie aber nicht auf die Agents.

- Ein reiner IPv6 OfficeScan Server kann Updates nicht direkt auf reine IPv4-Agents verteilen. Ebenso kann ein reiner IPv4 OfficeScan Server Updates nicht direkt auf reine IPv6-Agents verteilen. Ein Dual-Stack-Proxy-Server (z. B. DeleGate), der IP-Adressen umwandeln kann, muss zulassen, dass der OfficeScan Server Updates auf die Agents verteilen kann.

- Damit der Virenschutz immer aktuell ist, veröffentlicht Trend Micro regelmäßig neue Pattern-Dateien. Da Pattern-Datei-Updates regelmäßig verfügbar sind, verwendet OfficeScan den Mechanismus der „Komponentenduplizierung“, der schnellere Downloads von Pattern-Dateien ermöglicht. Weitere Informationen finden Sie unter *OfficeScan Server-Komponentenduplizierung auf Seite 6-22*.

- Wenn die Verbindung zum Internet über einen Proxy-Server hergestellt wird, müssen Sie für den Download der Updates die richtigen Proxy-Einstellungen verwenden.

- Fügen Sie im Dashboard der Webkonsole das Widget **Agent-Updates** hinzu, um die aktuellen Komponentenversionen anzuzeigen und die Anzahl der Agents mit aktualisierten und veralteten Komponenten zu ermitteln.

OfficeScan Server-Update-Adressen

Konfigurieren Sie den OfficeScan Server so, dass Komponenten vom Trend Micro ActiveUpdate Server oder einer anderen Adresse heruntergeladen werden. Sie können auch eine andere Quelle festlegen, wenn der OfficeScan Server den ActiveUpdate Server nicht direkt erreichen kann. Ein Beispielszenario finden Sie unter *Updates für isolierte OfficeScan Server auf Seite 6-25*.

Nach dem Download aller verfügbaren Updates kann der Server automatisch gemäß den von Ihnen unter **Updates** > **Agents** > **Automatisches Update** angegebenen Einstellungen die agents zum Komponenten-Update auffordern. Ist das Komponenten-Update unbedingt notwendig, sollte der Server die agents umgehend benachrichtigen.

Die entsprechenden Einstellungen nehmen Sie unter **Updates** > **Agents** > **Manuelles Update** vor.

Hinweis

Wenn Sie unter **Updates** > **Agents** > **Automatisches Update** keinen Verteilungszeitplan und keine ereignisbedingten Update-Einstellungen angeben, lädt der Server zwar die Updates herunter, fordert die agents aber nicht zum Update auf.

IPv6-Unterstützung für OfficeScan Server-Updates

Ein reiner IPv6-OfficeScan Server kann Updates nicht direkt aus reinen IPv4-Update-Adressen erhalten wie:

- Trend Micro ActiveUpdate Server
- Jede reine, benutzerdefinierte IPv4-Update-Adresse

Ebenso kann ein reiner IPv4 OfficeScan Server keine Updates direkt von reinen benutzerdefinierten IPv6-Quellen erhalten.

Ein Dual-Stack-Proxy-Server, der IP-Adressen wie DeleGate konvertieren kann, muss ermöglichen, dass der Server eine Verbindung zu den Update-Adressen herstellen kann.

Proxy für Updates von OfficeScan Server

Sie können auf dem Server-Computer gehostete Serverprogramme so konfigurieren, dass beim Herunterladen von Updates vom Trend Micro ActiveUpdate Server Proxy-Einstellungen verwendet werden. Zu den Serverprogrammen gehören der OfficeScan Server und der integrierte Smart Protection Server.

Proxy-Einstellungen für Server konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Einstellungen** > **Proxy**.

2. Klicken Sie auf die Registerkarte **Server**.
3. Wählen Sie die Option **Proxy-Server beim Herstellen einer Verbindung zu gehosteten Trend Micro Servern für Pattern-, Engine- und Lizenz-Updates verwenden** aus.
4. Geben Sie das Proxy-Protokoll, den Servernamen oder die IPv4-/IPv6-Adresse sowie die Portnummer an.
5. Falls der Proxy-Server eine Authentifizierung verlangt, geben Sie den Benutzernamen und das Kennwort ein.
6. Klicken Sie auf **Speichern**.

Die Update-Adresse des Servers konfigurieren

Prozedur

1. Navigieren Sie zu **Updates** > **Server** > **Update-Adresse**.
2. Wählen Sie den Ort aus, von dem das Update heruntergeladen werden soll.

   Stellen Sie bei Auswahl des ActiveUpdate Servers sicher, dass der Server mit dem Internet verbunden ist, und, falls Sie einen Proxy-Server verwenden, testen Sie, ob die Internet-Verbindung mit den Proxy-Einstellungen aufgebaut werden kann. Weitere Informationen finden Sie unter *Proxy für Updates von OfficeScan Server auf Seite 6-20*.

   Wenn Sie eine benutzerdefinierte Update-Adresse auswählen, konfigurieren Sie die entsprechende Umgebung und die Update-Ressourcen diese Update-Adresse. Stellen Sie auch sicher, dass der Servercomputer mit dieser Update-Adresse verbunden ist. Sollten Sie beim Einrichten einer Update-Adresse Hilfe benötigen, wenden Sie sich an Ihren Support-Anbieter.

   Hinweis

   Beim Download der Komponenten von der Update-Adresse verwendet der OfficeScan Server die Komponentenduplizierung. Weitere Informationen finden Sie unter *OfficeScan Server-Komponentenduplizierung auf Seite 6-22*.

3. Klicken Sie auf **Speichern**.

OfficeScan Server-Komponentenduplizierung

Zusammen mit der neuesten Version einer vollständigen Pattern-Datei werden auf dem Trend Micro ActiveUpdate Server auch 14 "inkrementelle Pattern-Dateien" zum Download zur Verfügung gestellt. Inkrementelle Pattern sind kleinere Versionen der vollständigen Pattern-Datei und umfassen den Unterschied zwischen der aktuellen und vorhergehenden vollständigen Versionen der Pattern-Datei. Wenn beispielsweise 175 die aktuelle 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 Netzwerkdatenverkehr, der durch den Download des aktuellen Patterns erzeugt wird, dupliziert OfficeScan Komponenten. Bei dieser Methode des Komponenten-Updates lädt der OfficeScan Server oder der Update-Agent nur inkrementelle Pattern herunter. Weitere Informationen darüber, wie der Update-Agent Komponenten dupliziert, finden Sie unter *Update-Agent-Komponenten duplizieren auf Seite 6-65*.

Komponentenduplizierung betrifft folgende Komponenten:

- Viren-Pattern
- Smart Scan Agent Pattern
- Damage Cleanup Template
- IntelliTrap Ausnahme-Pattern
- Spyware/Grayware-Pattern
- Spyware-Aktivmonitor-Pattern

Szenario einer Komponentenduplizierung

Das folgende Beispiel erläutert den Dupliziervorgang für den Server:

TABELLE 6-4. Szenario einer Server-Komponentenduplizierung

Vollständige Pattern auf dem OfficeScan Server	Aktuelle Version: 171 Andere verfügbare Versionen: 169	167	165	161	159	
Aktuelle Version auf dem ActiveUpdate Server	173.175	171.175	169.175	167.175	165.175	163.175
	161.175	159.175	157.175	155.175	153.175	151.175
	149.175	147.175				

1. Der OfficeScan Server vergleicht die aktuelle, vollständige Pattern-Version mit der neuesten Version auf dem ActiveUpdate Server. Beträgt der Unterschied zwischen beiden Versionen maximal 14, lädt der Server nur das inkrementelle Pattern herunter, das den Unterschied zwischen den beiden Versionen umfasst.

   Hinweis

   Ist der Unterschied größer als 14, lädt der Server automatisch die vollständige Version der Pattern-Datei und 14 inkrementelle Pattern herunter.

   Auf das Beispiel bezogen bedeutet das:

   - Der Unterschied zwischen den Versionen 171 und 175 ist zwei. Mit anderen Worten: Der Server verfügt nicht über die Versionen 173 und 175.
   - Der Server lädt das inkrementelle Pattern 171.175 herunter. Das inkrementelle Pattern umfasst den Unterschied zwischen den Versionen 171 und 175.

2. Der Server integriert das inkrementelle Pattern in sein aktuelles vollständiges Pattern und erhält so das neueste vollständige Pattern.

   Auf das Beispiel bezogen bedeutet das:

   - Auf dem Server integriert OfficeScan die Version 171 in das inkrementelle Pattern 171.175, um die Version 175 zu erhalten.
   - Der Server verfügt über ein inkrementelles Pattern (171.175) und das neueste vollständige Pattern (Version 175).

3. Der Server erzeugt inkrementelle Pattern basierend auf den anderen vollständigen Pattern, die auf dem Server verfügbar sind. Erzeugt der Server diese inkrementellen Pattern nicht, laden die agents, die den Download früherer inkrementeller Pattern versäumt haben, automatisch die vollständige Pattern-Datei herunter. Dadurch wird zusätzlicher Netzwerkdatenverkehr erzeugt.

   Auf das Beispiel bezogen bedeutet das:

   - Da der Server bereits über die Pattern-Versionen 169, 167, 165, 163, 161, 159 verfügt, kann er die folgenden inkrementellen Pattern erzeugen:

     169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - Der Server muss nicht Version 171 verwenden, da er bereits über das inkrementelle Pattern 171.175 verfügt.

   - Auf dem Server befinden sich nun sieben inkrementelle Pattern:

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - Der Server behält die letzten sieben vollständigen Pattern-Versionen (175, 171, 169, 167, 165, 163, 161). Ältere Versionen werden gelöscht (Version 159).

4. Der Server vergleicht seine aktuellen inkrementellen Pattern mit den auf dem ActiveUpdate Server verfügbaren inkrementellen Pattern und lädt die ihm fehlenden Dateien herunter.

   Auf das Beispiel bezogen bedeutet das:

   - Auf dem ActiveUpdate Server befinden sich nun 14 inkrementelle Pattern:

     173.175, 171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

   - Auf dem OfficeScan Server befinden sich nun 7 inkrementelle Pattern:

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - Auf dem OfficeScan Server befinden sich nun 7 inkrementelle Pattern:

     173.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

   - Auf dem Server befinden sich nun alle inkrementellen Pattern, die auf dem ActiveUpdate Server verfügbar sind.

5. Das neueste vollständige Pattern und die 14 inkrementellen Pattern werden den agents zur Verfügung gestellt.

Updates für isolierte OfficeScan Server

Gehört ein OfficeScan Server zu einem völlig von außen isolierten Netzwerk, können Sie die Serverkomponenten auf den neuesten Stand bringen, indem Sie ihn durch eine interne Quelle, die die neuesten Komponenten enthält, aktualisieren.

In diesem Themenbereich werden die Aufgaben dargestellt, die Sie durchführen müssen, um einen isolierten OfficeScan Server zu aktualisieren.

Isolierte OfficeScan Server aktualisieren

Dieser Prozess ist nur zu Ihrer Information. Wenn Sie alle Aufgaben dieses Ablaufs erfüllen können, fragen Sie Ihren Support-Anbieter nach detaillierten Anweisungen zu jeder Aufgabe.

Prozedur

1. Bestimmen Sie die Update-Adresse, wie z. B. Trend Micro Control Manager oder irgendeinen Host-Computer. Die Update-Adresse muss über Folgendes verfügen:
   - Eine zuverlässige Internetverbindung muss bestehen, damit die neuesten Komponenten vom Trend Micro ActiveUpdate Server heruntergeladen werden können. Ohne Internetverbindung haben Sie nur die Möglichkeit, sich die neuesten Komponenten bei Trend Micro zu besorgen und sie dann in die Update-Adresse zu kopieren.
   - Eine Verbindung mit dem OfficeScan Server. Konfigurieren Sie Proxy-Einstellungen, wenn zwischen dem OfficeScan Server und der Update-Adresse ein Proxy-Server ist. Weitere Informationen finden Sie unter *Proxy für Updates von OfficeScan Server auf Seite 6-20*.
   - Ausreichend Speicherplatz für heruntergeladene Komponenten
2. Weisen Sie dem OfficeScan Server die neuen Update-Adressen zu. Weitere Informationen finden Sie unter *OfficeScan Server-Update-Adressen auf Seite 6-19*.

3. Identifizieren Sie die Komponenten, die der Server auf die agents verteilt. Eine Liste der verteilbaren Komponenten finden Sie unter *OfficeScan Agent-Updates auf Seite 6-29*.

Tipp

Um festzustellen, ob eine Komponente auf agents verteilt wird, können Sie beispielsweise auf der Webkonsole zum Fenster **Übersicht aktualisieren** navigieren (**Updates** > **Zusammenfassung**). Die in diesem Fenster angezeigte Update-Rate einer Komponente, die verteilt wird, wird immer höher als 0% sein.

4. Festlegen, wie oft Komponenten heruntergeladen werden sollen. Pattern-Dateien werden oft aktualisiert (manche täglich). Deshalb ist es vorteilhaft, ein regelmäßiges Update durchzuführen. Bitten Sie Ihren Support-Anbieter, Sie zu benachrichtigen, wenn dringende Updates bei Rechnern und Drivern vorgenommen werden müssen.

5. In der Update-Adresse:

   a. Stellen Sie eine Verbindung mit dem ActiveUpdate Server her. Die Server-URL hängt von Ihrer OfficeScan Version ab.

   b. Laden Sie die folgenden Komponenten herunter:

      - Die `server.ini`-Datei. Diese Datei enthält Informationen über die neuesten Komponenten.
      - Die Komponenten, die Sie in Schritt 3 identifiziert haben.

   c. Speichern Sie die heruntergeladenen Komponenten in ein Verzeichnis der Update-Adresse.

6. Führen Sie ein manuelles Update von OfficeScan durch. Weitere Informationen finden Sie unter *Den OfficeScan Server manuell aktualisieren auf Seite 6-27*.

7. Wiederholen Sie Schritt 5 bis Schritt 6 immer, wenn Komponenten aktualisiert werden müssen.

OfficeScan Server-Update-Methoden

Aktualisieren Sie OfficeScan Server-Komponenten manuell oder indem Sie einen Update-Zeitplan konfigurieren.

Um dem Server die Verteilung der aktualisierten Komponenten an die agents zu ermöglichen, aktivieren Sie die Funktion für das automatische agent-Update. Weitere Informationen finden Sie unter *OfficeScan Agent Automatische Updates auf Seite 6-41*. Ist die Funktion 'Automatische agent-Updates' deaktiviert, lädt der Server die Updates herunter, verteilt sie jedoch nicht auf die agents.

Die Update-Methoden beinhalten:

- **Manuelles Server-Update**: Ist ein Update dringend, führen Sie ein manuelles Update durch, damit der Server umgehend das Update erhält. Weitere Informationen finden Sie unter *Den OfficeScan Server manuell aktualisieren auf Seite 6-27*.
- **Server-Update (zeitgesteuert)**: Der OfficeScan Server stellt am geplanten Tag zur festgelegten Zeit eine Verbindung mit der Update-Adresse her, um die aktuellen Komponenten zu erhalten. Weitere Informationen finden Sie unter *Updates für den OfficeScan Server planen auf Seite 6-28*.

Den OfficeScan Server manuell aktualisieren

Aktualisieren Sie die Komponenten des OfficeScan Servers nach der Installation oder einem Upgrade des Servers sowie bei einem Ausbruch manuell.

Prozedur

1. Navigieren Sie zu **Updates** > **Server** > **Manuelles Update**.
2. Wählen Sie die zu aktualisierenden Komponenten aus.
3. Klicken Sie auf **Aktualisieren**.

   Der Server lädt die aktualisierten Komponenten herunter.

Updates für den OfficeScan Server planen

Konfigurieren Sie den OfficeScan Server für die regelmäßige Überprüfung der Update-Adresse und für den automatischen Download verfügbarer Updates. Da agents normalerweise über den Server aktualisiert werden, können Sie durch das zeitgesteuerte Server-Update einfach und wirksam sicherstellen, dass der Schutz vor Sicherheitsrisiken immer auf dem neuesten Stand ist.

Prozedur

1. Navigieren Sie zu **Updates** > **Server** > **Zeitgesteuertes Update**.
2. Wählen Sie **Zeitgesteuertes Update des OfficeScan Servers aktivieren**.
3. Wählen Sie die zu aktualisierenden Komponenten aus.
4. Geben Sie den Update-Zeitplan an.

   Bei täglichen, wöchentlichen und monatlichen Updates gibt der Zeitraum die Anzahl der Stunden an, in denen OfficeScan das Update ausführt. OfficeScan führt das Update zu einem beliebigen Zeitpunkt innerhalb dieses Zeitraums aus.
5. Klicken Sie auf **Speichern**.

OfficeScan Server-Update-Protokolle

Hinweise zu eventuell aufgetretenen Problemen bei der Aktualisierung bestimmter Komponenten finden Sie in den Server-Update-Protokollen. Die Protokolle beziehen Komponenten-Updates für den OfficeScan Server mit ein.

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell, oder konfigurieren Sie eine zeitgesteuerte Löschung der Protokolle. Weitere Informationen zur Protokollverwaltung finden Sie unter *Protokollmanagement auf Seite 14-47*.

Update-Protokolle anzeigen

Prozedur

1. Navigieren Sie zu **Protokolle** > **Server-Update**.
2. Prüfen Sie in der Spalte **Ergebnis**, ob alle Komponenten aktualisiert wurden.
3. Wenn Sie das Protokoll als komma-separierte Datei (`CSV-Datei`) speichern möchten, klicken Sie auf **In CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Updates für den integrierten Smart Protection Server

Der integrierte Smart Protection Server lädt zwei Komponenten herunter, nämlich das Pattern der intelligenten Suche und die Webseiten-Sperrliste. Weitere Informationen zu diesen Komponenten und deren Aktualisierung finden Sie unter *Verwaltung des integrierten Smart Protection Servers auf Seite 4-19*.

OfficeScan Agent-Updates

Aktualisieren Sie die Agent-Komponenten regelmäßig, damit die Agents vor den neuesten Sicherheitsrisiken geschützt bleiben.

Überprüfen Sie vor dem Aktualisieren der Agents, ob ihre Update-Adresse über die aktuellen Komponenten (OfficeScan Server oder eine benutzerdefinierte Update-Adresse) verfügt. Weitere Informationen zum Update des OfficeScan Servers finden Sie unter *OfficeScan Server-Updates auf Seite 6-16*.

In der folgenden Tabelle sind alle Komponenten aufgeführt, die Update-Quellen auf Agents verteilen, sowie die Komponenten, die bei Benutzung einer bestimmten Suchmethode verwendet werden.

TABELLE 6-5. OfficeScan Komponenten, die auf Agents verteilt werden

KOMPONENTE	VERTEILUNG	
	AGENTS DER HERKÖMMLICHEN SUCHE	AGENTS DER INTELLIGENTEN SUCHE
Virenschutz		
Smart Scan Agent Pattern	Nein	Ja
Viren-Pattern	Ja	Nein
IntelliTrap Pattern	Ja	Ja
IntelliTrap Ausnahme-Pattern	Ja	Ja
Viren-Scan-Engine (32/64 Bit)	Ja	Ja
Speicher-Inspektions-Pattern	Ja	Ja
Frühstart Anti-Malware Muster 32-/64-Bit	Ja	Ja
Maschine für Kontextbezogene Intelligenz 32/64-Bit	Ja	Ja
Muster für kontextbezogene Intelligenz	Ja	Ja
Abfragehandhabung für kontextbezogene Intelligenz 32/64-Bit	Ja	Ja
Fortgeschrittenes Bedrohungssuchmaschine 32/64-Bit	Ja	Ja
Fortgeschrittenes Bedrohungskorrelationsmuster	Ja	Ja
Anti-spyware		
Spyware/Grayware-Pattern	Ja	Ja
Spyware-Aktivmonitor-Pattern	Ja	Nein

Komponente	Verteilung	
	Agents der herkömmlichen Suche	Agents der intelligenten Suche
Spyware/Grayware Scan Engine (32/64 Bit)	Ja	Ja
Damage Cleanup Services		
Damage Cleanup Template	Ja	Ja
Damage-Cleanup Engine 32/64 Bit	Ja	Ja
Early Boot Cleanup Driver 32-/64-Bit	Ja	Ja
Web-Reputation-Dienste		
URL-Filter-Engine	Ja	Ja
Firewall		
Pattern der allgemeinen Firewall	Ja	Ja
Allgemeiner Firewall-Treiber 32-/64-Bit	Ja	Ja
Komponenten der Verhaltensüberwachung		
Erkennungs-Pattern der Verhaltensüberwachung (32/64 Bit)	Ja	Ja
Kerntreiber der Verhaltensüberwachung 32/64 Bit	Ja	Ja
Kerndienst der Verhaltensüberwachung 32/64 Bit	Ja	Ja
Pattern zur Konfiguration der Verhaltensüberwachung	Ja	Ja
Pattern der Richtliniendurchsetzung	Ja	Ja
Pattern für digitale Signaturen	Ja	Ja

Komponente	Verteilung	
	Agents der herkömmlichen Suche	Agents der intelligenten Suche
Auslöse-Pattern zum Durchsuchen des Speichers (32/64 Bit)	Ja	Ja
Muster der Programmsinspektionsüberwachung	Ja	Ja
Schadensbehebungsmuster	Ja	Ja
Verdächtige Verbindungen		
Allgemeine C&C-IP-Liste	Ja	Ja
Pattern-Relevanzregeln	Ja	Ja
Lösung für Browser-Schwachstellen		
Pattern für die Prävention von Angriffen auf Browser	Ja	Ja
Einheitliches Skriptanalysemuster	Ja	Ja

OfficeScan Agent Update-Adressen

Agents können Updates aus Standard-Update-Adressen erhalten (OfficeScan Server) oder von bestimmten Komponenten aus benutzerdefinierten Update-Adressen wie dem Trend Micro ActiveUpdate Server. Weitere Informationen finden Sie unter *Standard-Update-Adresse für OfficeScan Agenten auf Seite 6-33* und *Benutzerdefinierte Update-Adressen für OfficeScan Agenten auf Seite 6-34*.

IPv6-Unterstützung für OfficeScan Agent-Updates

Ein reiner IPv6-agent kann sich nicht direkt über reine IPv4-Update-Adressen aktualisieren, wie etwa:

- Ein reiner IPv4-OfficeScan Server

- Ein reiner IPv4-Update-Agent
- Jede reine, benutzerdefinierte IPv4-Update-Adresse
- Trend Micro ActiveUpdate Server

Ebenfalls kann ein reiner IPv4-agent Updates nicht direkt aus reinen IPv6-Update-Adressen erhalten wie einem reinen IPv6 OfficeScan Server oder einem Update-Agent.

Ein Dual-Stack-Proxy-Server wie beispielsweise DeleGate, der IP-Adressen konvertieren kann, muss ermöglichen, dass die agents eine Verbindung zu den Update-Adressen herstellen können.

Standard-Update-Adresse für OfficeScan Agenten

Der OfficeScan Server ist die Standard-Update-Adresse für die agents.

Kann keine Verbindung zum OfficeScan Server hergestellt werden, hat der agents keine Backup-Quelle und veraltet deshalb. Um agents zu aktualisieren, die keine Verbindung zum OfficeScan Server aufbauen können, empfiehlt Trend Micro den Agent Packager zu verwenden. Verwenden Sie dieses Tool, um ein Paket mit den neuesten Komponenten des Servers zu erstellen, und starten Sie dann das Paket auf den agents.

Hinweis

Die IP-Adresse (IPv4 oder IPv6) des agents legt fest, ob eine Verbindung zum OfficeScan Server hergestellt werden kann. Weitere Informationen zur IPv6-Unterstützung für agent-Updates finden Sie unter *IPv6-Unterstützung für OfficeScan Agent-Updates auf Seite 6-32*.

Die Standard-Update-Adresse für OfficeScan Agenten konfigurieren

Prozedur

1. Navigieren Sie zu **Updates** > **Agents** > **Update-Adresse**.
2. Wählen Sie **Standard-Update-Adresse (Update vom OfficeScan Server)** aus.

3. Klicken Sie auf **Alle Agents benachrichtigen**.

OfficeScan Agent-Update-Prozess

Hinweis

Dieses Thema behandelt den Update-Prozess für OfficeScan Agents. Der Update-Prozess für Update-Agents wird in *Standard-Update-Adresse für OfficeScan Agenten auf Seite 6-33* dargestellt.

Wenn Sie die OfficeScan Agents für direktes Aktualisieren vom OfficeScan Server einrichten, verläuft der Update-Vorgang wie folgt:

1. Die OfficeScan Agent beziehen ihre Updates vom OfficeScan Server.
2. Sollte eine Aktualisierung vom OfficeScan Server aus nicht möglich sein, versucht der OfficeScan Agent, direkt eine Verbindung zum Trend Micro ActiveUpdate Server herzustellen, wenn die Option **OfficeScan Agents laden Updates vom Trend Micro ActiveUpdate Server herunter** unter **Agents** > **Agent-Verwaltung** aktiviert ist. Klicken Sie in diesem Fall auf **Einstellungen** > **Berechtigungen und andere Einstellungen** > **Andere Einstellungen (Registerkarte)** > **Update-Einstellungen**.

   Hinweis

   Es können nur Komponenten aus dem ActiveUpdate Server aktualisiert werden. Domäneneinstellungen sowie Programme und Hotfixes können nur vom OfficeScan oder von Update-Agents heruntergeladen werden. Sie können den Update-Prozess verkürzen, indem Sie OfficeScan Agents so konfigurieren, dass sie Pattern-Dateien nur vom ActiveUpdate Server herunterladen. Weitere Informationen finden Sie unter *ActiveUpdate Server als OfficeScan Agent-Update-Adresse auf Seite 6-40*.

Benutzerdefinierte Update-Adressen für OfficeScan Agenten

OfficeScan Agents können nicht nur von OfficeScan Servern aus, sondern auch von benutzerdefinierten Update-Adressen aus aktualisiert werden. Benutzerdefinierte Update-Adressen verringern den Datenverkehr für OfficeScan Agent-Updates zum

OfficeScan Server und sie ermöglichen auch solchen OfficeScan Agents rechtzeitige Updates, die keine Verbindung zum OfficeScan haben. Sie können in der Liste der benutzerdefinierten Update-Adressen bis zu 1024 benutzerdefinierte Update-Adressen festlegen.

Tipp

Trend Micro empfiehlt die Zuweisung einiger OfficeScan Agents als Update Agents und das anschließende Hinzufügen dieser Agents zur Liste.

Benutzerdefinierte Update-Adressen für OfficeScan Agenten konfigurieren

Wichtig

OfficeScan XG Service Pack 1 (oder höher) unterstützt die Verwendung von HTTPS als Kommunikationsprotokoll zwischen Update-Agents und den OfficeScan Agents, die für den Erhalt von Updates von Update-Agents konfiguriert sind. Sie müssen Update-Agents und alle OfficeScan Agents, die an die Update-Agents berichten, auf OfficeScan XG Service Pack 1 aktualisieren, bevor Sie das Kommunikationsprotokoll in HTTPS ändern.

Prozedur

1. Navigieren Sie zu **Updates** > **Agents** > **Update-Adresse**.
2. Wählen Sie **Benutzerdefinierte Update-Adresse** aus.
3. Wählen Sie aus, wie Update-Agents und OfficeScan Agents Updates erhalten.
   - **Update-Agents aktualisieren Komponenten, Domäneneinstellungen, Agent-Programme und Hotfixes nur vom OfficeScan Server aus**
   - OfficeScan Agents aktualisieren die folgenden Elemente vom OfficeScan Server, wenn keine benutzerdefinierten Adressen verfügbar sind oder gefunden wurden:
     - **Komponenten**
     - **Domäneneinstellungen**

- **OfficeScan Agent-Programme und Hotfixes**

Weitere Informationen finden Sie unter *OfficeScan Agent-Update-Prozess auf Seite 6-34*.

4. Wenn Sie mindestens einen Update-Agent als Update-Adresse festgelegt haben, klicken Sie auf **Update-Agent - Analysebericht**, um einen Bericht zu erstellen, der den Update-Status der Endpunkte anzeigt.

   Weitere Informationen zum Bericht finden Sie unter *Update-Agent - Analysebericht auf Seite 6-67*.

5. Fügen Sie die **Liste der benutzerdefinierten Update-Adressen** hinzu oder bearbeiten Sie sie.

   - Klicken Sie auf **Hinzufügen**, um eine neue Update-Adresse anzugeben.
   - Klicken Sie auf einen Wert in der Spalte **IP-Bereich**, um eine vorhandene Update-Adresse zu bearbeiten.

   Hinweis

   Bearbeiten Sie eine vorhandene Update-Adresse, um das Kommunikationsprotokoll eines vorhandenen Update-Agents für XG SP1 (oder höher) in HTTPS zu ändern.

   Der Bildschirm **IP-Bereich und Update-Adresse hinzufügen/bearbeiten** wird angezeigt.

6. Konfigurieren Sie die IP-Adressen von Endpunkten, die Updates von der Update-Adresse erhalten.

   - **IPv4**: Geben Sie den IPv4-Adressbereich der Endpunkte an, die die Update-Adresse verwenden
   - **IPv6**: Geben Sie IPv6-Präfix und -Länge der Endpunkte an, die die Update-Adresse verwenden

Hinweis

Stellen Sie sicher, dass sich die OfficeScan Agents mit der Update-Adresse verbinden können, indem sie ihre IP-Adresse verwenden. Wenn Sie beispielsweise einen IPv4-Adressbereich festgelegt haben, muss die Update-Adresse eine IPv4-Adresse haben. Wenn Sie ein IPv6-Präfix und eine -Länge festgelegt haben, muss die Update-Adresse eine IPv6-Adresse haben.

Weitere Informationen zur IPv6-Unterstützung für Endpunkt-Updates finden Sie unter *OfficeScan Agent Update-Adressen auf Seite 6-32*.

7. Geben Sie die Update-Adresse an. Sie können einen Update-Agent auswählen, falls vorhanden, oder den URL einer benutzerdefinierten Adresse eingeben.

   - **URL**: Geben Sie den URL der Update-Adresse an

     Hinweis

     Um ein vorhandenes Update-Agent-Protokoll von HTTP in HTTPS zu ändern, ändern Sie den Wert **URL**.

   - **Update-Agent**: Wählen Sie im Listenfeld einen vorkonfigurierten Update-Agent und geben Sie an, wie sich die OfficeScan Agents mit dem Update-Agent verbinden

     - **Update-Agent-IP-Adresse für Verbindung verwenden**
     - **Update-Agent-Hostnamen für Verbindung verwenden**

     Hinweis

     OfficeScan konfiguriert den URL der **externen Quelle** automatisch für die Verwendung des HTTPS-Protokolls, wenn der Update-Agent auf OfficeScan XG SP1 oder höher aktualisiert wurde.

8. Klicken Sie auf **Speichern**.

9. Verwalten Sie die **Liste der benutzerdefinierten Update-Adressen**.

   a. Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Löschen**, um eine Update-Adresse aus der Liste zu entfernen.

b. Klicken Sie auf den Aufwärts- oder Abwärtspfeil, um eine Update-Adresse zu verschieben. Es kann jeweils nur eine Adresse verschoben werden.

10. Klicken Sie auf **Alle Agents benachrichtigen**.

OfficeScan Agent-Update-Prozess

Hinweis

Dieses Thema behandelt den Update-Prozess für OfficeScan Agents. Der Update-Prozess für Update-Agents wird in *Benutzerdefinierte Update-Adresse für Update-Agents auf Seite 6-63* dargestellt.

Nachdem Sie die benutzerdefinierte Liste der Update-Adressen erstellt und gespeichert haben, wird der Update-Vorgang wie folgt durchgeführt:

1. Der OfficeScan Agent führt Updates anhand der ersten Quelle in der Liste durch.
2. Ist ein Update aus der ersten Quelle nicht möglich, führt der OfficeScan Agent ein Update aus der zweiten Quelle durch, usw.
3. Ist das Update aus keiner der Quellen möglich, überprüft der OfficeScan Agent die folgenden Einstellungen im Fenster **Update-Adresse**:

TABELLE 6-6. Zusätzliche Einstellungen für benutzerdefinierte Update-Adressen

EINSTELLUNG	BESCHREIBUNG
Update-Agents aktualisieren Komponenten, Domäneneinstellungen, Agent-Programme und Hotfixes nur vom OfficeScan Server aus	Wenn diese Einstellung aktiviert ist, werden Update-Agents direkt vom OfficeScan Server aktualisiert und die Liste der benutzerdefinierten Update-Adressen nicht beachtet. Wenn diese Option deaktiviert ist, übernehmen die Update-Agents die für normale agents konfigurierten benutzerdefinierten Einstellungen für die Update-Adresse.
OfficeScan Agents aktualisieren die folgenden Elemente vom OfficeScan Server, wenn keine benutzerdefinierten Adressen verfügbar sind oder gefunden wurden:	

EINSTELLUNG	BESCHREIBUNG
Komponenten	Wenn diese Einstellung aktiviert ist, aktualisiert der agent Komponenten vom OfficeScan Server. Ist die Option deaktiviert, versucht der agent, eine direkte Verbindung zum Trend Micro ActiveUpdate Server aufzubauen, sofern Folgendes ganz oder teilweise zutrifft: • Klicken Sie unter **Agents** > **Agent-Verwaltung** auf **Einstellungen** > **Berechtigungen und andere Einstellungen** > **Andere Einstellungen (Registerkarte)** > **Update-Einstellungen**. Die Option **OfficeScan Agents laden Updates vom Trend Micro ActiveUpdate Server herunter** ist aktiviert. • Der ActiveUpdate Server ist nicht in der Liste der benutzerdefinierten Update-Adressen enthalten. **Hinweis** Es können nur Komponenten aus dem ActiveUpdate Server aktualisiert werden. Domäneneinstellungen sowie Programme und Hotfixes können nur vom OfficeScan oder von Update-Agents heruntergeladen werden. Sie können den Update-Prozess verkürzen, indem Sie agents so konfigurieren, dass sie Pattern-Dateien nur vom ActiveUpdate Server herunterladen. Weitere Informationen finden Sie unter *ActiveUpdate Server als OfficeScan Agent-Update-Adresse auf Seite 6-40*.
Domäneneinstellungen	Wenn diese Einstellung aktiviert ist, aktualisiert der client_computer_singleagent Einstellungen der Domänenebene vom OfficeScan Server.
OfficeScan Agent-Programme und Hotfixes	Wenn diese Einstellung aktiviert ist, aktualisiert der agent Programme und Hotfixes vom OfficeScan Server.

4. Ist von allen möglichen Adressen kein Update möglich, bricht der agent den Update-Prozess ab.

ActiveUpdate Server als OfficeScan Agent-Update-Adresse

Wenn OfficeScan Agents Updates direkt vom Trend Micro ActiveUpdate Server herunterladen, können Sie das Herunterladen ausschließlich auf die Pattern-Dateien beschränken, um Bandbreite während Aktualisierungen einzusparen und den Aktualisierungsprozess zu beschleunigen.

Scan Engines und andere Komponenten werden nicht so häufig aktualisiert wie Pattern-Dateien, ein weiteres Argument dafür, den Download nur auf die Pattern-Dateien zu beschränken.

Ein reiner IPv6-agent kann Updates nicht direkt vom Trend Micro ActiveUpdate Server herunterladen. Ein Dual-Stack-Proxy-Server wie beispielsweise DeleGate, der IP-Adressen konvertieren kann, muss ermöglichen, dass die OfficeScan Agents eine Verbindung zum ActiveUpdate Server herstellen können.

Downloads vom ActiveUpdate Server begrenzen

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Klicken Sie auf die Registerkarte **System**.
3. Navigieren Sie zum Abschnitt **Updates**.
4. Wählen Sie **Pattern-Dateien nur vom ActiveUpdate Server während Updates herunterladen**.

OfficeScan Agent Update-Methoden

OfficeScan Agents , die Komponenten vom OfficeScan Server oder einer benutzerspezifischen Update-Adresse beziehen, können die folgenden Update-Methoden verwenden:

- **Automatische Updates**: Agent -Update wird automatisch bei bestimmten Ereignissen oder nach einem festgelegten Zeitplan ausgeführt. Weitere Informationen finden Sie unter *OfficeScan Agent Automatische Updates auf Seite 6-41*.
- **Manuelle Updates**: Ist ein Update dringend, verwenden Sie ein manuelles Update, um die agents umgehend zur Ausführung eines Komponenten-Updates aufzufordern. Weitere Informationen finden Sie unter *OfficeScan Agent Manuelle Updates auf Seite 6-47*.
- **Berechtigungsgesteuerte Updates**: Benutzer mit Update-Berechtigungen haben mehr Kontrolle darüber, wie der OfficeScan Agent auf ihrem Computer aktualisiert wird. Weitere Informationen finden Sie unter *Update-Berechtigungen und weitere Einstellungen konfigurieren auf Seite 6-49*.

OfficeScan Agent Automatische Updates

Das automatische Update befreit Sie von lästigen Update-Benachrichtigungen an alle agents und verringert so das Risiko veralteter Komponenten auf agent-Computern.

Die OfficeScan Agents erhalten beim automatischen Update die Komponenten und aktualisierte Konfigurationsdateien. Agents benötigen diese Konfigurationsdateien, um neue Einstellungen zu übernehmen. Bei jeder Änderung der OfficeScan Einstellungen über die Webkonsole ändern sich auch die Konfigurationsdateien. Um festzulegen, wie häufig Konfigurationsdateien auf agents übernommen werden, lesen Sie Schritt 3, *Automatische Updates für OfficeScan Agent konfigurieren auf Seite 6-43*.

Hinweis

Sie können agents so konfigurieren, dass beim automatischen Update Proxy-Einstellungen verwendet werden. Weitere Informationen finden Sie unter *Proxy für Updates von OfficeScan Agent-Komponenten auf Seite 6-53*.

Es gibt zwei Arten automatischer Updates:

- *Ereignisbedingte Updates auf Seite 6-42*
- *Zeitgesteuerte Updates auf Seite 6-43*

Ereignisbedingte Updates

Der Server versendet nach dem Download der neuesten Komponenten Update-Benachrichtigungen an die Online-Agents. Offline-Agents werden benachrichtigt, sobald sie neu gestartet wurden und sich wieder mit dem Server verbinden. Sie können nach dem Update optional die Funktion "Jetzt durchsuchen" (manuelle Suche) auf den OfficeScan Agent-Endpunkten durchführen.

TABELLE 6-7. Optionen für ereignisbedingte Updates

OPTIONEN	BESCHREIBUNG
Komponenten-Update auf den Agents sofort nach dem Download einer neuen Komponente auf dem OfficeScan Server starten	Der Server benachrichtigt die Agents, sobald ein Update abgeschlossen ist. Regelmäßig aktualisierte Agents müssen nur inkrementelle Pattern herunterladen. Dadurch wird weniger Zeit für die Aktualisierung benötigt (weitere Informationen zu inkrementellen Pattern finden Sie unter *OfficeScan Server-Komponentenduplizierung auf Seite 6-22*). Regelmäßige Updates können jedoch die Serverleistung negativ beeinflussen, insbesondere wenn eine hohe Anzahl von Agents gleichzeitig aktualisiert wird. Wenn sich Agents im unabhängigen Modus befinden und diese auch aktualisiert werden sollen, wählen Sie **Unabhängige und Offline-Agents berücksichtigen** aus. Weitere Informationen zum unabhängigen Modus finden Sie unter *Berechtigung "Unabhängiger Modus" von OfficeScan Agent auf Seite 15-20*.
Agents beginnen nach dem Neustart und dem Herstellen einer Verbindung zum OfficeScan Server mit dem Komponenten-Update (mit Ausnahme unabhängiger Agents)	Verpasst ein Agent ein Update, lädt dieser die Komponenten herunter, sobald eine Verbindung mit dem Server aufgebaut wird. Der Agent kann ein Update verpassen, wenn er offline ist, oder wenn der Endpunkt, auf dem der Agent installiert ist, nicht hochgefahren ist.
Nach dem Update 'Jetzt durchsuchen' ausführen (mit Ausnahme unabhängiger Agents)	Nach einem ereignisbedingten Update fordert der Server die Agents zum Durchsuchen auf. Aktivieren Sie gegebenenfalls diese Option, wenn ein bestimmtes Update eine Reaktion auf ein Sicherheitsrisiko ist, das sich bereits im Netzwerk ausgebreitet hat.

Hinweis

Kann der OfficeScan Server nach dem Herunterladen der Komponenten keine Update-Benachrichtigung an Agents senden, wiederholt er den Versuch automatisch nach 15 Minuten. Dies wiederholt er bis zu fünf Mal oder bis der Agent antwortet. Nach dem fünften Versuch wird keine Benachrichtigung mehr versendet. Wenn Sie die Option wählen, dass die Komponenten beim Neustart der Agents und der Verbindung mit dem Server aktualisiert werden, wird das Komponenten-Update fortgesetzt.

Zeitgesteuerte Updates

Die Ausführung zeitgesteuerter Updates erfordert eine Berechtigung. Wählen Sie zunächst OfficeScan Agents für die Berechtigung aus. Diese OfficeScan Agents führen dann Updates gemäß dem Zeitplan aus.

Hinweis

Informationen zur Verwendung des zeitgesteuerten Updates mit NAT (Network Adress Translation, Netzwerkadressübersetzung) finden Sie unter *Zeitgesteuerte OfficeScan Agent-Updates mit NAT konfigurieren auf Seite 6-45*.

Automatische Updates für OfficeScan Agent konfigurieren

Prozedur

1. Navigieren Sie zu **Updates** > **Agents** > **Automatisches Update**.
2. Wählen Sie die Ereignisse für **Ereignisbedingtes Update** aus:
   - **Komponenten-Update auf den Agents sofort nach dem Download einer neuen Komponente auf dem OfficeScan Server starten**
     - **Unabhängige und Offline-Agents berücksichtigen**
   - **Agents beginnen nach dem Neustart und dem Herstellen einer Verbindung zum OfficeScan Server mit dem Komponenten-Update (mit Ausnahme unabhängiger Agents)**
   - **Nach dem Update 'Jetzt durchsuchen' ausführen (mit Ausnahme unabhängiger Agents)**

Weitere Informationen zu den verfügbaren Optionen finden Sie unter *Ereignisbedingte Updates auf Seite 6-42*.

3. Konfigurieren Sie den Zeitplan für **Zeitgesteuertes Update**.

   - **Minute(n)** oder **Stunde(n)**

     Die Option **Agent-Konfigurationen nur einmal täglich aktualisieren** ist bei der Planung eines stündlichen oder auf Minuten basierenden Update-Intervalls verfügbar. Die Konfigurationsdatei enthält alle mit Hilfe der Webkonsole konfigurierten OfficeScan Agent-Einstellungen.

     Tipp

     Trend Micro aktualisiert die Komponenten häufig. Die OfficeScan Konfigurationseinstellungen ändern sich vermutlich weniger häufig. Das Update der Konfigurationsdateien mit den Komponenten erfordert mehr Bandbreite und erhöht den Zeitaufwand, den OfficeScan für das Update benötigt. Aus diesem Grund empfiehlt Trend Micro, die OfficeScan Agent-Konfigurationen nur einmal täglich zu aktualisieren.

   - **Täglich** oder **Wöchentlich**

     Geben Sie den Zeitpunkt des Updates und den Zeitraum an, während dem der OfficeScan Server Agents darüber benachrichtigt, dass Komponenten aktualisiert werden müssen.

     Tipp

     Dies verhindert, dass sich alle Online-Agents zur festgelegten Startzeit gleichzeitig mit dem Server verbinden, und reduziert den Datenverkehr zum Server erheblich. Wenn beispielsweise die Startzeit bei 12:00 Uhr liegt und der Zeitraum 2 Stunden beträgt, sendet OfficeScan zwischen 12:00 und 14:00 Uhr nach dem Zufallsprinzip Benachrichtigungen zum Komponenten-Update an alle Online-Agents.

Hinweis

Nach der Konfiguration des Update-Zeitplans aktivieren Sie den Zeitplan auf ausgewählten Agents.

Weitere Informationen zum Aktivieren zeitgesteuerter Updates finden Sie in Schritt 4 unter *Update-Berechtigungen und weitere Einstellungen konfigurieren auf Seite 6-49*.

4. Klicken Sie auf **Speichern**.

   OfficeScan kann Offline-Agents nicht sofort benachrichtigen. Wählen Sie **Agents beginnen nach dem Neustart und dem Herstellen einer Verbindung mit dem OfficeScan Server mit dem Komponenten-Update (Ausnahme: unabhängige Agents)** aus, um Offline-Agents zu aktualisieren, die erst nach Ablauf des festgelegten Zeitraums wieder online sind. Offline-Agents, für die diese Option nicht aktiviert ist, aktualisieren Komponenten zum nächsten geplanten Zeitpunkt oder bei einem manuellen Update.

Zeitgesteuerte OfficeScan Agent-Updates mit NAT konfigurieren

Folgende Probleme können auftreten, wenn das lokale Netzwerk NAT (Network Adress Translation, Netzwerkadressübersetzung) verwendet:

- OfficeScan Agents werden in der Webkonsole als offline angezeigt.
- Der OfficeScan Server kann die agents bei Updates und Konfigurationsänderungen nicht benachrichtigen.

Als Workaround bietet sich an, aktualisierte Komponenten und Konfigurationsdateien wie nachfolgend beschrieben per zeitgesteuertem Update vom Server auf den OfficeScan Agent zu verteilen.

Prozedur

- Vor der Installation des OfficeScan Agents auf agent-Computern:

  a. Konfigurieren Sie den Update-Zeitplan des agents im Abschnitt **Zeitgesteuertes Update** von **Updates** > **Agents** > **Automatisches Update**.

b. Erteilen Sie den agents die Berechtigung zum Aktivieren zeitgesteuerter Updates unter **Agents** > **Agent-Verwaltung** und klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen** > **Berechtigungen (Registerkarte)** > **Komponenten-Updates**.

- Wenn OfficeScan Agents bereits auf agent-Computern installiert sind:

  a. Erteilen Sie den agents die Berechtigung zum Durchführen von „Jetzt aktualisieren“ unter **Agents** > **Agent-Verwaltung** und klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen** > **Berechtigungen (Registerkarte)** > **Komponenten-Updates**.

  b. Weisen Sie die Benutzer an, die Komponenten auf dem agent-Endpunkt manuell zu aktualisieren (per Rechtsklick auf das OfficeScan Agent Symbol in der Taskleiste und Auswahl der Option "Jetzt aktualisieren"), um die aktualisierten Konfigurationseinstellungen zu beziehen.

OfficeScan Agents erhalten beim Update die aktualisierten Komponenten und die Konfigurationsdateien.

Domänenzeitplan-Update-Tool verwenden

Der Update-Zeitplan, der in den automatischen agent-Updates konfiguriert ist, wird nur auf agents angewendet, die über zeitgesteuerte Update-Berechtigungen verfügen. Sie können für alle anderen agents einen separaten Update-Zeitplan erstellen. Dafür müssen Sie einen Zeitplan über die agent-Hierarchiedomänen konfigurieren. Alle agents, die zu dieser Domäne gehören, wenden diesen Zeitplan an.

Hinweis

Es ist nicht möglich, einen Update-Zeitplan für einen bestimmten agent oder eine bestimmte Subdomäne aufzustellen. Alle Subdomänen wenden den Zeitplan an, der für ihre übergeordnete Domäne konfiguriert wurde.

Prozedur

1. Erfassen Sie die agent-Hierarchiedomänennamen und Update-Zeitpläne.

2. Navigieren Sie zu <*Installationsordner des Servers*>\PCCSRV\Admin\Utility\DomainScheduledUpdate.
3. Kopieren Sie die folgenden Dateien nach <Installationsordner des Servers>\PCCSRV:
   - DomainSetting.ini
   - dsu_convert.exe
4. Öffnen Sie DomainSetting.ini mit Hilfe eines Texteditors, beispielsweise Notepad.
5. Geben Sie eine Domäne aus der agent-Hierarchie an, und konfigurieren Sie dann den Update-Zeitplan für die Domäne. Wiederholen Sie diesen Schritt, um weitere Domänen hinzuzufügen.

   Hinweis

   Ausführliche Konfigurationsanweisungen werden in der .ini -Datei zur Verfügung gestellt.
6. Speichern Sie DomainSetting.ini.
7. Öffnen Sie eine Befehlszeile, und wechseln Sie in das Verzeichnis des PCCSRV-Ordners.
8. Geben Sie folgenden Befehl ein, und drücken Sie die Eingabetaste.

   ```
   dsuconvert.exe DomainSetting.ini
   ```
9. Navigieren Sie auf der Webkonsole zu **Agents** > **Globale Agent-Einstellungen**.
10. Klicken Sie auf **Speichern**.

OfficeScan Agent Manuelle Updates

Aktualisieren Sie OfficeScan Agent-Komponenten bei einem Ausbruch oder starker Veralterung der OfficeScan Agent-Komponenten manuell. OfficeScan Agent - Komponenten veralten stark, wenn der OfficeScan Agent seine Komponenten über einen längeren Zeitraum nicht über die Update-Adresse aktualisieren kann.

Zusätzlich zu den Komponenten erhalten OfficeScan Agents während des manuellen Updates automatisch aktualisierte Konfigurationsdateien. OfficeScan Agents benötigen diese Konfigurationsdateien, um neue Einstellungen zu übernehmen. Bei jeder Änderung der OfficeScan Einstellungen über die Webkonsole ändern sich auch die Konfigurationsdateien.

Hinweis

Außer manuelle Updates selbst zu initiieren, können Sie auch Benutzern die Berechtigung erteilen, manuelle Updates durchzuführen (auf den OfficeScan Agent-Endpunkten auch als **Jetzt aktualisieren** bezeichnet). Weitere Informationen finden Sie unter *Update-Berechtigungen und weitere Einstellungen konfigurieren auf Seite 6-49*.

OfficeScan Agenten manuell aktualisieren

Prozedur

1. Navigieren Sie zu **Updates** > **Agents** > **Manuelles Update**.
2. Jeweils auf dem OfficeScan Server verfügbare Komponenten sowie das letzte Aktualisierungsdatum dieser Komponenten werden oben im Fenster angezeigt Stellen Sie sicher, dass die Komponenten aktuell sind, bevor Sie die Agents über das Update benachrichtigen.

   Hinweis

   Sie können alle veralteten Server-Komponenten auch manuell aktualisieren.

   Weitere Informationen finden Sie unter *OfficeScan Agent Manuelle Updates auf Seite 6-47*.

3. Nur Agents mit veralteten Komponenten aktualisieren:

   a. Klicken Sie auf **Agents mit veralteten Komponenten auswählen**.

   b. (Optional) Wählen Sie **Unabhängige und Offline-Agents berücksichtigen** aus:

      - Unabhängige Agents aktualisieren, die mit dem Server verbunden sind.
      - Offline-Agents aktualisieren, wenn sie wieder online sind.

c. Klicken Sie auf **Update starten**.

Hinweis

Der Server sucht nach Agents, deren Komponentenversionen älter als die Versionen auf dem Server sind, und benachrichtigt anschließend diese Agents über das Update. Um den Benachrichtigungsstatus zu überprüfen, navigieren Sie zum Fenster **Updates** > **Zusammenfassung**.

4. Die Agents Ihrer Wahl aktualisieren:

   a. Wählen Sie **Agents manuell auswählen** aus.

   b. Klicken Sie auf **Auswählen**.

   c. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.

   d. Klicken Sie auf **Update starten**.

Hinweis

Der Server benachrichtigt alle Agents, aktualisierte Komponenten herunterzuladen. Um den Benachrichtigungsstatus zu überprüfen, navigieren Sie zum Fenster **Updates** > **Zusammenfassung**.

Update-Berechtigungen und weitere Einstellungen konfigurieren

Sie können Update-Einstellungen konfigurieren und Agent-Benutzern bestimmte Berechtigungen gewähren. So können Sie beispielsweise "Jetzt aktualisieren" verwenden und zeitgesteuerte Updates aktivieren.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.

2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.

3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.

4. Klicken Sie auf die Registerkarte **Andere Einstellungen**, und konfigurieren Sie die folgenden Optionen im Abschnitt **Update-Einstellungen**:

OPTION	BEZEICHNUNG
OfficeScan Agents laden Updates vom Trend Micro ActiveUpdate Server herunter	Nach dem Start des Updates erhalten die OfficeScan Agents Updates zuerst von der unter **Updates** > **Agents** > **Update-Adresse** festgelegten Update-Adresse. Schlägt das Update fehl, versuchen die Agents, sich über den OfficeScan Server zu aktualisieren. Mit dieser Option können Agents, deren Update über den OfficeScan Server fehlgeschlagen ist, das Update über den Trend Micro ActiveUpdate Server ausführen. **Hinweis** Ein reiner IPv6-Agent kann Updates nicht direkt vom Trend Micro ActiveUpdate Server herunterladen. Ein Dual-Stack-Proxy-Server wie beispielsweise DeleGate, der IP-Adressen konvertieren kann, muss ermöglichen, dass die Agents eine Verbindung zum ActiveUpdate Server herstellen können.
Zeitgesteuerte Updates auf OfficeScan Agents aktivieren	Durch Auswahl dieser Option werden für alle OfficeScan Agents standardmäßig zeitgesteuerte Updates aktiviert. Benutzer mit der Berechtigung **Zeitgesteuerte Updates aktivieren/deaktivieren** können diese Einstellung überschreiben. Weitere Informationen zum Konfigurieren des Update-Zeitplans finden Sie unter *Automatische Updates für OfficeScan Agent konfigurieren auf Seite 6-43*.
OfficeScan Agents aktualisieren nur die folgenden Komponenten	Diese Option steuert, wie Komponenten-Updates durchgeführt werden. Wählen Sie unter folgenden Optionen: • **Alle Komponenten (einschließlich Hotfixes und Agent-Programm)**: OfficeScan Agents aktualisieren alle Komponenten.

OPTION	BEZEICHNUNG
	• **Pattern-Dateien, Engines, Treiber**: OfficeScan Agents führen kein Upgrade des OfficeScan Agent-Programms durch und stellen keine Hotfixes bereit. • **Pattern-Dateien**: OfficeScan Agents führen kein Upgrade des OfficeScan Agent-Programms durch, stellen keine Hotfixes bereit und aktualisieren keine Engines und Treiber. **Hinweis** Die Auswahl von **Alle Komponenten (einschließlich Hotfixes und Agent-Programm)** kann die Serverleistung erheblich beeinträchtigen, da alle Agents gleichzeitig eine Verbindung zum Server herstellen, um ein Upgrade durchzuführen oder ein Hotfix zu installieren.

5. Klicken Sie auf die Registerkarte **Berechtigungen**, und konfigurieren Sie die folgenden Optionen im Abschnitt **Komponenten-Updates**:

OPTION	BEZEICHNUNG
"Jetzt aktualisieren" ausführen	Benutzer mit dieser Berechtigung können bei Bedarf Komponenten aktualisieren, indem sie in der Taskleiste mit der rechten Maustaste auf das OfficeScan Agent-Symbol klicken und anschließend **Jetzt aktualisieren** auswählen. **Hinweis** OfficeScan Agent Agent-Benutzer können während der Ausführung von "Jetzt aktualisieren" Proxy-Einstellungen verwenden. Weitere Informationen finden Sie unter *Proxy-Konfiguration, Berechtigungen gewähren auf Seite 15-59*.
Zeitgesteuerte Updates aktivieren/ deaktivieren	Durch Auswahl dieser Option können OfficeScan Agent-Benutzer zeitgesteuerte Updates mit hilfe des Kontextmenüs von OfficeScan Agent aktivieren bzw. deaktivieren, womit die Einstellung **Zeitgesteuerte Updates aktivieren** überschrieben werden kann.

OPTION	BEZEICHNUNG
	Hinweis Administratoren müssen zunächst auf der Registerkarte **Andere Einstellungen** die Option **Zeitgesteuerte Updates auf OfficeScan Agents aktivieren** auswählen, damit das entsprechende Menüelement im OfficeScan Agent-Menü angezeigt wird.

6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Reservierten Festplattenspeicher für OfficeScan Agenten-Updates konfigurieren

OfficeScan reserviert auf den agent-Festplatten eine bestimmte Menge Speicherplatz für Hotfixes, Pattern-Dateien, Scan Engines und Programm-Updates. OfficeScan reserviert standardmäßig 60 MB Speicherplatz.

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Klicken Sie auf die Registerkarte **System**.
3. Navigieren Sie zum Abschnitt **Updates**.

4. Wählen Sie **Reservieren__ MB des Festplatternspeichers für Updates** aus.
5. Wählen Sie die gewünschte Speicherplatzmenge aus.
6. Klicken Sie auf **Speichern**.

Proxy für Updates von OfficeScan Agent-Komponenten

OfficeScan Agents können Proxy-Einstellungen für automatische Updates verwenden sowie zum Ausführen der Funktion "Jetzt aktualisieren", falls sie dazu berechtigt sind.

TABELLE 6-8. Beim Update von OfficeScan Agent-Komponenten verwendete Proxy-Einstellungen

UPDATE-METHODE	VERWENDETE PROXY-EINSTELLUNGEN	VERWENDUNG
Automatisches Update	• Interne Proxy-Einstellungen. Weitere Informationen finden Sie unter *Proxy-Einstellungen für internen Agent konfigurieren auf Seite 15-56*.	1. Agents wenden zuerst interne Proxy-Einstellungen an. 2. Wenn Sie keine internen Proxy-Einstellungen konfigurieren, verwenden Agents keinerlei Proxy-Einstellungen.

UPDATE-METHODE	VERWENDETE PROXY-EINSTELLUNGEN	VERWENDUNG
Jetzt aktualisieren	• Interne Proxy-Einstellungen. Weitere Informationen finden Sie unter *Proxy-Einstellungen für internen Agent konfigurieren auf Seite 15-56*. • Benutzerdefinierte Proxy-Einstellungen. Sie können Agent-Benutzern die Berechtigung zur Konfiguration der Proxy-Einstellungen erteilen. Weitere Informationen finden Sie unter *Proxy-Konfiguration, Berechtigungen gewähren auf Seite 15-59*.	1. Agents wenden zuerst interne Proxy-Einstellungen an. 2. Wenn keine Proxy-Einstellungen aktiviert sind und Agent-Benutzer nicht über die erforderliche Berechtigung verfügen, verwenden Agents beim Aktualisieren der Komponenten keinen Proxy.

OfficeScan Agent-Update-Benachrichtigungen konfigurieren

OfficeScan benachrichtigt agent-Benutzer, wenn Update-bezogene Ereignisse auftreten.

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Klicken Sie auf die Registerkarte **Agent Kontrolle**.
3. Navigieren Sie zum Abschnitt **Alarmeinstellungen**.

4. Wählen Sie die folgenden Optionen:

   - **Warnsymbol in der Windows Taskleiste anzeigen, wenn die Viren-Pattern-Datei seit __ Tag(en) nicht aktualisiert wurde**: Ein Warnsymbol auf der Windows Taskleiste erinnert den Benutzer daran, das Viren-Pattern zu aktualisieren, das innerhalb der festgelegten Anzahl von Tagen nicht aktualisiert wurde. Zur Aktualisierung des Patterns verwenden Sie eine der Update-Methoden, die in *OfficeScan Agent Update-Methoden auf Seite 6-40* behandelt werden.

     Alle agents, die vom Server verwaltet werden, übernehmen diese Einstellung.

   - **Eine Benachrichtigung anzeigen, wenn der Endpunkt zum Laden eines Kerneltreibers neu gestartet werden muss**: Nach der Installation eines Hotfixes oder Upgrade-Pakets mit einer neuen Version des Kerneltreibers ist die Vorgängerversion des Treibers möglicherweise noch immer auf dem Endpunkt vorhanden. Eine Deinstallation der Vorgängerversion und die Installation der neuen Version ist nur nach einem Neustart des Endpunkts möglich. Nach dem Neustart des Endpunkts wird die neue Version automatisch installiert, und es ist kein weiterer Neustart erforderlich.

     Die Benachrichtigung wird direkt nach der Installation des Hotfixes oder Upgrade-Pakets auf dem agent-Endpunkt angezeigt.

5. Klicken Sie auf **Speichern**.

OfficeScan Agent Update-Protokolle anzeigen

Überprüfen Sie die agent-Update-Protokolle, um festzustellen, ob beim Aktualisieren des Viren-Patterns auf den agents Probleme auftreten.

Hinweis

In dieser Produktversion können nur Protokolle für Viren-Pattern-Updates von der Webkonsole aus abgefragt werden.

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell, oder konfigurieren Sie eine zeitgesteuerte Löschung der

Protokolle. Weitere Informationen zur Protokollverwaltung finden Sie unter *Protokollmanagement auf Seite 14-47*.

Prozedur

1. Navigieren Sie zu **Protokolle** > **Agents** > **Agent-Komponenten-Update**.
2. Klicken Sie in der Spalte **Fortschritt** auf **Ansicht**, um die Anzahl der agent-Updates anzuzeigen. Im daraufhin angezeigten Fenster **Fortschritt des Komponenten-Updates** wird die Gesamtzahl der aktualisierten agents und die Anzahl der agents, die im Abstand von 15 Minuten aktualisiert werden, angezeigt.
3. Klicken Sie in der Spalte **Details** auf **Ansicht**, um die agents mit aktualisiertem Viren-Pattern anzuzeigen.
4. Wenn Sie das Protokoll als komma-separierte Datei im CSV-Format speichern möchten, klicken Sie auf **In CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

OfficeScan Agent Updates erzwingen

Über die Einhaltung der Sicherheitsrichtlinien können Sie gewährleisten, dass sich auf den agents die neuesten Komponenten befinden. Bei der Prüfung der Richtlinieneinhaltung der Komponenten wird ermittelt, ob es Komponenten-Inkonsistenzen zwischen dem OfficeScan Server und den agents gibt. Inkonsistenzen treten üblicherweise dann auf, wenn die agents keine Verbindung zum Server aufbauen können, um die Komponenten zu aktualisieren. Wenn der agent ein Update von einer anderen Quelle erhält (z. B. einem ActiveUpdate Server), kann es vorkommen, dass eine Komponente auf dem agent neuer ist als dieselbe Komponente auf dem Server.

Weitere Informationen finden Sie unter *Einhaltung der Sicherheitsrichtlinien für verwaltete Agents auf Seite 15-63*.

Durchführen eines Rollbacks der Komponenten für OfficeScan Agenten

Ein Rollback ist eine Rückabwicklung zur vorherigen Version des Viren-Patterns, des Agent-Patterns der intelligenten Suche und der Viren-Scan-Engine. Wenn diese

Komponenten nicht ordnungsgemäß ausgeführt werden, führen Sie eine Rollback auf frühere Versionen durch. OfficeScan behält die aktuelle und die vorherige Version der Viren-Scan-Engine sowie die letzten fünf Versionen des Viren-Patterns und des Agent-Patterns der intelligenten Suche bei.

Hinweis

Nur die oben genannten Komponenten können rückabgewickelt werden.

OfficeScan 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 im entsprechenden Bereich auf **Mit Server synchronisieren**.
   a. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
   b. Klicken Sie auf **Rollback**.
   c. Klicken Sie auf **Update-Protokolle anzeigen**, um das Ergebnis zu überprüfen oder **Zurück**, um zum Fenster Rollback zurückzugehen.
3. Wenn eine ältere Pattern-Datei auf dem Server vorhanden ist, klicken Sie auf **Rollback für Server und Agents**, um ein Rollback der Pattern-Datei sowohl auf dem Agent als auch auf dem Server durchzuführen.

Touch Tool für OfficeScan Agent Hot Fixes ausführen

Das Touch Tool passt den Zeitstempel einer Datei an den Zeitstempel einer anderen Datei oder an die Systemzeit des Endpunkts an. Wenn Sie erfolglos versuchen, einen Hotfix auf dem OfficeScan Server zu installieren, verwenden Sie das Touch Tool, um

den Zeitstempel des Hotfixes zu ändern. Dadurch erkennt OfficeScan den Hotfix als neu, und der Server versucht automatisch, den Hotfix erneut zu verteilen.

Prozedur

1. Öffnen Sie auf dem OfficeScan Server den Ordner <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\Touch`.

2. Kopieren Sie die Datei `TMTouch.exe` in den Ordner, in dem sich die Datei befindet, die Sie ändern möchten. Bei der Synchronisierung des Zeitstempels der Datei mit dem einer anderen Datei müssen sich beide Dateien zusammen mit dem Touch Tool am selben Speicherort befinden.

3. Öffnen Sie ein Befehlszeilenfenster, und wechseln Sie in das Verzeichnis mit der Touch Tool Anwendung.

4. Geben Sie folgenden Befehl ein:

   ```
   TmTouch.exe <Zieldateiname> <Quelldateiname>
   ```

   Wobei gilt:

   - `<Zieldateiname>` ist der Name der Hotfix-Datei, deren Zeitstempel geändert werden soll.
   - `<Quelldateiname>` ist der Name der Datei, deren Zeitstempel kopiert werden soll.

   Hinweis

   Wenn Sie keinen Quelldateinamen angeben, wird der Zeitstempel der Zieldatei an die Systemzeit des Endpunkts angepasst. Das Platzhalterzeichen (*) darf im Zieldateinamen, jedoch nicht im Quelldateinamen verwendet werden.

5. Um zu überprüfen, ob der Zeitstempel geändert wurde, geben Sie `dir` in die Befehlszeile ein, oder überprüfen Sie die Eigenschaften der Datei in Windows Explorer.

Update-Agents

Für die Zuordnung des Verteilvorgangs von Komponenten, Domäneneinstellungen oder Agent-Programmen und Hotfixes an OfficeScan Agents verwenden Sie OfficeScan Agents als Update-Agents oder Update-Adressen für andere OfficeScan Agents. Auf diese Weise erhalten die OfficeScan Agents rechtzeitig ihre Updates, ohne die Verbindung zum OfficeScan Server durch ein hohes Netzwerk-Datenverkehrsvolumen zu belasten.

Wenn das Netzwerk beispielsweise nach Standorten segmentiert ist und das Datenaufkommen über die Netzwerkverbindung besonders hoch ist, sollten Sie mindestens einen Update-Agent pro Standort einrichten.

Hinweis

OfficeScan Agents Agents, für die die Aktualisierung von Komponenten über einen Update-Agent zugewiesen ist, erhalten über den Update-Agent nur aktualisierte Komponenten und Einstellungen. Alle OfficeScan Agents melden ihren Status weiterhin an den OfficeScan Server.

Systemvoraussetzungen des Update-Agents

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

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

Konfiguration des Update-Agents

Update-Agents werden in zwei Schritten konfiguriert:

1. Weisen Sie den OfficeScan Agent als Update-Agent für bestimmte Komponenten zu.

2. Legen Sie die agents fest, die über diesen Update-Agent aktualisiert werden.

Hinweis

Die Anzahl der gleichzeitigen agent-Verbindungen, die ein einzelner Update-Agent bearbeiten kann, hängt von den jeweiligen Hardware-Spezifikationen des Endpunkt ab.

OfficeScan Agenten als Update-Agents zuweisen

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Wählen Sie in der agent-Hierarchie die agents aus, die als Update-Agents vorgesehen werden sollen.

Hinweis

Das Symbol der Root-Domäne können Sie jedoch nicht auswählen, da dann alle agents als Update-Agents festgelegt würden. Ein reiner IPv6-Update-Agent kann Updates nicht direkt auf reine IPv4-agents verteilen. Ebenso kann ein reiner IPv4-Update-Agent keine Updates direkt auf reine IPv6-agents verteilen. Ein Dual-Stack-Proxy-Server wie beispielsweise DeleGate, der IP-Adressen konvertieren kann, muss ermöglichen, dass der Update-Agent Updates auf die agents verteilen kann.

3. Klicken Sie auf **Einstellungen** > **Update-Agent-Einstellungen**.
4. Wählen Sie die Komponenten aus, die Update-Agents freigeben können.
   - Komponenten-Updates
   - Domäneneinstellungen
   - OfficeScan Agent-Programme und Hotfixes
5. Klicken Sie auf **Speichern**.

OfficeScan Agenten festlegen, die über einen Update-Agent aktualisiert werden

Prozedur

1. Navigieren Sie zu **Updates** > **Agents** > **Update-Adresse**.
2. Klicken Sie unter **Liste der benutzerdefinierten Update-Adresse** auf **Hinzufügen**.
3. Geben Sie im angezeigten Fenster die agents-IP-Adresse ein. Sie können einen IPv4-Bereich und/oder ein IPv6-Präfix und die -Länge eingeben.
4. Wählen Sie im Feld **Update-Agent** den Update-Agent aus, den Sie den agents zuordnen möchten.

   Hinweis

   Stellen Sie sicher, dass sich die agents mit dem Update-Agent verbinden können, indem sie ihre IP-Adresse verwenden. Wenn Sie beispielsweise einen IPv4-Adressbereich festgelegt haben, muss der Update-Agent eine IPv4-Adresse haben. Wenn Sie ein IPv6-Präfix und eine -Länge festgelegt haben, muss der Update-Agent eine IPv6-Adresse haben.

5. Klicken Sie auf **Speichern**.

Update-Adresse für Update-Agents

Update-Agents können Updates von verschiedenen Adressen beziehen, beispielsweise vom OfficeScan Server oder von einer benutzerspezifischen Update-Adresse. Konfigurieren Sie die Update-Adresse im Fenster Update-Adresse der Webkonsole.

IPv6-Unterstützung für Update-Agents

Ein reiner IPv6-Update-Agent kann Updates nicht direkt aus reinen IPv4-Update-Adressen erhalten wie:

- Ein reiner IPv4-OfficeScan Server
- Jede reine, benutzerdefinierte IPv4-Update-Adresse
- Trend Micro ActiveUpdate server

Ebenfalls kann ein reiner IPv4-Update-Agent Updates nicht direkt aus reinen IPv6-Update-Adressen erhalten wie einem reinen IPv6 OfficeScan Server.

Ein Dual-Stack-Proxy-Server, der IP-Adressen wie DeleGate konvertieren kann, muss ermöglichen, dass die Update-Agents eine Verbindung zu den Update-Adressen herstellen können.

Standard-Update-Adresse für Update-Agents

Der OfficeScan Server ist die Standard-Update-Adresse für die Update-Agents. Wenn Sie die Agents für direktes Aktualisieren vom OfficeScan Server einrichten, verläuft der Update-Vorgang wie folgt:

1. Der Update-Agent bezieht die Updates vom OfficeScan Server.
2. Ist die Aktualisierung vom OfficeScan Server aus nicht möglich, versucht der Agent, eine direkte Verbindung zum Trend Micro ActiveUpdate Server aufzubauen, sofern Folgendes ganz oder teilweise zutrifft:
   - Wenn Sie in **Agents** > **Agent-Verwaltung** auf **Einstellungen** > **Berechtigungen und andere Einstellungen** > **Andere Einstellungen** > **Update-Einstellungen** klicken, wird die Option **OfficeScan Agents laden Dateien vom Trend Micro ActiveUpdate Server herunter** aktiviert.
   - Der ActiveUpdate Server ist der ersten Eintrag in der Liste der benutzerdefinierten Update-Adressen.

Tipp

Setzen Sie den ActiveUpdate Server nur dann an die erste Stelle der Liste, wenn das Update über den OfficeScan Server Probleme bereitet. Wenn Update-Agents die Updates direkt vom ActiveUpdate Server beziehen, wird viel Bandbreite zwischen Netzwerk und Internet benötigt.

3. Ist von allen möglichen Adressen kein Update möglich, bricht der Update-Agent den Update-Vorgang ab.

Benutzerdefinierte Update-Adresse für Update-Agents

Neben dem OfficeScan Server können Update-Agents auch von anderen Update-Adressen aus aktualisiert werden. Benutzerdefinierte Update-Adressen tragen dazu bei, den Datenverkehr zum agent Server bei der Aktualisierung von OfficeScan zu reduzieren. Sie können in der Liste der benutzerdefinierten Update-Adressen bis zu 1024 benutzerdefinierte Update-Adressen festlegen. Weitere Informationen zum Konfigurieren der Liste finden Sie unter *Benutzerdefinierte Update-Adressen für OfficeScan Agenten auf Seite 6-34*.

Hinweis

Stellen Sie sicher, dass die Option **Update-Agents aktualisieren Komponenten, Domäneneinstellungen, Agent-Programme und Hotfixes nur vom OfficeScan Server aus** im Fenster **Update-Adressen für Agents** (**Updates** > **Agents** > **Update-Adresse**) deaktiviert ist, damit die Update-Agents Verbindungen mit den benutzerdefinierten Update-Adressen herstellen.

Nachdem Sie die Liste erstellt und gespeichert haben, wird der Update-Vorgang wie folgt ausgeführt:

1. Der Update-Agent führt das Update anhand des ersten Eintrags in der Liste durch.
2. Wenn es nicht möglich ist, anhand des ersten Eintrags zu aktualisieren, führt der Agent das Update vom zweiten Eintrag aus durch, usw.
3. Falls kein Eintrag ein Update ermöglicht, prüft der Agent die folgenden Optionen unter **OfficeScan Agents aktualisieren die folgenden Elemente vom OfficeScan Server, wenn keine benutzerdefinierten Adressen verfügbar sind oder gefunden wurden**:

    - **Komponenten**: Sofern aktiviert, bezieht der Agent die Updates vom OfficeScan Server.

      Ist die Option deaktiviert, versucht der Agent, eine direkte Verbindung zum Trend Micro ActiveUpdate Server aufzubauen, sofern Folgendes ganz oder teilweise zutrifft:

Hinweis

Sie können nur Komponenten vom ActiveUpdate Server aktualisieren. Domäneneinstellungen sowie Programme und Hotfixes können nur vom Server oder von Update-Agents heruntergeladen werden.

- Wenn Sie in **Agents** > **Agent-Verwaltung** auf **Einstellungen** > **Berechtigungen und andere Einstellungen** > **Andere Einstellungen** > **Update-Einstellungen** klicken, wird die Option **Agents laden Dateien vom Trend Micro ActiveUpdate Server herunter** aktiviert.
- Der ActiveUpdate Server ist nicht in der Liste der benutzerdefinierten Update-Adressen enthalten.

- **Domäneneinstellungen**: Sofern aktiviert, bezieht der Agent die Updates vom OfficeScan Server.
- **OfficeScan Agent-Programme und Hotfixes**: Sofern aktiviert, bezieht der Agent die Updates vom OfficeScan Server.

4. Ist von allen möglichen Adressen kein Update möglich, bricht der Update-Agent den Update-Vorgang ab.

Das Update wird anders ausgeführt, wenn die Option **Standardmäßige Update-Adresse (Update vom OfficeScan Server)** aktiviert ist, und der OfficeScan Server den Agent über das Komponenten-Update benachrichtigt. Die folgenden Schritte werden ausgeführt:

1. Der Agent bezieht Updates direkt vom OfficeScan Server und ignoriert die Liste der Update-Adressen.
2. Ist die Aktualisierung vom Server nicht möglich, versucht der Agent, eine direkte Verbindung zum Trend Micro ActiveUpdate Server aufzubauen, sofern Folgendes ganz oder teilweise zutrifft:
   - Wenn Sie in **Agents** > **Agent-Verwaltung** auf **Einstellungen** > **Berechtigungen und andere Einstellungen** > **Andere Einstellungen** > **Update-Einstellungen** klicken, wird die Option **OfficeScan Agents laden Dateien vom Trend Micro ActiveUpdate Server herunter** aktiviert.

- Der ActiveUpdate Server ist der ersten Eintrag in der Liste der benutzerdefinierten Update-Adressen.

Tipp

Setzen Sie den ActiveUpdate Server nur dann an die erste Stelle der Liste, wenn das Update über den OfficeScan Server Probleme bereitet. Wenn OfficeScan Agents direkt vom ActiveUpdate Server aktualisiert werden, wird viel Bandbreite zwischen Netzwerk und Internet benötigt.

3. Ist von allen möglichen Adressen kein Update möglich, bricht der Update-Agent den Update-Vorgang ab.

Update-Adresse für den Update-Agenten konfigurieren

Prozedur

1. Navigieren Sie zu **Updates** > **Agents** > **Update-Adresse**.
2. Wählen Sie aus, ob Updates über die Standard-Update-Adresse für Update-Agents (OfficeScan Server) oder über die benutzerdefinierten Update-Adressen für Update-Agents bezogen werden sollen.
3. Klicken Sie auf **Alle Agents benachrichtigen**.

Update-Agent-Komponenten duplizieren

Beim Download von Komponenten verwenden Update-Agents ebenso wie der OfficeScan Server die Komponentenduplizierung. Weitere Informationen darüber, wie der Server Komponenten dupliziert, finden Sie unter *OfficeScan Server-Komponentenduplizierung auf Seite 6-22*.

Die Komponentenduplizierung für Update-Agents funktioniert wie folgt:

1. Der Update-Agent vergleicht die aktuelle, vollständige Pattern-Version mit der neuesten Version auf der Update-Adresse. Beträgt der Unterschied zwischen beiden Versionen maximal 14, lädt der Update-Agent das inkrementelle Pattern herunter, das den Unterschied zwischen den beiden Versionen umfasst.

Hinweis

Ist der Unterschied größer als 14, lädt der Update-Agent automatisch die vollständige Version der Pattern-Datei herunter.

2. Der Update-Agent integriert das inkrementelle, gerade heruntergeladene Pattern in sein aktuelles vollständiges Pattern und erhält so das neueste vollständige Pattern.
3. Der Update-Agent lädt die restlichen inkrementellen Pattern von der Update-Adresse herunter.
4. Das neueste vollständige Pattern und alle inkrementellen Pattern werden den agents zur Verfügung gestellt.

Update-Methoden für Update-Agents

Update-Agents verwenden die gleichen Update-Methoden, die auch für reguläre agents verfügbar sind. Weitere Informationen finden Sie unter *OfficeScan Agent Update-Methoden auf Seite 6-40*.

Mit dem Konfigurationsassistenten für das zeitgesteuerte Update können Sie auch zeitgesteuerte Updates auf Update-Agents aktivieren und konfigurieren, die mit Hilfe von Agent Packager installiert wurden.

Hinweis

Dieser Assistent ist nicht verfügbar, wenn der Update-Agent auf eine andere Art installiert wurde. Weitere Informationen finden Sie unter *Überlegungen zur Verteilung auf Seite 5-12*.

Den Konfigurationsassistenten für das zeitgesteuerte Update verwenden

Prozedur

1. Navigieren Sie auf dem Update-Agent-Endpunkt zu <*Installationsordner des Agents*>.
2. Doppelklicken Sie auf die Datei `SUCTool.exe`, um den Assistenten auszuführen. Die Konsole des Konfigurationsassistenten für das zeitgesteuerte Update wird geöffnet.

3. Klicken Sie auf **Zeitgesteuertes Update aktivieren**.
4. Geben Sie den Startzeitpunkt und das Zeitintervall für die Updates an.
5. Klicken Sie auf **Übernehmen**.

Update-Agent - Analysebericht

Erzeugen Sie den Update-Agent - Analysebericht zur Analyse der Update-Infrastruktur und ermitteln Sie, welche agents die Downloads von teilweisen Updates über Update-Agents und andere Update-Adressen vornehmen.

Hinweis

Dieser Bericht enthält alle OfficeScan Agents, die für den Empfang teilweiser Updates von Update-Agents konfiguriert sind. Wenn Sie die Aufgabe, eine oder mehrere Domänen zu verwalten, auf andere Administratoren übertragen haben, sehen diese auch alle OfficeScan Agents, die für den Empfang von teilweisen Updates von Update-Agents konfiguriert sind, die Domänen angehören, welche nicht von ihnen verwaltet werden.

OfficeScan exportiert den Update-Agent - Analysebericht in einer komma-separierten Datei (`.csv`).

Dieser Bericht enthält die folgenden Informationen:

- OfficeScan Agent Endpunkt
- IP-Adresse
- Agent Pfad der Agent-Hierarchie
- Update-Adresse
- Wenn agents Folgendes von Update-Agents herunterladen:
  - Komponenten
  - Domäneneinstellungen
  - OfficeScan Agent Agent-Programme und Hotfixes

Wichtig

Der Update-Agent - Analysebericht enthält nur OfficeScan Agents, für die teilweise Updates über einen Update Agent konfiguriert sind. OfficeScan Agents für die vollständige Updates von einem Update-Agent konfiguriert sind (einschließlich Komponenten, Domäneneinstellungen und OfficeScan Agent-Programmen und Hotfixes) sind nicht im Bericht enthalten.

Weitere Informationen zum Generieren des Berichts finden Sie unter *Benutzerdefinierte Update-Adressen für OfficeScan Agenten auf Seite 6-34*.

Komponenten-Update - Zusammenfassung

Im Fenster **Übersicht aktualisieren** auf der Webkonsole (navigieren Sie zu **Updates** > **Zusammenfassung**) erhalten Sie Informationen über den allgemeinen Status der Komponenten-Updates und können veraltete Komponenten aktualisieren. Wenn Sie zeitgesteuerte Server-Updates aktivieren, zeigt das Fenster auch den nächsten Update-Zeitplan.

Aktualisieren Sie das Fenster regelmäßig, um den aktuellen Status des Komponenten-Updates anzuzeigen.

Hinweis

Um Komponenten-Updates auf dem integrierten Smart Protection Server anzuzeigen, navigieren Sie zu **Administration** > **Smart Protection** > **Integrierter Server**.

Update-Status für OfficeScan Agenten

Wenn Sie das Komponenten-Update für agents gestartet haben, betrachten Sie die folgenden Informationen in diesem Abschnitt:

- Anzahl der zum Komponenten-Update aufgeforderten agents
- Anzahl der noch nicht benachrichtigten agents, die sich aber bereits in der Warteschlange befinden. Um die Benachrichtigung dieser agents abzubrechen, klicken Sie auf **Benachrichtigung abbrechen**.

Komponenten

Die Tabelle **Update-Status** zeigt den Update-Status für jede Komponente an, die der OfficeScan Server herunterlädt und verteilt.

Für jede Komponente sehen Sie die aktuelle Version und das Datum des letzten Updates. Sie können durch Klicken auf den Link mit der Nummer agents mit veralteten Komponenten anzeigen. agents mit nicht aktuellen Komponenten manuell aktualisieren.

Kapitel 7

Nach Sicherheitsrisiken suchen

In diesem Kapitel wird erläutert, wie Sie Endpunkte mit der dateibasierten Suche vor Sicherheitsrisiken schützen.

Es werden folgende Themen behandelt:

- *Info über Sicherheitsrisiken auf Seite 7-2*
- *Suchmethodentypen auf Seite 7-9*
- *Suchtypen auf Seite 7-16*
- *Gemeinsame Einstellungen für alle Suchtypen auf Seite 7-29*
- *Suchberechtigungen und andere Einstellungen auf Seite 7-62*
- *Allgemeine Sucheinstellungen auf Seite 7-79*
- *Benachrichtigungen bei Sicherheitsrisiken auf Seite 7-90*
- *Sicherheitsrisiko-Protokolle auf Seite 7-101*
- *Ausbrüche von Sicherheitsrisiken auf Seite 7-117*

Info über Sicherheitsrisiken

Sicherheitsrisiko ist der Sammelbegriff für Viren/Malware und Spyware/Grayware. OfficeScan schützt Endpunkte vor Sicherheitsrisiken, indem zunächst Dateien durchsucht werden. Anschließend wird für jedes erkannte Sicherheitsrisiko eine bestimmte Aktion durchgeführt. Eine große Anzahl erkannter Sicherheitsrisiken innerhalb kurzer Zeit deutet auf einen Virenausbruch hin. Durch Anwendung von Ausbruchspräventionsrichtlinien und vorübergehende Isolation infizierter Endpunkte können mit Hilfe von OfficeScan schädliche Auswirkungen vermieden bzw. minimiert werden. Benachrichtigungen und Protokolle helfen bei der Verfolgung der Sicherheitsrisiken und alarmieren Sie, wenn ein sofortiges Handeln erforderlich ist.

Viren und Malware

Zehntausende von Viren und Malware-Typen sind bereits bekannt, und täglich kommen neue hinzu. Endpunkt-Viren 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 Websites von Unternehmen ausnutzen.

TABELLE 7-1. Viren-/Malware-Typen

VIREN-/ MALWARE-TYP	BESCHREIBUNG
Scherzprogramm	Scherzprogramme sind virenähnliche Programme, die oftmals die Anzeige auf dem Endpunkt-Bildschirm verändern.
Andere	Die Kategorie „Andere“ umfasst sämtliche Viren und Malware, die nicht zu einem der anderen Virus- bzw. Malware-Typen zählen.
Packer	Packer sind komprimierte und/oder verschlüsselte ausführbare Programme für Windows oder Linux™; häufig handelt es sich dabei um Trojaner. In komprimierter Form ist ein Packer für ein Antiviren-Programm schwieriger zu erkennen.

Viren-/ Malware-Typ	Beschreibung
Ransomware	Ransomware ist eine Bedrohungsart, die Dateien verschlüsselt, ändert oder sperrt und anschließend versucht, den Benutzer zur Zahlung von Lösegeld zu erpressen, damit dieser die Daten wieder abrufen kann. Einige Ransomware-Bedrohungen löschen die Daten automatisch, wenn das Lösegeld nicht rechtzeitig gezahlt wird.
Rootkit	Rootkits sind Programme (oder Sammlungen von Programmen), die Code auf einem System ohne Zustimmung oder Wissen des Endbenutzers installieren und ausführen. Sie nutzen 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.
Test virus	Testviren sind inaktive Dateien, die sich wie Viren verhalten und von Antiviren-Software erkannt werden. Mit Testviren wie dem EICAR-Testskript können Sie die Funktion Ihrer Antiviren-Software überprüfen.
Trojaner	Trojaner verschaffen sich oft über Ports Zugriff auf Computer oder ausführbare Programme. 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-/ Malware-Typ	Beschreibung
Virus	Viren sind Programme, die sich replizieren. 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. • **Bootvirus**: 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. • **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 Endpunkt-Systeme (meist per E-Mail) verteilen kann.
Netzwerkvirus	Nicht jeder Virus, der sich über ein Netzwerk verbreitet, ist zwangsläufig ein Netzwerkvirus. Nur einige der Viren-/Malware-Typen zählen zu dieser Kategorie. Netzwerkviren verbreiten sich grundsätzlich über Netzwerkprotokolle wie TCP, FTP, UDP, HTTP und E-Mail-Protokolle. Systemdateien und die Bootsektoren von Festplatten werden meist nicht verändert. Stattdessen infizieren Netzwerkviren den Arbeitsspeicher von agent Endpunkte und erzwingen so eine Überflutung des Netzwerks mit Daten. Dies führt zu einer Verlangsamung oder, schlimmer noch, dem vollständigen Ausfall des Netzwerks. Mit herkömmlichen, auf Dateiein und -ausgabe basierenden Suchmethoden können Netzwerkviren, die im Arbeitsspeicher resident sind, in der Regel nicht entdeckt werden.

VIREN-/ MALWARE-TYP	BESCHREIBUNG
Wahrscheinlich Virus/ Malware	Wahrscheinliche Viren/Malware sind verdächtige Dateien, die einige Eigenschaften von Viren/Malware aufweisen. Weitere Informationen finden Sie in der Trend Micro Bedrohungsenzyklopädie: http://about-threats.trendmicro.com/de/threatencyclopedia#malware **Hinweis** Die Aktion "Säubern" kann nicht auf wahrscheinliche Viren/ Malware ausgeführt werden, aber die Suchaktion ist konfigurierbar.

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 Endpunkte 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 Endpunkt angegriffen werden kann.

Senden Sie verdächtige Dateien oder Anwendungen, die OfficeScan nicht als Grayware erkennen kann, zur Analyse an Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

TYP	BESCHREIBUNG
Spyware	Diese Software sammelt Daten, z. B. Benutzernamen und Kennwörter, und leitet sie an Dritte weiter.

Typ	Beschreibung
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 Endpunkt-Internet-Einstellungen und erzwingt auf dem Endpunkt das Wählen von voreingestellten Telefonnummern. Oft handelt es sich um Pay-per-Call oder internationale Rufnummern, die dem Unternehmen beträchtliche Kosten verursachen können.
Scherzprogramm	Diese Software verursacht ungewöhnliches Endpunkt-Verhalten, z. B. das Öffnen und Schließen des CD-ROM-Laufwerks oder die Anzeige zahlreicher Nachrichtenfelder.
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.

So gelangt Spyware/Grayware in das Netzwerk

Spyware/Grayware gelangt häufig bei der Installation heruntergeladener rechtmäßiger Software in das Unternehmensnetzwerk. Die meisten Software-Programme enthalten eine Endbenutzer-Lizenzvereinbarung (EULA), die der Benutzer vor dem Download akzeptieren muss. Die EULA weist zwar auf die zusätzlich installierte Anwendung und das Sammeln persönlicher Daten hin; viele Benutzer überlesen dies jedoch oder verstehen die juristische Ausdruckweise nicht, mit der die Anwendung beschrieben wird.

Mögliche Risiken und Bedrohungen

Spyware und andere Typen von Grayware im Netzwerk können folgende Gefahren bergen:

TABELLE 7-2. Mögliche Risiken und Bedrohungen

RISIKO ODER BEDROHUNG	BESCHREIBUNG
Verringerte Endpunkt-Leistung	Spyware/Grayware beansprucht oft beträchtliche Ressourcen (Prozessor, Arbeitsspeicher).
Mehr Abstürze des Webbrowsers	Bestimmte Grayware-Typen, wie z. B. Adware, zeigen oftmals Informationen in einem Browser-Rahmen oder -Fenster an. Je nachdem, wie der Code dieser Programme in die Systemprozesse eingreift, führt Grayware in manchen Fällen zum Absturz oder Einfrieren des Browsers, so dass möglicherweise ein Neustart des Endpunkts erforderlich ist.
Geringere Benutzereffizienz	Durch die negativen Auswirkungen von Scherzprogrammen und Popup-Fenstern, die ständig geschlossen werden müssen, werden die Benutzer von ihrer eigentlichen Tätigkeit abgelenkt.
Verringerung der Netzwerkbandbreite	Häufig übermittelt Spyware/Grayware die gesammelten Daten in regelmäßigen Abständen an Anwendungen im Netzwerk oder außerhalb.
Verlust persönlicher und unternehmensintern er Informationen	Nicht alle von Spyware/Grayware gesammelten Daten sind so harmlos wie Listen besuchter Websites. Spyware/Grayware sammelt auch Benutzernamen und Kennwörter für den Zugriff auf persönliche Konten, wie z. B. Bank- oder Firmenkonten von Benutzern in Ihrem Netzwerk.
Höheres Risiko von Haftungsansprüche n	Mit Hilfe der gestohlenen Endpunkt-Ressourcen aus Ihrem Netzwerk können Hacker möglicherweise unter Verwendung des agents Angriffe starten oder Spyware/Grayware auf Computern außerhalb des Netzwerks installieren. Dadurch könnten gegenüber Ihrem Unternehmen Haftungsansprüche geltend gemacht werden.

Schutz vor Spyware/Grayware und anderen Bedrohungen

Es gibt viele Möglichkeiten, die Installation von Spyware/Grayware auf Ihrem Endpunkt zu verhindern. Trend Micro empfiehlt Folgendes:

- Konfigurieren Sie alle Virensuchtypen (manuelle Suche, Echtzeitsuche, zeitgesteuerte Suche und Jetzt durchsuchen), um Spyware-/Grayware-Dateien und -Anwendungen zu suchen und zu entfernen. Weitere Informationen finden Sie unter *Suchtypen auf Seite 7-16*.

- Weisen Sie die agent-Benutzer darauf hin,

  - die Endbenutzer-Lizenzvereinbarung (EULA) und die zugehörige Dokumentation für Anwendungen, die sie herunterladen oder installieren, aufmerksam zu lesen;

  - Klicken Sie auf **Nein**, wenn Sie aufgefordert werden, dem Download und der Installationen von Software zuzustimmen, es sei denn, die agent-Benutzer sind sich sicher, dass sowohl der Hersteller der Software als auch die geöffnete Website vertrauenswürdig sind.

  - unerwünschte und kommerzielle E-Mails (Spam) zu ignorieren, insbesondere, wenn der Benutzer aufgefordert wird, auf eine Schaltfläche oder einen Link zu klicken.

- Konfigurieren Sie die Einstellungen des Webbrowsers so, dass eine strenge Sicherheitsstufe gewährleistet ist. Trend Micro empfiehlt, den Webbrowser so einzustellen, dass Benutzer vor der Installation von ActiveX-Steuerelementen informiert werden.

- Konfigurieren Sie die Sicherheitseinstellungen in Microsoft Outlook so, dass HTML-Elemente, wie z. B. Bilder in Spam-Nachrichten, nicht automatisch heruntergeladen werden.

- Untersagen Sie die Nutzung von Peer-to-Peer-Tauschbörsen. Hinter mp3-Dateien, die von den Benutzern heruntergeladen werden, könnte sich Spyware oder Grayware verbergen.

- Überprüfen Sie regelmäßig, ob es sich bei der auf den Agent-Computern installierten Software um Spyware oder andere Grayware handelt.

- Installieren Sie stets die aktuellen Microsoft Patches auf Ihrem Windows Betriebssystem. Weitere Informationen finden Sie auf der Microsoft Website.

Suchmethodentypen

Bei der Suche nach Sicherheitsrisiken können OfficeScan Agents eine von zwei Suchmethoden anwenden: Die Suchmethoden sind intelligente Suche und herkömmliche Suche.

- **Intelligente Suche**

  OfficeScan Agents, die die intelligente Suche 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**

  Agents, die keine intelligente Suche durchführen, werden als **Agents der herkömmlichen Suche** bezeichnet. Ein agent der herkömmlichen Suche speichert alle OfficeScan Agent-Komponenten auf dem Endpunkt und durchsucht alle Dateien lokal.

Standard-Suchmethode

In dieser Version von OfficeScan wird bei Erstinstallationen die intelligente Suche als Standard-Suchmethode festgelegt. Dies bedeutet, dass alle vom Server verwalteten Agents die intelligente Suche verwenden, sofern Sie nach einer Erstinstallation des OfficeScan Servers nicht die Suchmethode über die Webkonsole ändern.

Wenn Sie den OfficeScan Server von einer Vorgängerversion upgraden und das automatische Agent-Upgrade aktiviert ist, verwenden alle vom Server verwalteten Agents weiterhin die Suchmethode, die vor dem Upgrade konfiguriert wurde. Wenn Sie beispielsweise ein Upgrade von einer früheren Version von OfficeScan durchführen, die die intelligente Suche sowie die herkömmliche Suche unterstützt, verwenden alle aktualisierten Agents mit intelligenter Suche weiterhin die intelligente Suche und alle Agents mit herkömmlicher Suche die herkömmliche Suche.

Suchmethoden im Vergleich

Die folgende Tabelle beinhaltet einen Vergleich zwischen den beiden Suchmethoden:

TABELLE 7-3. Vergleich zwischen herkömmlicher Suche und intelligenter Suche

VERGLEICHSGRUNDLAGE	HERKÖMMLICHE SUCHE	INTELLIGENTE SUCHE
Verfügbarkeit	In dieser OfficeScan Version und allen früheren OfficeScan Versionen verfügbar	Verfügbar ab OfficeScan 10
Suchverhalten	Der agent der herkömmlichen Suche durchsucht den lokalen Endpunkt.	• Der agent der intelligenten Suche durchsucht den lokalen Endpunkt. • Wenn der agent das Risiko der Datei während der Suche nicht ermitteln kann, überprüft der agent dies, indem er eine Suchabfrage an die Smart Protection Quelle sendet. • Der agent legt die Suchabfrageergebnisse zur Verbesserung der Suchleistung in einem Zwischenspeicher ab.
Verwendete und aktualisierte Komponenten	Alle unter der Update-Adressse verfügbaren Komponenten, außer das Agent-Pattern der intelligenten Suche	Alle unter der Update-Adressse verfügbaren Komponenten, außer das Viren-Pattern und das Pattern zur aktiven Spyware-Überwachung
Typische Update-Adresse	OfficeScan Server	OfficeScan Server

Suchmethode ändern

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Sucheinstellungen** > **Suchmethoden**.
4. Wählen Sie **Herkömmliche Suche** oder **Intelligente Suche** aus.
5. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Wechsel von der intelligenten Suche zur herkömmlichen Suche

In der folgenden Tabelle sind einige Aspekte aufgeführt, die Sie beachten sollten, bevor Sie die von OfficeScan Agents verwendete Suchmethode ändern.

1. Anzahl der umzuschaltenden OfficeScan Agents

   Wenn Sie eine relativ kleine Anzahl von OfficeScan Agents gleichzeitig umschalten, werden die Ressourcen von OfficeScan Server und Smart Protection Server effizient genutzt. Diese Server können andere wichtige Aufgaben ausführen, während OfficeScan Agents die Suchmethoden ändern.

2. Timing

   Wenn Suchmethoden geändert werden, müssen OfficeScan Agents die Vollversionen der erforderlichen Pattern-Dateien für die neue Suchmethode herunterladen.

   Der Wechsel sollte außerhalb der Spitzenzeiten erfolgen, um die Auswirkungen auf die Bandbreite und die Unterbrechung der täglichen Aufgaben der Endbenutzer möglichst gering zu halten. Trend Micro empfiehlt, während des Konvertierungsvorgangs die Option "Jetzt aktualisieren" in OfficeScan Agents zu deaktivieren.

3. Einstellungen der Agent-Hierarchie

   Die Suchmethode ist eine granulare Einstellung, die Sie auf Root- oder Domänenebene oder für einen einzelnen OfficeScan Agent festlegen können. Wenn Sie die Suchmethode wechseln, können Sie:

   - Erstellen Sie eine neue agent-Hierarchiedomäne und ordnen Sie die herkömmliche Suche als Suchmethode zu. Alle agent, die Sie in diese Domäne verschieben, werden die herkömmliche Suche verwenden. Wenn Sie den agent verschieben, aktivieren Sie die Einstellung **Einstellungen der neuen Domäne für ausgewählte Agents übernehmen**.
   - Wählen Sie eine Domäne aus, und konfigurieren Sie diese zur Verwendung der herkömmlichen Suche. agents der intelligenten Suche, die einer Domäne angehören, werden für die herkömmliche Suche aktiviert.
   - Wählen Sie einen oder mehrere agents der intelligenten Suche aus einer Domäne aus und schalten Sie diese dann auf die herkömmliche Suche um.

Hinweis

Alle Änderungen an der Suchmethode der Domäne überschreiben die Suchmethode, die Sie für individuelle agents konfiguriert haben.

Wechsel von der herkömmlichen Suche zur intelligenten Suche

Wenn Sie agents von der herkömmlichen Suche auf die intelligente Suche umstellen, sollte Smart Protection-Dienste eingerichtet sein.

Weitere Informationen finden Sie unter *Smart Protection Services einrichten auf Seite 4-13*.

Die folgende Tabelle enthält weitere Überlegungen zur Umstellung auf die intelligente Suche.

TABELLE 7-4. Überlegungen bei der Umstellung auf die intelligente Suche

ÜBERLEGUNG	DETAILS
Produktlizenz	Um die intelligente Suche zu verwenden, vergewissern Sie sich, dass Sie die Lizenzen für die folgenden Dienste aktiviert haben und die Lizenzen nicht abgelaufen sind: • Virenschutz • Web Reputation und Anti-Spyware
OfficeScan Server	Stellen Sie sicher, dass die Agents eine Verbindung zum OfficeScan Server aufbauen können. Nur Online-Agents erhalten die Benachrichtigung, die intelligente Suche zu aktivieren. Offline-Agents erhalten die Benachrichtigung erst dann, wenn sie wieder online gehen. Unabhängige Agents werden benachrichtigt, wenn sie wieder online sind oder wenn zeitgesteuerte Updates ausgeführt werden (wenn der Agent Berechtigungen für zeitgesteuerte Updates aufweist). Stellen Sie auch sicher, dass der OfficeScan Server über die neuesten Komponenten verfügt, weil Agents der intelligenten Suche das Agent-Pattern der intelligenten Suche vom Server herunterladen müssen. Informationen zum Update von Komponenten finden Sie unter *OfficeScan Server-Updates auf Seite 6-16*.

Überlegung	Details
Anzahl der umzuschaltenden agents	Wenn Sie eine relativ kleine Anzahl von Agents gleichzeitig umstellen, werden die Ressourcen des OfficeScan Servers effizient genutzt. Der OfficeScan Server kann andere kritische Aufgaben ausführen, während Agents ihre Suchmethoden ändern.
Timing	Wenn Sie zum ersten Mal auf die intelligente Suche umstellen, müssen Agents die Vollversion des Agent-Pattern der intelligenten Suche vom OfficeScan Server herunterladen. Das Smart Scan Pattern wird nur von Agents der intelligenten Suche verwendet. Die Umschaltung sollte bei geringem Netzaufkommen durchgeführt werden, um sicherzustellen, dass der Download-Prozess in kurzer Zeit beendet wird. Außerdem sollten Sie dann umschalten, wenn keine Aktualisierung eines Agents über den Server geplant ist. Deaktivieren Sie außerdem vorübergehend die Funktion "Jetzt aktualisieren", und aktivieren Sie sie wieder, nachdem die Umschaltung der Agents zur intelligenten Suche beendet wurde.

Überlegung	Details
Agent-Hierarchieeinstellungen	Die Suchmethode ist eine granuläre Einstellung, die auf Stamm- oder Domänenebene oder für einzelne Agents festgelegt werden kann. Bei der Umschaltung zur intelligenten Suche können Sie Folgendes tun: • Erstellen Sie eine neue Agent-Hierarchiedomäne, und ordnen Sie die intelligente Suche als Suchmethode zu. Alle Agents, die Sie in diese Domäne verschieben, werden die intelligente Suche verwenden. Wenn Sie den Agent verschieben, aktivieren Sie die Einstellung **Einstellungen der neuen Domäne für ausgewählte Agents übernehmen**. • Wählen Sie eine Domäne aus, und konfigurieren Sie diese zur Verwendung der intelligenten Suche. Agents der herkömmlichen Suche, die einer Domäne angehören, werden für die intelligente Suche aktiviert. • Wählen Sie einen oder mehrere Agents der herkömmlichen Suche aus einer Domäne, und schalten Sie diese dann auf die intelligente Suche um. **Hinweis** Alle Änderungen an der Suchmethode der Domäne überschreiben die Suchmethode, die Sie für einzelne Agents konfiguriert haben.

Überlegung	Details
IPv6-Unterstützung	Die Agents der intelligenten Suche senden Suchabfragen an Smart Protection Quellen. Ein reiner IPv6-Agent der intelligenten Suche kann Abfragen nicht direkt an IPv4-Quellen senden wie zum Beispiel: • Smart Protection Server 2.0 (integriert oder standalone) **Hinweis** IPv6-Unterstützung für Smart Protection Server ist ab Version 2.5 verfügbar. • Trend Micro Smart Protection Network Entsprechend kann ein reiner IPv4-Agent der intelligenten Suche ebenfalls keine Abfragen an reine IPv6 Smart Protection Server senden. Ein Dual-Stack-Proxy-Server wie beispielsweise DeleGate, der IP-Adressen konvertieren kann, muss ermöglichen, dass Agents der intelligenten Suche eine Verbindung zu den Quellen herstellen können.

Suchtypen

OfficeScan unterstützt die folgenden Suchtypen, um OfficeScan Agent-Computer vor Sicherheitsrisiken zu schützen:

Tabelle 7-5. Suchtypen

Suchtyp	Beschreibung
Echtzeitsuche	Bei jedem Empfang, Öffnen, Herunterladen, Kopieren oder Ändern einer Datei auf dem Endpunkt wird diese automatisch durchsucht. Weitere Informationen finden Sie unter *Echtzeitsuche auf Seite 7-17*.

SUCHTYP	BESCHREIBUNG
Manuelle Suche	Eine vom Benutzer eingeleitete Suche, bei der eine vom Benutzer angeforderte Datei oder ein Dateisatz durchsucht wird. Weitere Informationen finden Sie unter *Manuelle Suche auf Seite 7-20*.
Zeitgesteuerte Suche	Durchsucht Dateien automatisch auf dem Endpunkt basierend auf dem Zeitplan, der vom Administrator oder einem Endbenutzer konfiguriert wurde. Weitere Informationen finden Sie unter *Zeitgesteuerte Suche auf Seite 7-22*.
Jetzt durchsuchen	Eine vom Administrator eingeleitete Suche, bei der Dateien auf einem oder mehreren Zielcomputern durchsucht werden Weitere Informationen finden Sie unter *Jetzt durchsuchen auf Seite 7-25*.

Echtzeitsuche

Die Echtzeitsuche wird kontinuierlich und dauerhaft ausgeführt. Bei jedem Empfang, Öffnen, Herunterladen, Kopieren oder Ändern einer Datei wird diese durch die Echtzeitsuche durchsucht. Wenn der OfficeScan Agent kein Sicherheitsrisiko erkennt, können Benutzer mit dem Zugriff auf die Datei fortfahren. Wenn der OfficeScan Agent ein Sicherheitsrisiko oder eine mögliche Viren-/Malware-Infektion erkennt, wird eine Benachrichtigung mit dem Namen der infizierten Datei und des speziellen Sicherheitsrisikos angezeigt.

Die Echtzeitsuche verwaltet einen permanenten Zwischenspeicher für die Suche, der bei jedem Start des OfficeScan Agent neu geladen wird. Der OfficeScan Agent verfolgt Änderungen an Dateien oder Ordnern nach, die seit dem Beenden des OfficeScan Agents erfolgt sind, und entfernt diese Dateien aus dem Zwischenspeicher.

Hinweis

Um die Benachrichtigung zu ändern, öffnen Sie die Webkonsole, und navigieren Sie zu **Administration** > **Benachrichtigungen** > **Agent**.

Sie können die Einstellungen für die Echtzeitsuche für einen oder mehrere OfficeScan Agents und Domänen bzw. für alle OfficeScan Agents, die vom Server verwaltet werden, konfigurieren und anwenden.

Einstellungen der Echtzeitsuche konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Sucheinstellungen** > **Echtzeitsuche – Einstellungen**.
4. Wählen Sie die folgenden Optionen:
   - **Suche nach Viren/Malware aktivieren**
   - **Suche nach Spyware/Grayware aktivieren**

   Hinweis

   Wenn Sie die Suche nach Viren/Malware deaktivieren, wird auch die Suche nach Spyware/Grayware deaktiviert. Während eines Virenausbruchs ist es nicht möglich, die Echtzeitsuche zu deaktivieren (sie wird automatisch aktiviert, wenn sie ursprünglich deaktiviert wurde), um zu verhindern, dass der Virus Dateien oder Ordner auf den agent-Computern ändert oder löscht.
5. Konfigurieren Sie auf der Registerkarte **Ziel** die folgenden Suchkriterien:
   - *Benutzerdefinierte Aktionen für Dateien auf Seite 7-30*
   - *Zu durchsuchende Dateien auf Seite 7-30*
   - *Sucheinstellungen auf Seite 7-31*
6. Klicken Sie auf die Registerkarte **Aktion**, und konfigurieren Sie Folgendes:

TABELLE 7-6. Suchaktionen

AKTION	NACHSCHLAGEWERKE
Viren-/Malware-Aktion	Primäraktion (wählen Sie eine aus): • *ActiveAction verwenden auf Seite 7-43* • *Gleiche Aktion für alle Arten von Viren/Malware auf Seite 7-45* • *Bestimmte Aktion für jede Art von Viren/Malware auf Seite 7-45* **Hinweis** Weitere Informationen zu den einzelnen Aktionen finden Sie unter *Viren-/Malware-Suchaktionen auf Seite 7-41*. Zusätzliche Viren-/Malware-Aktionen: • *Quarantäne-Ordner auf Seite 7-45* • *Dateien vor dem Säubern sichern auf Seite 7-48* • *Damage Cleanup Services auf Seite 7-48* • *Bei Viren-/Malware-Fund Benachrichtigung anzeigen auf Seite 7-49* • *Bei Viren-/Malware-Verdacht Benachrichtigung anzeigen auf Seite 7-49*
Spyware-/Grayware-Aktion	Primäraktion: • *Spyware-/Grayware-Suchaktionen auf Seite 7-55* Zusätzliche Spyware-/Grayware-Aktion: • *Bei Spyware-/Grayware-Fund Benachrichtigung anzeigen auf Seite 7-56*

7. Konfigurieren Sie auf der Registerkarte **Suchausschlüsse** die Verzeichnisse, Dateien und Dateitypen, die von der Suche ausgeschlossen werden sollen.

   Weitere Informationen finden Sie unter *Suchausschlüsse auf Seite 7-34*.

8. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Manuelle Suche

Bei der manuellen Suche handelt es sich um eine Suche bei Bedarf, die direkt ausgeführt wird, nachdem ein Benutzer die Suche auf der OfficeScan Agent-Konsole startet. Die Dauer der Suche hängt von der Anzahl der Dateien und den Hardware-Ressourcen des OfficeScan Agent-Endpunkts ab.

Sie können die Einstellungen für die manuelle Suche für einen oder mehrere agents und Domänen bzw. für alle agents, die vom Server verwaltet werden, konfigurieren und anwenden.

Einstellungen für manuelle Suche konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Sucheinstellungen** > **Einstellungen für manuelle Suche**.

4. Konfigurieren Sie auf der Registerkarte **Ziel** die folgenden Suchkriterien:

   - *Zu durchsuchende Dateien auf Seite 7-30*
   - *Sucheinstellungen auf Seite 7-31*
   - *CPU-Auslastung auf Seite 7-33*

5. Klicken Sie auf die Registerkarte **Aktion**, und konfigurieren Sie Folgendes:

   TABELLE 7-7. Suchaktionen

AKTION	NACHSCHLAGEWERKE
Viren-/Malware-Aktion	Primäraktion (wählen Sie eine aus): • *ActiveAction verwenden auf Seite 7-43* • *Gleiche Aktion für alle Arten von Viren/Malware auf Seite 7-45* • *Bestimmte Aktion für jede Art von Viren/Malware auf Seite 7-45* **Hinweis** Weitere Informationen zu den einzelnen Aktionen finden Sie unter *Viren-/Malware-Suchaktionen auf Seite 7-41*. Zusätzliche Viren-/Malware-Aktionen: • *Quarantäne-Ordner auf Seite 7-45* • *Dateien vor dem Säubern sichern auf Seite 7-48* • *Damage Cleanup Services auf Seite 7-48*
Spyware-/Grayware-Aktion	Primäraktion: • *Spyware-/Grayware-Suchaktionen auf Seite 7-55*

6. Konfigurieren Sie auf der Registerkarte **Suchausschlüsse** die Verzeichnisse, Dateien und Dateitypen, die von der Suche ausgeschlossen werden sollen.

   Weitere Informationen finden Sie unter *Suchausschlüsse auf Seite 7-34*.

7. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Zeitgesteuerte Suche

Die zeitgesteuerte Suche wird automatisch zur angegebenen Uhrzeit am angegebenen Datum ausgeführt. Verwenden Sie die zeitgesteuerte Suche, um die routinemäßige Suche auf dem agent zu automatisieren und die Verwaltung der Virensuche zu optimieren.

Sie können die Einstellungen für die zeitgesteuerte Suche für einen oder mehrere agents und Domänen bzw. für alle agents, die vom Server verwaltet werden, konfigurieren und anwenden.

Einstellungen für zeitgesteuerte Suche konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Sucheinstellungen** > **Zeitgesteuerte Suche – Einstellungen**.
4. Wählen Sie die folgenden Optionen:

- **Suche nach Viren/Malware aktivieren**
- **Suche nach Spyware/Grayware aktivieren**

Hinweis

Bevor Sie nach Spyware/Grayware suchen können, müssen Sie die Viren-/Malware-Suche aktivieren.

5. Konfigurieren Sie auf der Registerkarte **Ziel** die folgenden Suchkriterien:
   - *Zeitplan auf Seite 7-34*
   - *Zu durchsuchende Dateien auf Seite 7-30*
   - *Sucheinstellungen auf Seite 7-31*
   - *CPU-Auslastung auf Seite 7-33*
6. Klicken Sie auf die Registerkarte **Aktion**, und konfigurieren Sie Folgendes:

TABELLE 7-8. Suchaktionen

AKTION	NACHSCHLAGEWERKE
Viren-/Malware-Aktion	Primäraktion (wählen Sie eine aus): • *ActiveAction verwenden auf Seite 7-43* • *Gleiche Aktion für alle Arten von Viren/Malware auf Seite 7-45* • *Bestimmte Aktion für jede Art von Viren/Malware auf Seite 7-45* **Hinweis** Weitere Informationen zu den einzelnen Aktionen finden Sie unter *Viren-/Malware-Suchaktionen auf Seite 7-41*. Zusätzliche Viren-/Malware-Aktionen: • *Quarantäne-Ordner auf Seite 7-45* • *Dateien vor dem Säubern sichern auf Seite 7-48* • *Damage Cleanup Services auf Seite 7-48* • *Bei Viren-/Malware-Fund Benachrichtigung anzeigen auf Seite 7-49* • *Bei Viren-/Malware-Verdacht Benachrichtigung anzeigen auf Seite 7-49*
Spyware-/Grayware-Aktion	Primäraktion: • *Spyware-/Grayware-Suchaktionen auf Seite 7-55* Zusätzliche Spyware-/Grayware-Aktion: • *Bei Spyware-/Grayware-Fund Benachrichtigung anzeigen auf Seite 7-56*

7. Konfigurieren Sie auf der Registerkarte **Suchausschlüsse** die Verzeichnisse, Dateien und Dateitypen, die von der Suche ausgeschlossen werden sollen.

   Weitere Informationen finden Sie unter *Suchausschlüsse auf Seite 7-34*.

8. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Jetzt durchsuchen

Die sofortige Suche ("Jetzt durchsuchen") wird von Administratoren von einem Remote-Standort aus über die Webkonsole gestartet und kann für einen oder mehrere OfficeScan Agent-Endpunkte ausgeführt werden.

Sie können die Einstellungen für 'Jetzt durchsuchen' für einen oder mehrere OfficeScan Agents und Domänen bzw. für alle OfficeScan Agents, die vom Server verwaltet werden, konfigurieren und anwenden.

Einstellungen von Jetzt durchsuchen konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Sucheinstellungen** > **Einstellungen für 'Jetzt durchsuchen'**.
4. Wählen Sie die folgenden Optionen:

- **Suche nach Viren/Malware aktivieren**
- **Suche nach Spyware/Grayware aktivieren**

> **Hinweis**
>
> Bevor Sie nach Spyware/Grayware suchen können, müssen Sie die Viren-/Malware-Suche aktivieren.

5. Konfigurieren Sie auf der Registerkarte **Ziel** die folgenden Suchkriterien:
   - *Zu durchsuchende Dateien auf Seite 7-30*
   - *Sucheinstellungen auf Seite 7-31*
   - *CPU-Auslastung auf Seite 7-33*
6. Klicken Sie auf die Registerkarte **Aktion**, und konfigurieren Sie Folgendes:

TABELLE 7-9. Suchaktionen

AKTION	NACHSCHLAGEWERKE
Viren-/Malware-Aktion	Primäraktion (wählen Sie eine aus): • *ActiveAction verwenden auf Seite 7-43* • *Gleiche Aktion für alle Arten von Viren/Malware auf Seite 7-45* • *Bestimmte Aktion für jede Art von Viren/Malware auf Seite 7-45* **Hinweis** Weitere Informationen zu den einzelnen Aktionen finden Sie unter *Viren-/Malware-Suchaktionen auf Seite 7-41*. Zusätzliche Viren-/Malware-Aktionen: • *Quarantäne-Ordner auf Seite 7-45* • *Dateien vor dem Säubern sichern auf Seite 7-48* • *Damage Cleanup Services auf Seite 7-48*
Spyware-/Grayware-Aktion	Primäraktion: • *Spyware-/Grayware-Suchaktionen auf Seite 7-55*

7. Konfigurieren Sie auf der Registerkarte **Suchausschlüsse** die Verzeichnisse, Dateien und Dateitypen, die von der Suche ausgeschlossen werden sollen.

   Weitere Informationen finden Sie unter *Suchausschlüsse auf Seite 7-34*.

8. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Jetzt durchsuchen starten

Starten Sie "Jetzt durchsuchen" auf Computern, von denen Sie vermuten, dass sie infiziert sind.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der agent-Hierarchie auf das Stammsymbol ( ), um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
3. Klicken Sie auf **Aufgaben** > **Jetzt durchsuchen**.
4. Um vor der Suche die vorkonfigurierten Einstellungen von **Jetzt durchsuchen** zu ändern, klicken Sie auf **Einstellungen**.

   Das Fenster **Einstellungen für 'Jetzt durchsuchen'** wird geöffnet. Weitere Informationen finden Sie unter *Jetzt durchsuchen auf Seite 7-25*.
5. Wählen Sie in der agent-Hierarchie die agents für die Suche aus und klicken Sie dann auf **'Jetzt durchsuchen' starten**.

   Der Server sendet eine Benachrichtigung an die agents.
6. Überprüfen Sie den Benachrichtigungsstatus und ob alle agents benachrichtigt wurden.
7. Klicken Sie auf **Nicht benachrichtigte Endpunkte auswählen** und anschließend auf **'Jetzt durchsuchen' starten**, um die Benachrichtigung erneut an noch nicht benachrichtigte agents zu senden.

   Beispiel: agents (gesamt): 50

TABELLE 7-10. Agent-Szenarios ohne Benachrichtigung

AGENT-ANSICHT – AUSWAHL	BENACHRICHTIGTE AGENTS (NACH KLICKEN AUF "'JETZT DURCHSUCHEN' STARTEN")	NICHT BENACHRICHTIGTE AGENTS
Keine (alle 50 agents werden automatisch ausgewählt)	35 von 50 agents	15 agents
Manuelle Auswahl (45 von 50 agents ausgewählt)	40 von 45 agents	5 agents plus weitere 5 agents, die in der manuellen Auswahl nicht enthalten sind

8. Klicken Sie auf **Benachrichtigung beenden**, damit OfficeScan die Benachrichtigung für die derzeit benachrichtigten agents abbricht. Bereits benachrichtigte Agents, auf denen eine Suche ausgeführt wird, ignorieren diesen Befehl.

9. Klicken Sie auf **'Jetzt durchsuchen' beenden**, um agents, auf denen die Suche bereits ausgeführt wird, zum Beenden aufzufordern.

Gemeinsame Einstellungen für alle Suchtypen

Sie können für jeden Suchtyp drei verschiedene Einstellungstypen konfigurieren: Suchkriterien, Suchausschlüsse und Suchaktionen. Sie können diese Einstellungen auf einen oder mehrere agents und Domänen bzw. auf alle agents, die vom Server verwaltet werden, verteilen.

Suchkriterien

Mit den Dateiattributen wie Dateityp und Erweiterung geben Sie an, welche Dateien ein bestimmter Suchtyp durchsuchen soll. Geben Sie außerdem die Bedingungen an, die die

Suche auslösen. Sie können beispielsweise die Echtzeitsuche so konfigurieren, dass jede Datei nach dem Herunterladen auf den Endpunkt durchsucht wird.

Benutzerdefinierte Aktionen für Dateien

Wählen Sie Aktivitäten im Zusammenhang mit Dateien aus, die die Echtzeitsuche auslösen sollen. Wählen Sie dazu eine der folgenden Optionen aus:

- **Dateien durchsuchen, die erstellt/bearbeitet werden**: Durchsucht neue Dateien, die auf den Endpunkt kopiert oder erstellt wurden (z. B. nach dem Herunterladen einer Datei), oder Dateien, die geändert wurden
- **Dateien durchsuchen, die abgefragt werden**: Durchsucht Dateien, wenn sie geöffnet werden
- **Dateien durchsuchen, die erstellt/bearbeitet und gelesen werden**

Wenn z. B. die dritte Option aktiviert wird, wird eine neue Datei durchsucht, wenn sie auf den Endpunkt heruntergeladen wird. Die Datei bleibt an ihrem aktuellen Speicherort, wenn keine Sicherheitsrisiken erkannt werden. Dieselbe Datei wird durchsucht, wenn ein Benutzer die Datei öffnet und, falls der Benutzer die Datei ändert, bevor die Änderungen gespeichert werden.

Zu durchsuchende Dateien

Wählen Sie dazu eine der folgenden Optionen aus:

- **Alle durchsuchbaren Dateien**: Alle Dateien durchsuchen
- **Von IntelliScan durchsuchte Dateitypen**: Durchsucht nur Dateien, die potenziell bösartigen Code enthalten, selbst wenn dieser sich hinter einer scheinbar harmlosen Erweiterung verbirgt.

  Weitere Informationen finden Sie unter *IntelliScan auf Seite E-6*.

- **Dateien mit diesen Erweiterungen**: Durchsucht nur Dateien mit Erweiterungen, die in der Dateierweiterungsliste enthalten sind. Sie können neue Erweiterungen hinzufügen und beliebige vorhandene Erweiterungen entfernen.

Sucheinstellungen

Aktivieren Sie mindestens eine der folgenden Optionen:

- **Diskettenlaufwerk beim Herunterfahren des Systems durchsuchen**: Die Echtzeitsuche durchsucht alle Diskettenlaufwerke nach Boot-Viren, bevor der Endpunkt heruntergefahren wird. Dadurch wird verhindert, dass Viren/Malware ausgeführt werden, wenn der Benutzer den Endpunkt von der Diskette neu startet.
- **Versteckte Ordner durchsuchen**: Lässt zu, dass OfficeScan während der manuellen Suche versteckte Ordner auf dem Endpunkt erkennt und anschließend durchsucht.
- **Netzlaufwerk durchsuchen**: Durchsucht während der manuellen Suche oder der Echtzeitsuche Netzwerklaufwerke oder Ordner, die dem OfficeScan Agent-Endpunkt zugeordnet sind.
- **Bootsektor des USB-Speichergeräts nach dem Anschließen durchsuchen**: Durchsucht jedes Mal, wenn ein USB-Speichergerät angeschlossen wird, automatisch den Bootsektor des Geräts (Echtzeitsuche).
- **Alle Dateien auf Wechselspeichermedien nach dem Anschließen durchsuchen**: Durchsucht jedesmal, wenn ein USB-Speichergerät angeschlossen wird, automatisch alle Dateien auf dem Gerät (Echtzeitsuche).
- **Im Arbeitsspeicher entdeckte Malware-Varianten unter Quarantäne stellen**: Die Verhaltensüberwachung überprüft den Systemarbeitsspeicher auf verdächtige Prozesse, und die Echtzeitsuche ordnet den Prozess zu und überprüft ihn auf Malware-Bedrohungen. Falls eine Malware-Bedrohung existiert, wird der Prozess und/oder die Datei von der Echtzeitsuche unter Quarantäne gestellt.

  Hinweis

  Diese Funktion setzt voraus, dass der Unauthorized Change Prevention Service (Dienst zum Schutz vor unbefugten Änderungen) und der erweiterte Schutzdienst vom Administrator aktiviert wurden.

- **Komprimierte Dateien durchsuchen**: Lässt zu, dass OfficeScan die angegebene Anzahl an Komprimierungsebenen durchsucht und tiefere Ebenen überspringt. Darüber hinaus bereinigt und löscht OfficeScan infizierte Dateien in komprimierten Dateien. Beträgt das Maximum zum Beispiel zwei Ebenen, die zu

durchsuchende Datei enthält aber sechs Ebenen, durchsucht OfficeScan die ersten beiden Ebenen und übergeht die letzten vier. Wenn eine komprimierte Datei Sicherheitsbedrohungen enthält, säubert oder löscht OfficeScan die Datei.

Hinweis

OfficeScan behandelt Microsoft Office 2007 Dateien im Office Open XML-Format wie komprimierte Dateien. Office Open XML, das Dateiformat für Office 2007 Anwendungen, verwendet die ZIP-Komprimierungstechnologien. Um Dateien, die von diesen Anwendungen erstellt wurden, nach Viren und Malware zu durchsuchen, muss die Suche in komprimierten Dateien aktiviert werden.

- **OLE-Objekte durchsuchen**: Wenn eine Datei mehrere OLE-Ebenen (Object Linking and Embedding) enthält, durchsucht OfficeScan die angegebene Anzahl von Schichten und ignoriert die verbleibenden Schichten.

  Alle Agents, die vom Server verwaltet werden, überprüfen diese Einstellung während der manuellen Suche, Echtzeitsuche, zeitgesteuerten Suche und der Ausführung der Funktion "Jetzt durchsuchen". Jede Schicht wird nach Viren/Malware und Spyware/Grayware durchsucht.

  Beispiel:

  Sie geben zwei Schichten an. Bei der ersten Schicht handelt es sich um ein Microsoft Word-Dokument, das in eine Datei eingebettet ist, bei der zweiten Schicht um eine Microsoft Excel-Tabelle, die in ein Word-Dokument eingebettet ist. In der Tabelle befindet sich darüber hinaus eine `.exe`-Datei (dritte Schicht). OfficeScan durchsucht das Word-Dokument und die Excel-Tabelle und überspringt die `.exe`-Datei.

  - **Exploit-Code in OLE-Dateien erkennen**: Bei der Funktion 'Erkennung von ausgenutzten OLE-Schwachstellen' wird Malware heuristisch gesucht, indem in Dateien von Microsoft Office nach Exploit-Code gesucht wird.

    Hinweis

    Die angegebene Anzahl von Schichten betrifft die Optionen **OLE-Objekte durchsuchen** und **Exploit-Code erkennen**.

- **IntelliTrap aktivieren**: Erkennt und entfernt Viren/Malware in komprimierten ausführbaren Dateien. Diese Option steht nur für die Echtzeitsuche zur Verfügung.

Weitere Informationen finden Sie unter *IntelliTrap auf Seite E-7*.

- **Suche nach CVE-Schwachstellen für Dateien aktivieren, die über Internet- oder E-Mail-Kanäle heruntergeladen wurden**: Sperren Sie Prozesse, die bekannte Schwachstellen in handelsüblichen Produkten ausnutzen, indem Sie das CVE-System (Common Vulnerabilities and Exposures) verwenden. Diese Option steht nur für die Echtzeitsuche zur Verfügung.

- **Bootbereich durchsuchen**: Durchsucht während der manuellen Suche, zeitgesteuerten Suche und der Ausführung der Funktion "Jetzt durchsuchen" den Bootsektor der Festplatte nach Viren/Malware.

CPU-Auslastung

OfficeScan kann nach dem Durchsuchen einer Datei eine Pause einlegen, bevor die nächste Datei durchsucht wird. Diese Einstellung wird während der manuellen Suche, zeitgesteuerten Suche und der Funktion "Jetzt durchsuchen" verwendet.

Wählen Sie dazu eine der folgenden Optionen aus:

- **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

Wenn Sie beim Starten der Suche "Mittel" oder "Niedrig" auswählen und sich die CPU-Auslastung innerhalb der Grenzwerte befindet (50 % oder 20 %), legt OfficeScan keine Pause zwischen den Durchsuchungen ein. Dadurch wird die Suche beschleunigt. Bei diesem Vorgehen verwendet OfficeScan mehr CPU-Ressourcen, weil die CPU-Auslastung im optimalen Rahmen liegt. Dadurch wird die Endpunkt-Leistung nicht drastisch beeinträchtigt. Wenn die CPU-Auslastung den Schwellenwert überschreitet, legt OfficeScan eine Pause ein, um die CPU-Auslastung zu reduzieren. Die Pause wird beendet, sobald die Auslastung wieder innerhalb der Grenzwerte liegt.

Wenn Sie als Einstellung "Hoch" wählen, überprüft OfficeScan nicht die tatsächlichen CPU-Auslastung, und durchsucht die Dateien, ohne dabei Pausen einzulegen.

Zeitplan

Konfigurieren Sie, wie oft (täglich, wöchentlich oder monatlich) und zu welcher Zeit die zeitgesteuerte Suche ausgeführt werden soll.

Sie können angeben, ob monatliche, zeitgesteuerte Suchvorgänge an einem bestimmten Monatstag oder an einem bestimmten Wochentag im Monat stattfinden sollen.

- **Ein bestimmter Monatstag**: Wählen Sie einen Wert zwischen 1 und 31 aus. Falls Sie den 29., 30. oder 31. Tag gewählt haben, führt OfficeScan die zeitgesteuerte Suche in den Monaten, in denen es diesen Tag nicht gibt, am letzten Tag dieses Monats aus. Beispiele:
  - Falls Sie "29" ausgewählt haben, wird die zeitgesteuerte Suche am 28. Februar (falls es sich nicht um ein Schaltjahr handelt) und am 29. jedes anderen Monats ausgeführt.
  - Falls Sie "30" ausgewählt haben, wird die zeitgesteuerte Suche am 28. bzw. 29. Februar und am 30. jedes anderen Monats ausgeführt.
  - Falls Sie "31" ausgewählt haben, wird die zeitgesteuerte Suche am 28. bzw. 29. Februar, am 30. April, 30. Juni, 30. September, 30. November und am 31. jedes anderen Monats ausgeführt.
- **Ein bestimmter Wochentag im Monat**: Ein Wochentag kommt in einem Monat vier- oder fünfmal vor. Beispielsweise hat ein Monat gewöhnlich vier Montage. Geben Sie einen Wochentag und seine Reihenfolge seines Vorkommens im Monat an. Wählen Sie für die Ausführung der zeitgesteuerten Suche beispielsweise den zweiten Montag jedes Monats aus. Falls Sie das fünfte Vorkommen eines Tages ausgewählt haben, findet die zeitgesteuerte Suche in Monaten, in denen der entsprechende Wochentag nicht fünfmal vorkommt, am vierten Auftreten des Wochentags statt.

Suchausschlüsse

Sie können Suchausschlüsse definieren, um die Suchleistung zu erhöhen und Dateien zu überspringen, die Fehlalarme auslösen. Wenn ein bestimmter Suchtyp ausgeführt wird, überprüft OfficeScan die Suchausschlussliste, um zu ermitteln, welche Dateien auf dem Endpunkt von der Suche nach Viren/Malware und Spyware/Grayware ausgeschlossen sind.

Wenn Sie Suchausschlüsse aktivieren, führt OfficeScan unter den folgenden Bedingungen keine Durchsuchung der Datei durch:

- Die Datei befindet sich in einem bestimmten Verzeichnis (oder einem seiner Unterverzeichnisse).
- Der Dateiname stimmt mit einem der Namen auf der Ausschlussliste überein.
- Die Dateinamenserweiterung stimmt mit einer der Erweiterungen auf der Ausschlussliste überein.

Tipp

Eine Liste der von Trend Micro empfohlenen Produkte (mit Ausnahme von Echtzeitsuchdiensten) finden Sie unter:

http://esupport.trendmicro.com/solution/en-US/1059770.aspx

Ausnahmen mit Platzhaltern

Die Suchausschlusslisten für Dateien und Verzeichnisse unterstützen die Verwendung von Platzhalterzeichen. Verwenden Sie als Platzhalterzeichen das "?", um ein Zeichen zu ersetzen, und das "*", um mehrere Zeichen zu ersetzen.

Setzen Sie Platzhalterzeichen mit Bedacht ein. Bei der Verwendung des falschen Zeichens können Dateien und Verzeichnisse ausgeschlossen werden, die eigentlich eingeschlossen werden sollten. Beispielsweise wird durch Hinzufügen von `C:\*` zur Ausschlussliste für Virensuche (Dateien) das gesamte Laufwerk `C:\` ausgeschlossen.

TABELLE 7-11. Ausschlüsse von der Suche mit Platzhalterzeichen

WERT	AUSGESCHLOSSEN	NICHT AUSGESCHLOSSEN

`c:\director*\fil\*.txt`	`c:\directory\fil\doc.txt`
	`c:\directories\fil\files\document.txt`
		`c:\directory\file\`
		`c:\directories\files\`
		`c:\directory\file\doc.txt`
		`c:\directories\files\document.txt`

WERT	AUSGESCHLOSSEN	NICHT AUSGESCHLOSSEN
`c:\director?\file\*.txt`	`c:\directory\file\doc.txt`	`c:\directories\file\document.txt`
`c:\director?\file\?.txt`	`c:\directory\file\1.txt`	`c:\directory\file\doc.txt` `c:\directories\file\document.txt`
`c:\*.txt`	Alle `.txt`-Dateien im `C:\`-Verzeichnis	Alle anderen Dateitypen im `C:\`-Verzeichnis
`[]`	Nicht unterstützt	Nicht unterstützt

Ausschlussliste für Virensuche (Verzeichnisse)

OfficeScan durchsucht keine Dateien, die sich unterhalb eines bestimmten Verzeichnisses auf dem Computer befinden. Sie können maximal 256 Verzeichnisse angeben.

Hinweis

Durch das Ausschließen eines Verzeichnisse von der Suche schließt OfficeScan automatisch auch alle Unterverzeichnisse des Verzeichnisses von der Suche aus.

Sie können auch die Option **Verzeichnisse ausschließen, in denen Trend Micro Produkte installiert sind** wählen. Wenn Sie diese Option auswählen, schließt OfficeScan automatisch die Verzeichnisse der folgenden Trend Micro Produkte von der Suche aus:

- <*Installationsordner des Servers*>

  Hinweis

  Während einer manuellen Suche durchsucht OfficeScan weiterhin den Installationsordner des Servers.

- IM-Sicherheit

- InterScan eManager 3.5x
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall
- ScanMail eManager™ 3.11, 5.1, 5.11, 5.12
- ScanMail for Lotus Notes™ eManager NT
- ScanMail™ für Microsoft Exchange

Wenn Sie ein Produkt von Trend Micro haben, das nicht in der Liste enthalten ist, fügen Sie die Produktverzeichnisse manuell zur Ausschlussliste hinzu.

Konfigurieren Sie OfficeScan darüber hinaus so, dass Microsoft Exchange 2000/2003-Verzeichnisse ausgeschlossen werden. Navigieren Sie dazu zum Abschnitt **Sucheinstellungen** unter **Agents** > **Globale Agent-Einstellungen** auf der Registerkarte **Sicherheitseinstellungen**. Microsoft Exchange 2007 Verzeichnisse oder höher werden manuell zur Ausschlussliste hinzugefügt. Einzelheiten zu den Suchausschlüssen finden Sie auf der folgenden Website:

http://technet.microsoft.com/en-us/library/bb332342.aspx

Wenn Sie die Dateienliste konfigurieren, können Sie aus den folgenden Optionen wählen:

- **Aktuelle Liste wird beibehalten** (Standard): OfficeScan bietet diese Option an, um das versehentliche Überschreiben der vorhandenen Ausschlussliste des agents zu verhindern. Wählen Sie eine der folgenden Optionen aus, um Änderungen an der Ausschlussliste zu speichern und zu verteilen.
- **Überschreibt**: Diese Option entfernt die gesamte Ausschlussliste auf dem agent und ersetzt sie durch die aktuelle Liste. Nach dem Klicken auf **Auf alle Agents anwenden** zeigt OfficeScan eine Bestätigungswarnmeldung an.

- **Pfade werden hinzugefügt zu**: Diese Option fügt die Einträge in der aktuellen Liste zur bestehenden Ausschlussliste des agents hinzu. Sollte ein Eintrag in der Ausschlussliste des agents bereits vorhanden sein, ignoriert der agent den Eintrag.
- **Pfade werden entfernt aus**: Diese Option entfernt die Einträge in der aktuellen Liste aus der bestehenden Ausschlussliste des agents.

Unterstützte Systemvariablen für Ausschlussliste für Virensuche (Verzeichnisse)

Sie können die Ausschlussliste für die Virensuche (Verzeichnisse) über allgemeine Windows-Systemvariablen konfigurieren. Die folgende Tabelle enthält die von OfficeScan unterstützten Variablen.

SYSTEMVARIABLE	BESCHREIBUNG

%ALLUSERSPROFILE%	Bezieht sich auf den Ordner `%PROFILESFOLDER%\Public` oder `%PROFILESFOLDER%\all users`
	
	Beispiel:
	• Der Standardspeicherort von %ALLUSERSPROFILE% in Windows 7:
	`C:\ProgramData`
	• Der Standardspeicherort von %ALLUSERSPROFILE% in Windows XP:
	`C:\Dokumente und Einstellungen\Alle Benutzer`

%COMMONPROGRAMFILES%	Bezieht sich auf den Ordner, der die Komponenten enthält, auf die von Anwendungen gemeinsam zugegriffen wird. Ein typischer Pfad ist `C:\Programme\Common`. **Hinweis** Gilt nur für Endpunkte unter Windows NT, Windows 2000 und Windows XP.

SYSTEMVARIABLE	BESCHREIBUNG
%COMMONPROGRAMFILES(X86)%	Bezieht sich auf den Ordner `C:\Programme (x86)\Common Files` auf 64-Bit-Systemen.
%PROGRAMFILES%	Der Ordner "Programme" Ein typischer Pfad ist `C:\Programme`
%PROGRAMFILES(X86)%	Bezieht sich auf den Ordner `C:\Programme (x86)` auf 64-Bit-Systemen.
%SYSTEMROOT%	Bezieht sich auf den Root-Ordner des Systemlaufwerks. Ein typischer Pfad ist `C:\Windows`
%WINDIR%	Bezieht sich auf den Windows-Ordner auf dem Systemlaufwerk. Ein typischer Pfad ist `C:\Windows`

Ausschlussliste für Virensuche (Dateien)

OfficeScan führt keine Durchsuchung einer Datei durch, wenn der Dateiname einem der Namen in dieser Ausschlussliste entspricht. Wenn Sie eine Datei ausschließen möchten, die sich an einem bestimmten Speicherort auf dem Endpunkt befindet, geben Sie den Dateipfad an, z. B. `C:\Temp\sample.jpg`.

Sie können maximal 256 Dateien angeben.

Wenn Sie die Dateienliste konfigurieren, können Sie aus den folgenden Optionen wählen:

- **Aktuelle Liste wird beibehalten** (Standard): OfficeScan bietet diese Option an, um das versehentliche Überschreiben der vorhandenen Ausschlussliste des agents zu verhindern. Wählen Sie eine der folgenden Optionen aus, um Änderungen an der Ausschlussliste zu speichern und zu verteilen.
- **Überschreibt**: Diese Option entfernt die gesamte Ausschlussliste auf dem agent und ersetzt sie durch die aktuelle Liste. Nach dem Klicken auf **Auf alle Agents anwenden** zeigt OfficeScan eine Bestätigungswarnmeldung an.

- **Pfade werden hinzugefügt zu**: Diese Option fügt die Einträge in der aktuellen Liste zur bestehenden Ausschlussliste des agents hinzu. Sollte ein Eintrag in der Ausschlussliste des agents bereits vorhanden sein, ignoriert der agent den Eintrag.
- **Pfade werden entfernt aus**: Diese Option entfernt die Einträge in der aktuellen Liste aus der bestehenden Ausschlussliste des agents.

Ausschlussliste für Virensuche (Dateierweiterungen)

OfficeScan führt keine Durchsuchung einer Datei durch, wenn die Dateinamenerweiterung einer der Erweiterungen in dieser Ausschlussliste entspricht. Es können maximal 256 Dateierweiterungen angegeben werden. Ein Punkt (.) ist bei der Angabe der Dateierweiterung nicht erforderlich.

Verwenden Sie bei der manuellen Suche, der zeitgesteuerten Suche und der sofortigen Suche ("Jetzt durchsuchen") als Platzhalter ein Fragezeichen (?), um ein einzelnes Zeichen zu ersetzen, oder ein Sternchen (*), um mehrere Zeichen zu ersetzen. Wenn Sie beispielsweise nicht alle Dateien durchsuchen möchten, deren Erweiterung mit "D" beginnt, wie z. B. `DOC`, `DOT` oder `DAT`, geben Sie `D*` oder `D?` ein.

Hinweis

Die Echtzeitsuche bietet keine Unterstützung für die Verwendung von Platzhalterzeichen bei der Angabe von Erweiterungen.

Einstellungen für den Suchausschluss auf alle Suchtypen anwenden

Mit OfficeScan können Sie die Einstellungen für Suchausschlüsse für einen bestimmten Suchtyp konfigurieren und anschließend dieselben Einstellungen auf alle anderen Suchtypen übernehmen. Beispiel:

Am 1. Januar stellte der OfficeScan Administrator Chris fest, dass sich auf den agent-Computern viele `JPG`-Dateien befinden und diese Dateien kein Sicherheitsrisiko darstellen. Chris fügte `JPG` der Dateiausschlussliste für die manuelle Suche hinzu und übernahm diese Einstellung auf alle Suchtypen. Echtzeitsuche, "Jetzt durchsuchen" und zeitgesteuerte Suche sind nun so konfiguriert, dass `.jpg`-Dateien übersprungen werden.

Eine Woche ypäter entfernte Chris `JPG` von der Ausschlussliste für die Echtzeitsuche, jedoch übernahm er die Suchausschlusseinstellungen nicht auf alle Suchtypen. `JPG`-Dateien werden nun durchsucht, jedoch nur während der Echtzeitsuche.

Suchaktionen

Geben Sie die Aktion an, die OfficeScan durchführt, wenn ein bestimmter Suchtyp ein Sicherheitsrisiko erkennt. OfficeScan verwendet bei der Suche nach Viren/Malware und nach Spyware/Grayware jeweils unterschiedliche Suchaktionen.

Viren-/Malware-Suchaktionen

Die von OfficeScan durchgeführte Suchaktion hängt vom Viren-/Malware-Typ und dem Suchtyp ab, der den Virus bzw. die Malware entdeckt hat. Sobald OfficeScan beispielsweise bei der manuellen Suche (Suchtyp) einen Trojaner (Viren-/Malware-Typ) entdeckt, wird diese infizierte Datei gesäubert (Aktion).

Informationen über die verschiedenen Viren-/Malware-Typen finden Sie unter *Viren und Malware auf Seite 7-2*.

Im Folgenden handelt es sich um Aktionen, die OfficeScan für Viren/Malware durchführen kann:

TABELLE 7-12. Viren-/Malware-Suchaktionen

AKTION	BESCHREIBUNG
Löschen	OfficeScan löscht die infizierte Datei.

AKTION	BESCHREIBUNG
Quarantäne	OfficeScan benennt die infizierte Datei um, verschlüsselt und verschiebt sie in ein temporäres Quarantäneverzeichnis im Agent-Endpunkt, der sich in <*Installationsordner des Agents*>`\Suspect` befindet. Der OfficeScan Agent sendet anschließend die Dateien in Quarantäne an den vorgesehenen Quarantäne-Ordner. Weitere Informationen finden Sie unter *Quarantäne-Ordner auf Seite 7-45*. Das Standard-Quarantäneverzeichnis befindet sich auf dem OfficeScan-Server unter <*Installationsordner des Servers*>`\PCCSRV\Virus`. Mit der "Zentralen Quarantänewiederherstellung" können Sie beliebige Dateien in der Quarantäne wiederherstellen. Weitere Informationen finden Sie unter *Dateien in der Quarantäne wiederherstellen auf Seite 7-50*.
Säubern	OfficeScan säubert die infizierte Datei, bevor es den vollständigen Zugriff erlaubt. Lässt sich die Datei nicht säubern, führt OfficeScan zusätzlich eine der folgenden Aktionen durch: Quarantäne, Löschen, Umbenennen und Übergehen. Um die zweite Aktion zu konfigurieren, wechseln Sie zu **Agents** > **Agent-Verwaltung**. Klicken Sie auf die Registerkarte **Einstellungen** > **Sucheinstellungen** > **{Suchtyp}** > **Aktion**. Diese Aktion kann auf alle Arten von Malware angewendet werden, außer wahrscheinliche Viren/Malware.
Umbenennen	OfficeScan ändert die Erweiterung der infizierten Datei in "`vir`". 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	OfficeScan kann diese Suchaktion nur dann durchführen, wenn bei der manuellen Suche, der zeitgesteuerten Suche und der Funktion "Jetzt durchsuchen" ein Virus entdeckt wird. OfficeScan kann diese Suchaktion während der Echtzeitsuche nicht verwenden. Beim Versuch, eine infizierte Datei zu öffnen oder auszuführen, könnte bei fehlender Suchaktion der Virus oder die Malware ausgeführt werden. Alle anderen Suchaktionen können bei der Echtzeitsuche verwendet werden.
Zugriff verweigern	Diese Suchaktion kann nur bei der Echtzeitsuche durchgeführt werden. Entdeckt OfficeScan einen Versuch, eine inifizierte Datei zu öffnen oder auszuführen, wird dieser Vorgang umgehend gesperrt. Die infizierte Datei kann manuell gelöscht werden.

ActiveAction verwenden

Unterschiedliche Viren-/Malware-Typen erfordern unterschiedliche Suchaktionen. Unterschiedliche Suchaktionen benutzerdefiniert festzulegen, setzt jedoch grundlegendes Wissen über Viren/Malware voraus und kann äußerst zeitaufwändig sein. OfficeScan verwendet ActiveAction, um diesem Problem entgegenzuwirken.

In ActiveAction sind mehrere bereits vorkonfigurierte Aktionen für die Suche nach Viren/Malware zusammengefasst. Trend Micro empfiehlt die Verwendung von ActiveAction, wenn Sie mit 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 ändern sich permanent. Die ActiveAction Einstellungen werden aktualisiert, um vor den neuesten Bedrohungen und Methoden von Viren-/Malware-Angriffen zu schützen.

Hinweis

ActiveAction ist nicht für die Suche nach Spyware/Grayware verfügbar.

Die folgende Tabelle zeigt, wie ActiveAction mit den jeweiligen Viren-/Malware-Typen verfährt:

TABELLE 7-13. Von Trend Micro empfohlene Suchaktionen gegen Viren und Malware

VIREN-/ MALWARE-TYP	ECHTZEITSUCHE		MANUELLE SUCHE/ ZEITGESTEUERTE SUCHE/ JETZT DURCHSUCHEN	
	ERSTE AKTION	ZWEITE AKTION	ERSTE AKTION	ZWEITE AKTION
CVE-Schwachstelle	Zugriff verweigern	n. v.	n. z.	n. z.
Scherzprogramm	Quarantäne	n. v.	Quarantäne	n. v.
Trojaner	Quarantäne	n. v.	Quarantäne	n. v.
Virus	Säubern	Quarantäne	Säubern	Quarantäne
Testvirus	Zugriff verweigern	n. v.	Übergehen	n. v.
Packer	Quarantäne	n. v.	Quarantäne	n. v.
Mögliche Malware	Zugriff verweigern oder vom Benutzer konfigurierte Aktion	n. z.	Übergehen oder vom Benutzer konfigurierte Aktion	n. z.
Andere Malware	Säubern	Quarantäne	Säubern	Quarantäne

Als Standardaktion bei einem Verdacht auf Malware wird während der Echtzeitsuche die Option "Zugriff verweigern" verwendet. Während einer manuellen Suche, einer zeitgesteuerten Suche und bei Verwendung der Funktion "Jetzt durchsuchen" wird die Option "Übergehen" ausgewählt. Sind das nicht Ihre bevorzugten Aktionen, können Sie sie ändern in Quarantäne, Löschen oder Umbenennen.

Gleiche Aktion für alle Arten von Viren/Malware

Wählen Sie diese Option, wenn dieselbe Aktion auf alle Viren-/Malware-Typen ausgeführt werden soll, außer bei Viren-/Malware-Verdacht. Wenn Sie "Säubern" als erste Aktion auswählen, wählen Sie eine zweite Aktion, die OfficeScan ausführt, wenn die Säuberung nicht erfolgreich verläuft. Wenn es sich bei der ersten Aktion nicht um "Säubern" handelt, kann keine zweite Aktion konfiguriert werden.

Wenn Sie als erste Aktion "Säubern" wählen, führt OfficeScan die zweite Aktion durch, wenn mögliche Viren/Malware entdeckt werden.

Bestimmte Aktion für jede Art von Viren/Malware

Wählen Sie manuell eine Suchaktion für jeden Viren-/Malware-Typ aus.

Für alle Arten von Viren/Malware sind alle Suchaktionen verfügbar, außer für mögliche Viren/Malware. Wenn Sie "Säubern" als erste Aktion auswählen, wählen Sie eine zweite Aktion, die OfficeScan ausführt, wenn die Säuberung nicht erfolgreich verläuft. Wenn es sich bei der ersten Aktion nicht um "Säubern" handelt, kann keine zweite Aktion konfiguriert werden.

Für mögliche Viren/Malware sind alle Suchaktionen außer "Säubern" verfügbar.

Quarantäne-Ordner

Wenn es sich bei der Aktion für eine infizierte Datei um "Quarantäne" handelt, wird die Datei vom OfficeScan Agent verschlüsselt und in den temporären Quarantäne-Ordner verschoben, der sich im Ordner <*Installationsordner des Agents*>\SUSPECT befindet. Anschließend wird die Datei in den vorgesehenen Quarantäne-Ordner verschoben.

Hinweis

Sie können die verschlüsselten Dateien in der Quarantäne wiederherstellen, falls Sie zu einem späteren Zeitpunkt darauf zugreifen möchten.

Weitere Informationen finden Sie unter *Verschlüsselte Dateien wiederherstellen auf Seite 7-51*.

Übernehmen Sie den Quarantäne-Ordner, der sich standardmäßig auf dem OfficeScan Server-Computer befindet. Das Verzeichnis ist im URL-Format angegeben und enthält den Hostnamen oder die IP-Adresse des Servers.

- Verwaltet der Server sowohl IPv4- als auch IPv6-Agents verwenden Sie den Hostnamen, damit alle OfficeScan Agents in Quarantäne verschobene Dateien an den Server senden können.
- Hat der Server nur eine IPv4-Adresse oder wird über sie identifiziert, können nur reine IPv4- und Dual-Stack-OfficeScan Agents Quarantäne-Dateien an den Server senden.
- Hat der Server nur eine IPv6-Adresse oder wird über sie identifiziert, können nur reine IPv6- und Dual-Stack-OfficeScan Agents Quarantäne-Dateien an den Server senden.

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

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

TABELLE 7-14. Quarantäne-Ordner

QUARANTÄNE-ORDNER	KOMPATIBLES FORMAT	BEISPIEL	HINWEISE
Ein Verzeichnis auf dem Verwaltungsserver-Computer	URL	`http://<osceserver>`	Dabei handelt es sich um das Standardverzeichnis. Sie können die Einstellungen für dieses Verzeichnis konfigurieren, z. B. die Größe des Quarantäne-Ordners. Weitere Informationen finden Sie unter *Quarantäne-Manager auf Seite 14-70*.
	UNC-Pfad	`\\<osceserver>\ofcscan\Virus`	
Ein Verzeichnis auf einem anderen OfficeScan Server-Computer (falls sich in Ihrem Netzwerk andere OfficeScan Server befinden)	URL	`http://<osceserver2>`	Vergewissern Sie sich, dass OfficeScan Agents eine Verbindung zu diesem Verzeichnis aufbauen können. Bei Angabe eines ungültigen Verzeichnisses behält der OfficeScan Agent die unter Quarantäne gestellten Dateien im Ordner "SUSPECT", 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	`\\<osceserver2>\ofcscan\Virus`	
Ein anderer Endpunkt im Netzwerk	UNC-Pfad	`\\<computer_name>\temp`	
Ein anderes Verzeichnis auf dem OfficeScan Agent	Absoluter Pfad	`C:\temp`	

Dateien vor dem Säubern sichern

Wenn OfficeScan so konfiguriert ist, dass eine infizierte Datei gesäubert werden soll, kann zunächst eine Datensicherung der Datei erstellt werden. Auf diese Weise können Sie die Datei wiederherstellen, falls Sie sie zu einem späteren Zeitpunkt benötigen. OfficeScan verschlüsselt die Sicherungsdatei, um zu verhindern, dass sie geöffnet werden kann, und sichert die Datei anschließend im Ordner <*Installationsordner des Agents*>`\Backup`.

Informationen zur Wiederherstellung verschlüsselter Sicherungsdateien finden Sie unter *Verschlüsselte Dateien wiederherstellen auf Seite 7-51*.

Damage Cleanup Services

Damage Cleanup Services beseitigt dateibasierte und Netzwerkviren sowie Überreste von Viren und Würmern (Trojanern, Registrierungseinträgen, Virendateien) auf Computern.

Je nach Suchtyp löst der agent Damage Cleanup Services vor oder nach der Viren-/Malware-Suche aus.

- Während einer manuellen Suche, einer zeitgesteuerten Suche oder der Funktion "Jetzt durchsuchen" löst der OfficeScan Agent die Damage Cleanup Services zuerst aus und fährt anschließend mit der Viren-/Malware-Suche fort. Während der Viren-/Malware-Suche löst der agent möglicherweise Damage Cleanup Services nochmals aus, wenn eine Säuberung erforderlich sein sollte.
- Bei der Echtzeitsuche führt der OfficeScan Agent zuerst die Viren-/Malware-Suche durch und löst im Anschluss daran die Damage Cleanup Services aus, falls eine Säuberung erforderlich sein sollte.

Sie können den Cleanup-Typ auswählen, den Damage Cleanup Services durchführt:

- **Standardsäuberung**: Während einer Standardsäuberung führt der OfficeScan Agent die folgenden Aktionen durch:
  - Entdeckt und entfernt aktive Trojaner
  - Beendet durch Trojaner ausgelöste Prozesse

- Repariert von Trojanern geänderte Systemdateien
- Löscht von Trojanern hinterlassene Dateien und Anwendungen

- **Erweiterte Säuberung**: Zusätzlich zu den durchgeführten Standardsäuberungsaktionen beendet der OfficeScan Agent Aktivitäten, die von einer bösartigen Sicherheitssoftware (auch als FakeAV bekannt) und bestimmten Rootkit-Varianten ausgeführt werden. Der OfficeScan Agent setzt ebenfalls Regeln für die erweiterte Säuberung zur proaktiven Erkennung und zum Beenden von Anwendungen ein, die ein FakeAV- und Rootkit-Verhalten zeigen.

Hinweis

Das erweiterte Cleanup bietet zwar proaktiven Schutz, löst aber auch viele Fehlalarme aus.

Damage Cleanup Services führt kein Cleanup bei Viren-/Malware-Verdacht durch, außer Sie wählen die Option **Cleanup bei Viren-/Malware-Verdacht durchführen**. Sie können diese Option nur auswählen, wenn die Aktion bei Viren-/Malware-Verdacht nicht **Übergehen** oder **Zugriff verweigern** ist. Wenn der OfficeScan Agent beispielsweise mögliche Viren/Malware während der Echtzeitsuche entdeckt und die Aktion Quarantäne gewählt wurde, verschiebt der OfficeScan Agent die infizierte Datei zuerst in den Quarantäne-Ordner und führt dann das erforderliche Cleanup durch. Die Wahl des entsprechenden Cleanup-Typs (Standard oder erweitert) ist Ihnen überlassen.

Bei Viren-/Malware-Fund Benachrichtigung anzeigen

Wenn OfficeScan während der Echtzeitsuche und zeitgesteuerten Suche Viren/Malware erkennt, kann eine Benachrichtigung angezeigt werden, die den Benutzer über die Löschung informiert.

Wählen Sie zum Ändern der Benachrichtigung **Virus/Malware** aus dem Dropdown-Menü **Typ** unter **Administration** > **Benachrichtigungen** > **Agent**.

Bei Viren-/Malware-Verdacht Benachrichtigung anzeigen

Wenn OfficeScan während der Echtzeitsuche und zeitgesteuerten Suche mögliche Viren/Malware erkennt, kann eine Benachrichtigung angezeigt werden, die den Benutzer über die Löschung informiert.

Wählen Sie zum Ändern der Benachrichtigung **Virus/Malware** aus dem Dropdown-Menü **Typ** unter **Administration** > **Benachrichtigungen** > **Agent**.

Dateien in der Quarantäne wiederherstellen

Sie können Dateien wiederherstellen, die von OfficeScan unter Quarantäne gestellt wurden, wenn Sie der Meinung sind, dass sie zu unrecht als verdächtig eingestuft wurden. Mit der Funktion "Zentrale Quarantänewiederherstellung" können Sie nach Dateien im Quarantäne-Ordner suchen und die SHA1-Überprüfung durchführen, um sicherzustellen, dass die wiederherzustellenden Dateien nicht auf irgendeine Weise geändert wurden.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Wählen Sie in der Agent-Hierarchie eine Domäne oder einen Agent aus.
3. Klicken Sie auf **Aufgaben** > **Zentrale Quarantänewiederherstellung**.

   Das Fenster **Kriterien der zentralen Quarantänewiederherstellung** wird angezeigt.
4. Geben Sie den Namen der Datei, die Sie wiederherstellen möchten, in das Feld **Infizierte(s) Datei/Objekt** ein.
5. Geben Sie optional den Zeitraum, den Namen der Sicherheitsbedrohung und den Dateipfad der Daten an.
6. Klicken Sie auf **Suchen**.

   Das Fenster **Zentrale Quarantänewiederherstellung** wird mit den Suchergebnissen angezeigt.
7. Wählen Sie **Wiederhergestellte Datei zur Ausschlussliste auf Domänenebene hinzufügen** aus, um sicherzustellen, dass alle OfficeScan Agents in den Domänen, in denen die Dateien wiederhergestellt werden, die Datei zur Ausschlussliste für die Virensuche hinzufügen.

   Dadurch wird sichergestellt, dass OfficeScan die Datei bei künftigen Suchvorgängen nicht als Bedrohung einstuft.

8. Geben Sie optional den SHA-1-Wert der Datei zur Überprüfung ein.

9. Wählen Sie die Dateien, die wiederhergestellt werden sollen, aus der Liste aus, und klicken Sie auf **Wiederherstellen**.

Tipp

Um die einzelnen OfficeScan Agents anzuzeigen, die die Datei wiederherstellen, klicken Sie auf den Link in der Spalte **Endpunkte**.

10. Klicken Sie in dem Bestätigungsdialogfeld auf **Schließen**.

Weitere Informationen zum Überprüfen, ob die verdächtige Datei in Quarantäne von OfficeScan wiederhergestellt wurde, finden Sie unter *Protokolle der zentralen Quarantänewiederherstellung anzeigen auf Seite 7-109*.

Verschlüsselte Dateien wiederherstellen

Um zu verhindern, dass infizierte Dateien geöffnet werden, wird die betreffende Datei während der folgenden Aktionen von OfficeScan verschlüsselt:

- Bevor eine Datei in Quarantäne verschoben wird
- Wenn vor der Säuberung eine Sicherheitskopie der Datei angefertigt wird

OfficeScan enthält ein Tool zum Entschlüsseln und anschließendem Wiederherstellen der Datei, falls Sie Informationen von der Datei abrufen müssen. OfficeScan kann die folgenden Dateien entschlüsseln und wiederherstellen:

TABELLE 7-15. Dateien, die OfficeScan entschlüsseln und wiederherstellen kann

DATEI	BESCHREIBUNG
Dateien in der Quarantäne auf dem agent Endpunkt	Diese Dateien befinden sich im Ordner <*Installationsordner des Agents*>`\SUSPECT\Backup`, und sie werden automatisch nach 7 Tagen gelöscht. Diese Dateien werden darüber hinaus in den vorgesehenen Quarantäne-Ordner auf dem OfficeScan Server hochgeladen.

DATEI	BESCHREIBUNG
Dateien in der Quarantäne im vorgesehenen Quarantäne-Ordner	Dieses Verzeichnis befindet sich standardmäßig auf dem OfficeScan Server-Computer. Weitere Informationen finden Sie unter *Quarantäne-Ordner auf Seite 7-45*.
Gesicherte verschlüsselte Dateien	Dabei handelt es sich um Sicherheitskopien der infizierten Dateien, die OfficeScan säubern konnte. Diese Dateien befinden sich im Ordner `<Installationsordner des Agents>\Backup`. Um diese Dateien wiederherzustellen, müssen Sie sie in den Ordner `<Installationsordner des Agents>\SUSPECT\Backup` verschieben. OfficeScan erstellt nur Sicherungskopien und verschlüsselt Dateien vor dem Säubern, wenn Sie die Option **Vor dem Säubern Sicherungskopie erstellen** aktiviert haben. Navigieren Sie hierzu zu **Agents** > **Agent-Verwaltung** und klicken Sie auf **Einstellungen** > **Sucheinstellungen** > **{Suchtyp}** > **Aktion**.

Warnung!

Durch das Wiederherstellen einer infizierten Datei könnte sich der Virus/die Malware auf andere Dateien und Computer übertragen. Bevor Sie die Datei wiederherstellen, isolieren Sie den infizierten Endpunkt, und erstellen Sie Sicherheitskopien wichtiger Dateien auf diesem Endpunkt.

Dateien entschlüsseln und wiederherstellen

Prozedur

- Wenn sich die Datei auf dem OfficeScan Agent-Endpunkt befindet:

  a. Öffnen Sie die Eingabeaufforderung, und navigieren Sie zum Ordner <*Installationsordner des Agents*>.

  b. Führen Sie `VSEncode.exe` aus, indem Sie auf die Datei doppelklicken oder indem Sie an der Eingabeaufforderung Folgendes eingeben:

  ```
  VSEncode.exe /u
  ```

Dieser Parameter öffnet ein Fenster mit einer Liste der Dateien im Ordner `<Installationsordner des Agents>\SUSPECT\Backup`.

c. Wählen Sie die Datei, die wiederhergestellt werden soll, und klicken Sie auf **Wiederherstellen**. Mit dem Tool können Sie jeweils nur eine Datei wiederherstellen.

d. Geben Sie im daraufhin angezeigten Fenster den Ordners an, in dem die Datei wiederhergestellt werden soll.

e. Klicken Sie auf **Ok**. Die Datei wird im angegebenen Ordner wiederhergestellt.

Hinweis

Unter Umständen kann OfficeScan 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 *Suchausschlüsse auf Seite 7-34*.

f. Klicken Sie auf **Schließen**, wenn Sie alle Dateien wiederhergestellt haben.

- Wenn sich die Datei auf dem OfficeScan Server oder in einem benutzerdefinierten Quarantäne-Ordner befindet:

  a. Wenn sich die Datei auf dem OfficeScan Server-Computer befindet, öffnen Sie die Eingabeaufforderung, und navigieren Sie zum Ordner <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\VSEncrypt`.

  Wenn sich die Datei in einem benutzerdefinierten Quarantäne-Ordner befindet, navigieren Sie zum Ordner `<Installationsordner des Servers>\PCCSRV\Admin\Utility`, und kopieren Sie den Ordner `VSEncrypt` auf den Endpunkt, auf dem sich das benutzerdefinierte Quarantäne-Verzeichnis befindet.

  b. Erstellen Sie eine Textdatei. Geben Sie anschließend den vollständigen Pfad zu den Dateien ein, die Sie ver- bzw. entschlüsseln möchten.

  Um beispielsweise Dateien im Verzeichnis `C:\Eigene Dateien\Reports wiederherzustellen, geben Sie C:\Eigene Dateien\Reports \*.*` in die Textdatei ein.

Auf dem OfficeScan Server-Computer befinden sich die Dateien in der Quarantäne unter `<Installationsordner des Servers>\PCCSRV\Virus`.

c. Speichern Sie die Textdatei mit der Erweiterung `INI` oder `TXT`. Speichern Sie sie beispielsweise unter `ZurVerschluesselung.ini` auf Laufwerk `C:`.

d. Öffnen Sie die Eingabeaufforderung, und navigieren Sie zum Verzeichnis, in dem sich der Ordner `VSEncrypt` befindet.

e. 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-Datei>` ist der Pfad der von Ihnen erstellten `INI`- oder `TXT`-Datei (z. B. `C:\ForEncryption.ini`).

f. Verwenden Sie die anderen Parameter, um verschiedene Befehle auszuführen.

TABELLE 7-16. 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 Endpunkt. Auf dem OfficeScan Agent-Endpunkt wird das Debug-Protokoll `VSEncrypt.log` im Ordner `<Installationsordner des Agents>` 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

PARAMETER	BESCHREIBUNG
/u	Startet die Benutzeroberfläche des Tools
/r <Zielordner>	Der Ordner, in dem eine Datei wiederhergestellt wird
/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 OfficeScan die ent- oder verschlüsselte Datei im selben Ordner. Vergewissern Sie sich, bevor Sie eine Datei entschlüsseln oder verschlüsseln, dass diese nicht gesperrt ist.

Spyware-/Grayware-Suchaktionen

Die von OfficeScan durchgeführte Suchaktion hängt vom Suchtyp ab, der die Spyware/Grayware entdeckt. Während bestimmte Aktionen für jeden Viren-/Malware-Typ konfiguriert werden können, kann nur eine Aktion für alle Typen von Spyware/Grayware konfiguriert werden. Sobald OfficeScan beispielsweise bei der manuellen Suche (Suchtyp) Spyware/Grayware entdeckt, werden die betroffenen Systemressourcen gesäubert (Aktion).

Informationen zu den verschiedenen Arten von Spyware/Grayware finden Sie unter *Spyware und Grayware auf Seite 7-5*.

Hinweis

Die Spyware-/Grayware-Suchaktionen können nur über die Webkonsole konfiguriert werden. Die OfficeScan Agent-Konsole bietet keinen Zugriff auf diese Einstellungen.

Beim Folgenden handelt es sich um Aktionen, die OfficeScan für Spyware/Grayware durchführen kann:

TABELLE 7-17. Spyware-/Grayware-Suchaktionen

AKTION	BESCHREIBUNG
Säubern	OfficeScan beendet Prozesse oder löscht Registrierungseinträge, Dateien, Cookies und Verknüpfungen. Nach dem Säubern von Spyware/Grayware sichern die OfficeScan Agents Spyware-/Grayware-Daten, die Sie wiederherstellen können, wenn Sie den Zugriff auf die entsprechende Spyware/Grayware für sicher halten. Weitere Informationen finden Sie unter *Spyware/Grayware wiederherstellen auf Seite 7-59*.
Übergehen	OfficeScan führt keine Aktion durch, speichert aber den Spyware-/Grayware-Fund in den Protokollen. Diese Aktion kann nur während der manuellen Suche, der zeitgesteuerten Suche und der Funktion "Jetzt durchsuchen" durchgeführt werden . Während der Echtzeitsuche wird die Aktion "Zugriff verweigern" ausgeführt. OfficeScan führt keine Aktion aus, wenn sich die erkannte Spyware/Grayware auf der Liste der zulässigen Software befindet. Weitere Informationen finden Sie unter *Liste der zugelassenen Spyware/Grayware auf Seite 7-57*.
Zugriff verweigern	OfficeScan verweigert den Zugriff (Kopieren, Öffnen) auf die entdeckten Spyware-/Grayware-Komponenten. Diese Aktion kann nur bei der Echtzeitsuche durchgeführt werden. Während der manuellen Suche, der zeitgesteuerten Suche und der Funktion "Jetzt durchsuchen" wird die Aktion "Übergehen" ausgeführt.

Bei Spyware-/Grayware-Fund Benachrichtigung anzeigen

Wenn OfficeScan während der Echtzeitsuche und der zeitgesteuerten Suche Spyware/Grayware erkennt, kann eine Benachrichtigung angezeigt werden, die den Benutzer über die Löschung informiert.

Um die Benachrichtigung zu ändern, wählen Sie **Spyware/Grayware** im Listenfeld **Typ** unter **Administration** > **Benachrichtigungen** > **Agent**.

Liste der zugelassenen Spyware/Grayware

Der OfficeScan Agent stellt eine Liste der "zulässigen" Spyware/Grayware bereit, die Dateien oder Anwendungen enthält, die nicht als Spyware oder Grayware behandelt werden sollen. Wenn während der Suche eine bestimmte Spyware/Grayware erkannt wird, überprüft der OfficeScan Agent die Liste der zulässigen Software und führt bei einer Übereinstimmung keine Aktion aus.

Sie können die Liste der zulässigen Software auf einen oder mehrere OfficeScan Agents und Domänen bzw. auf alle OfficeScan Agents, die vom Server verwaltet werden, verteilen. Die Liste der zulässigen Software gilt für alle Suchtypen, d. h. dieselbe Liste der zulässigen Software wird während der manuellen Suche, der Echtzeitsuche, der zeitgesteuerten Suche und der Funktion "Jetzt durchsuchen" verwendet.

Bereits entdeckte Spyware/Grayware zur Liste Zugelassen hinzufügen

Prozedur

1. Navigieren Sie zu einer der folgenden Optionen:
   - **Agents** > **Agent-Verwaltung**
   - **Protokolle** > **Agents** > **Sicherheitsrisiken**
2. Klicken Sie in der agent-Hierarchie auf das Stammsymbol ( ), um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
3. Klicken Sie auf **Protokolle** > **Spyware-/Grayware-Protokolle** oder **Protokolle anzeigen** > **Spyware-/Grayware-Protokolle**.
4. Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.
5. Wählen Sie Protokolle aus und klicken Sie auf **Zur Liste der zulässigen Programme hinzufügen**.
6. Wenden Sie die zulässige Spyware/Grayware nur auf ausgewählten agent-Computern oder bestimmten Domänen an.

7. Klicken Sie auf **Speichern**. Die ausgewählten agents übernehmen die Einstellung und der OfficeScan Server fügt die Spyware/Grayware der Liste der zulässigen Software hinzu, die sich unter **Agents** > **Agent-Verwaltung > Einstellungen** > **Liste der zugelassenen Spyware/Grayware** befindet.

Hinweis

Die OfficeScan Liste der zugelassenen Spyware/Grayware kann maximal 1024 Einträge enthalten.

Die Liste der zugelassenen Spyware/Grayware verwalten

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Liste der zugelassenen Spyware/Grayware**.
4. Wählen Sie aus der Tabelle **Name der Spyware/Grayware** einen Namen aus. Um mehrere Namen auszuwählen, halten Sie die Strg-Taste bei der Auswahl gedrückt.
   - Sie können auch ein Schlüsselwort in das Feld **Suchen** eingeben und auf **Suchen** klicken. Die Tabelle wird mit den Namen aktualisiert, die dem Schlüsselwort entsprechen.
5. Klicken Sie auf **Hinzufügen**.

   Die Namen werden in die Tabelle **Liste 'Zulässig'** verschoben.
6. Wählen Sie die Namen aus, und klicken Sie auf **Entfernen**, um die Namen aus der Liste zu löschen. Um mehrere Namen auszuwählen, halten Sie die Strg-Taste bei der Auswahl gedrückt.
7. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

- **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Spyware/Grayware wiederherstellen

Nach dem Säubern von Spyware/Grayware sichern die OfficeScan Agents die Spyware-/Grayware-Daten. Benachrichtigen Sie einen Online-agent, die gesicherten Daten wiederherzustellen, wenn Sie die Daten als harmlos einstufen. Wählen Sie die wiederherzustellenden Spyware-/Grayware-Daten nach dem Sicherungszeitpunkt aus.

Hinweis

OfficeScan Agent Benutzer können die Wiederherstellung von Spyware/Grayware nicht einleiten und erhalten keine Benachrichtigung darüber, welche Backup-Daten der agent wiederherstellen konnte.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Öffnen Sie in der agent-Hierarchie eine Domäne, und wählen Sie einen agent aus.

   Hinweis

   Die Spyware-/Grayware-Wiederherstellung kann immer nur für einen agent ausgeführt werden.

3. Klicken Sie auf **Aufgaben** > **Spyware/Grayware wiederherstellen**.
4. Um die jeweils wiederherzustellenden Elemente anzuzeigen, klicken Sie auf **Anzeigen**.

Ein neues Fenster wird geöffnet. Klicken Sie auf **Zurück**, um zum vorherigen Fenster zurückzukehren.

5. Wählen Sie die wiederherzustellenden Datensegmente aus.

6. Klicken Sie auf **Wiederherstellen**.

   OfficeScan informiert Sie über den Wiederherstellungsstatus. Den vollständigen Bericht finden Sie in den Spyware- und Grayware-Wiederherstellungsprotokollen. Weitere Informationen finden Sie unter *Spyware-/Grayware-Wiederherstellungsprotokolle anzeigen auf Seite 7-114*.

Liste der vertrauenswürdigen Programme

Sie können OfficeScan Agents so konfigurieren, dass die Suche für vertrauenswürdige Prozesse bei der Echtzeitsuche und der Verhaltensüberwachung übersprungen werden. Nach dem Hinzufügen eines Programms zur Liste der vertrauenswürdigen Programme führt der OfficeScan Agent keine Echtzeitsuche für das Programm oder für vom Programm ausgeführte Prozesse aus. Fügen Sie vertrauenswürdige Programme zur Liste der vertrauenswürdigen Programme hinzu, um die Suchleistung auf Endpunkten zu verbessern.

Hinweis

Sie können Dateien zur Liste der vertrauenswürdigen Programme hinzufügen, wenn die folgenden Anforderungen erfüllt sind:

- Die Datei befindet sich nicht im Windows-Systemverzeichnis.
- Die Datei weist eine gültige digitale Signatur auf.

Nachdem Sie ein Programm zur Liste der vertrauenswürdigen Programme hinzugefügt haben, schließt der OfficeScan Agent das Programm automatisch von den folgenden Suchvorgängen aus:

- Dateiprüfung mit der Echtzeitsuche
- Verhaltensüberwachung

- Durchsuchen von Prozessen mit der Echtzeitsuche

Liste der vertrauenswürdigen Programme konfigurieren

Die Liste der vertrauenswürdigen Programme schließt Programme und alle untergeordneten Prozesse aus, die über die Echtzeitsuche und die Verhaltensüberwachung vom Programm aufgerufen werden.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Liste der vertrauenswürdigen Programme**.
4. Geben Sie den vollständigen Programmpfad für das Programm an, das von der Liste ausgeschlossen werden soll.
5. Klicken Sie auf **Zur Liste vertrauenswürdiger Programme hinzufügen**.
6. Um ein Programm aus der Liste zu entfernen, klicken Sie auf das Symbol **Löschen**.
7. Um die Liste der vertrauenswürdigen Programme zu exportieren, klicken Sie auf **Exportieren** und wählen Sie einen Speicherort für die Datei aus.

   Hinweis

   OfficeScan speichert die Liste im `DAT`-Format.

8. Um eine Liste der vertrauenswürdigen Programme zu importieren, klicken Sie auf **Importieren** und wählen Sie einen Speicherort für die Datei aus.

   a. Klicken Sie auf **Durchsuchen...** und wählen Sie den Speicherort für die `DAT`-Datei aus.

   b. Klicken Sie auf **Importieren**.

9. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

    - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

    - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Suchberechtigungen und andere Einstellungen

Benutzer mit Suchberechtigungen haben mehr Kontrolle darüber, wie die Dateien auf ihren Computern gescannt werden. Suchberechtigungen ermöglichen Benutzern oder dem OfficeScan Agent, folgende Aufgaben auszuführen:

- Benutzer können Einstellungen für die manuelle Suche, die zeitgesteuerte Suche und die Echtzeitsuche konfigurieren. Weitere Informationen finden Sie unter *Berechtigungen für die Sucharten auf Seite 7-63*.

- Benutzer können die zeitgesteuerte Suche verschieben, beenden oder überspringen. Weitere Informationen finden Sie unter *Zeitgesteuerte Suchberechtigungen und andere Einstellungen auf Seite 7-65*.

- Benutzer können das Durchsuchen von POP3-E-Mail-Nachrichten nach Viren/Malware aktivieren. Weitere Informationen finden Sie unter *Mail-Scan-Berechtigungen und andere Einstellungen auf Seite 7-71*.

- Der OfficeScan Agent kann Cache-Einstellungen verwenden, um die Suchleistung zu verbessern. Weitere Informationen finden Sie unter *Cache-Einstellungen für die Suche auf Seite 7-73*.

- Die Benutzer können eine individuelle Liste der vertrauenswürdigen Programme anpassen. Weitere Informationen finden Sie unter *Berechtigung für die Liste der vertrauenswürdigen Programme auf Seite 7-77*.

Berechtigungen für die Sucharten

Berechtigt Benutzer, die Einstellungen für die manuelle Suche, die Echtzeitsuche und die zeitgesteuerte Suche selbst zu konfigurieren.

Berechtigungen für die Sucharten gewähren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Navigieren Sie auf der Registerkarte **Berechtigungen** zum Abschnitt **Suchvorgänge**.
5. Wählen Sie die Suchtypen aus, die von den Benutzern konfiguriert werden dürfen.
6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Sucheinstellungen für den OfficeScan Agent konfigurieren

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das OfficeScan Agent Symbol in der Taskleiste und wählen Sie **OfficeScan Agent-Konsole öffnen** aus.

2. Klicken Sie auf **Einstellungen** > **{Suchtyp}**.

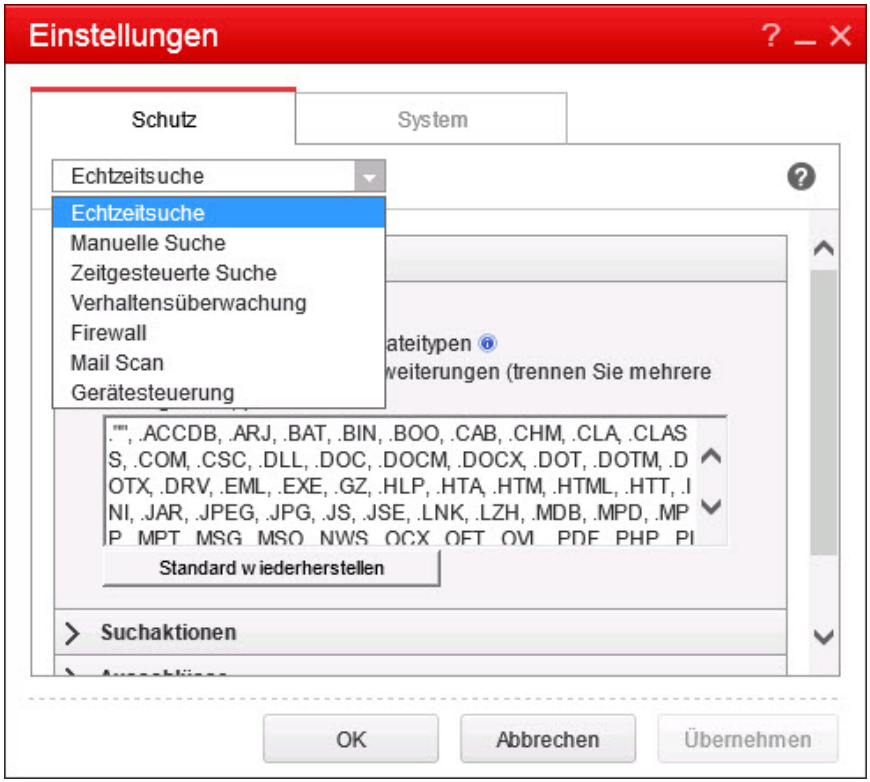


ABBILDUNG 7-1. Sucheinstellungen auf der OfficeScan Agent-Konsole

3. Konfigurieren Sie die folgenden Einstellungen:

- Echtzeitsuche - Einstellungen: Benutzerdefinierte Aktionen für Dateien, Zu durchsuchende Dateien, Sucheinstellungen, Suchausschlüsse, Suchaktionen
- Manuelle Suche - Einstellungen: Zu durchsuchende Dateien, Sucheinstellungen, CPU-Nutzung, Suchausschlüsse, Suchaktionen
- Zeitgesteuerte Suche - Einstellungen: Zeitplan, Zu durchsuchende Dateien, Sucheinstellungen, CPU-Nutzung, Suchausschlüsse, Suchaktionen

4. Klicken Sie auf **OK**.

Zeitgesteuerte Suchberechtigungen und andere Einstellungen

Wird eine zeitgesteuerte Suche auf dem agent durchgeführt, können Benutzer die zeitgesteuerte Suche aufschieben oder überspringen/anhalten.

Zeitgesteuerte Suche verschieben

Benutzer mit der Berechtigung "Zeitgesteuerte Suche verschieben" können die folgenden Aktionen durchführen:

- Zeitgesteuerte Suche verschieben, bevor diese durchgeführt wird, und anschließend die Dauer der Verschiebung festlegen. Die zeitgesteuerte Suche kann nur einmal verschoben werden.
- Wenn die zeitgesteuerte Suche gerade durchgeführt wird, können Benutzer die Suche beenden und später neu starten. Der Benutzer legt anschließend fest, nach wie viel Minuten die Suche erneut durchgeführt werden soll. Wenn die Suche erneut durchgeführt wird, werden alle bereits durchsuchten Dateien nochmal durchsucht. Die zeitgesteuerte Suche kann nur einmal beendet und neu gestartet werden.

Hinweis

Die minimale Verschiebungsdauer/abgelaufene Zeit, die Benutzer angeben können, beträgt 15 Minuten. Das Maximum sind 12 Stunden und 45 Minuten.

Sie können den Zeitpunkt der Verschiebung ändern, indem Sie zu **Agents** > **Globale Agent-Einstellungen** auf der Registerkarte **Sicherheitseinstellungen** navigieren. Ändern Sie im Abschnitt **Einstellungen für zeitgesteuerte Suche** die Einstellung **Zeitgesteuerte Suche verschieben um __ Stunde(n) und __ Minute(n)**.

Zeitgesteuerte Suche überspringen und beenden

Durch diese Berechtigung können Benutzer folgende Aktionen durchführen:

- Zeitgesteuerte Suche überspringen, bevor diese durchgeführt wird
- Zeitgesteuerte Suche beenden, wenn diese gerade durchgeführt wird

Hinweis

Benutzer können eine zeitgesteuerte Suche nur einmal überspringen oder beenden. Selbst nach einem Neustart des Systems setzt die zeitgesteuerte Suche die Suche basierend auf dem nächsten geplanten Zeitpunkt fort.

Berechtigung zur zeitgesteuerten Suche

Damit Benutzer von den Berechtigungen zur zeitgesteuerten Suche profitieren können, sollten Sie sie an die gewährten Berechtigungen erinnern, indem Sie OfficeScan so konfigurieren, dass eine Benachrichtigung vor der Ausführung der zeitgesteuerten Suche angezeigt wird.

Berechtigungen für die zeitgesteuerte Suche gewähren und die Berechtigungsbenachrichtigung anzeigen

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.

2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.

3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.

4. Navigieren Sie auf der Registerkarte **Berechtigungen** zum Abschnitt **Zeitgesteuerte Suchvorgänge**.

5. Wählen Sie die folgenden Optionen:

   - **Zeitgesteuerte Suche verschieben**
   - **Zeitgesteuerte Suche überspringen und beenden**

6. Navigieren Sie auf der Registerkarte **Andere Einstellungen** zum Bereich **Einstellungen zur zeitgesteuerten Suche**.

7. Wählen Sie **Benachrichtigung anzeigen, bevor die zeitgesteuerte Suche ausgeführt wird** aus.

   Wenn Sie diese Option aktivieren, wird eine Benachrichtigung auf dem agent-Endpunkt einige Minuten vor der zeitgesteuerten Suche angezeigt. Benutzer werden über den Zeitplan der Suche (Datum und Uhrzeit) und über erteilte Berechtigungen der zeitgesteuerten Suche, wie z. B. Verschieben, Überspringen oder Beenden der zeitgesteuerten Suche, informiert.

   Hinweis

   Sie können die Dauer der Anzeige in Minuten festlegen. Navigieren Sie zum Konfigurieren der Minutenanzahl zu **Agents** > **Globale Agent-Einstellungen** auf der Registerkarte **Sicherheitseinstellungen**. Ändern Sie im Abschnitt **Einstellungen für zeitgesteuerte Suche** die Einstellung **Benutzer __ Minuten vor Suchbeginn an die zeitgesteuerte Suche erinnern**.

8. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Zeitgesteuerte Suche verschieben/überspringen und beenden auf dem Agent

Prozedur

- Wenn die zeitgesteuerte Suche nicht gestartet wurde:

  a. Klicken Sie mit der rechten Maustaste in der Taskleiste auf das Symbol für OfficeScan Agent, und wählen Sie **Erweiterte zeitgesteuerte Suche - Einstellungen**.

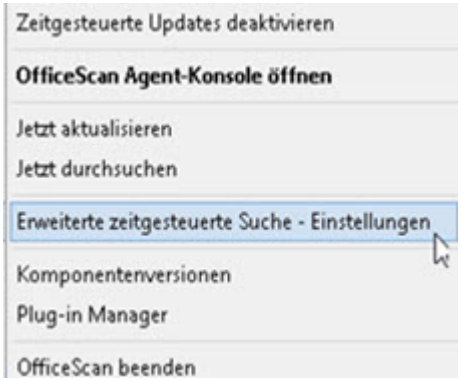


ABBILDUNG 7-2. Option Zeitgesteuerte Suche – Erweiterte Einstellungen

Hinweis

Benutzer müssen diesen Schritt nicht durchführen, wenn die Benachrichtigung aktiviert und so eingestellt ist, dass sie einige Minuten vor der zeitgesteuerten Suche angezeigt wird. Weitere Informationen zur Benachrichtigungsmeldung finden Sie unter *Berechtigung zur zeitgesteuerten Suche auf Seite 7-66*.

b. Wählen Sie im angezeigten Benachrichtigungsfenster eine der folgenden Optionen:

- **Suche verschieben um __ Stunden und __ Minuten.**
- **Diese zeitgesteuerte Suche überspringen. Die nächste zeitgesteuerte Suche wird am <Datum> um <Uhrzeit> durchgeführt.**

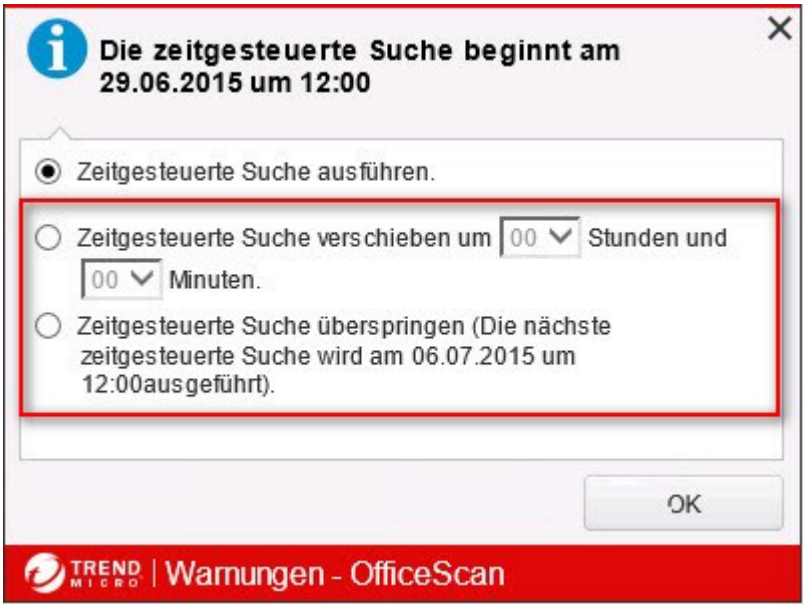


ABBILDUNG 7-3. Berechtigungen für die zeitgesteuerte Suche auf dem OfficeScan Agent Endpunkt

- Wenn die zeitgesteuerte Suche durchgeführt wird:

  a. Klicken Sie mit der rechten Maustaste in der Taskleiste auf das Symbol für OfficeScan Agent, und wählen Sie **Zeitgesteuerte Suche – Erweiterte Einstellungen**.

  b. Wählen Sie im angezeigten Benachrichtigungsfenster eine der folgenden Optionen:

- **Suche beenden. Die Suche neu starten nach __ Stunden und __ Minuten.**
- **Suche beenden. Die nächste zeitgesteuerte Suche wird am <Datum> um <Uhrzeit> durchgeführt.**

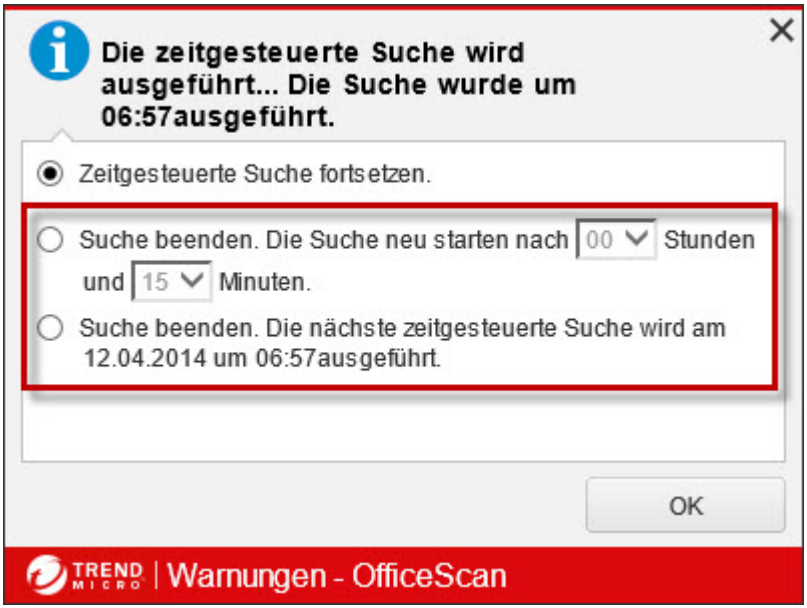


ABBILDUNG 7-4. Berechtigungen zur zeitgesteuerten Suche auf dem OfficeScan Agent Endpunkt

Mail-Scan-Berechtigungen und andere Einstellungen

Wenn OfficeScan Agents Mail-Scan-Berechtigungen haben, wird die Option **Mail Scan** auf der OfficeScan Agent-Konsole angezeigt. Mit der Option **Mail Scan** wird der POP3 Mail Scan angezeigt.

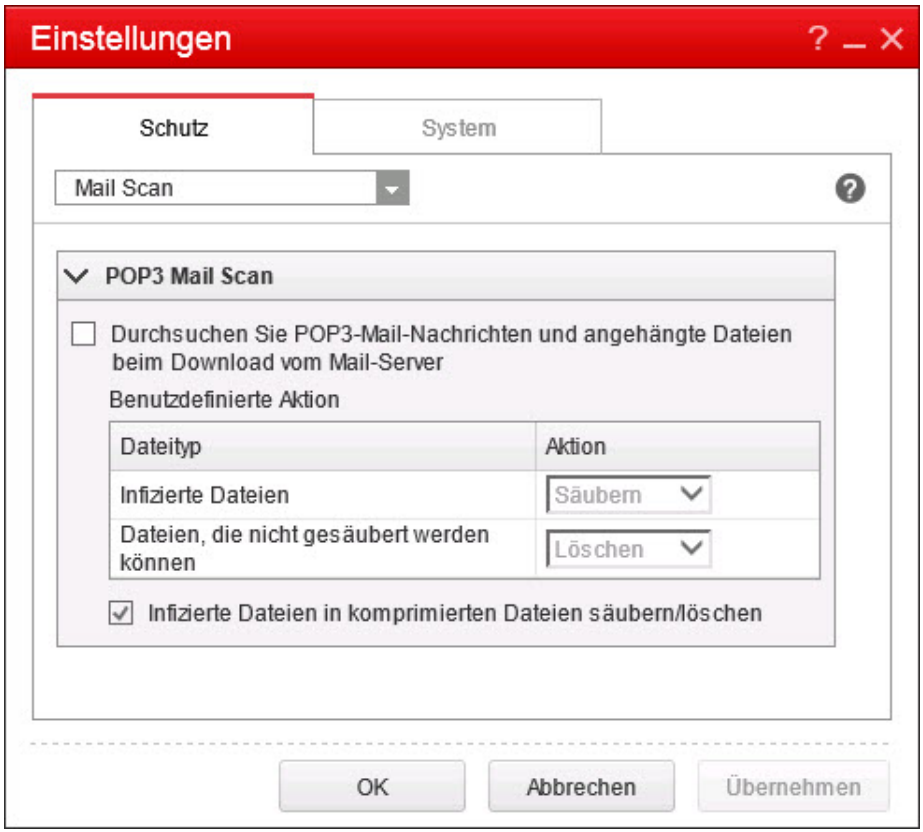


ABBILDUNG 7-5. Mail Scan-Einstellungen auf der OfficeScan Agent-Konsole

In der folgenden Tabelle wird das POP3 Mail Scan-Programm beschrieben.

TABELLE 7-18. Mail Scan Programme

DETAILS	BESCHREIBUNG
Zweck	Durchsucht POP3 E-Mail-Nachrichten nach Viren/Malware
Voraussetzungen	• Müssen vom Administrator auf der Webkonsole aktiviert werden, bevor sie der Benutzer verwenden kann **Hinweis** Weitere Informationen zum Aktivieren von POP3 Mail Scan finden Sie unter *Mail Scan-Berechtigungen gewähren und POP3 Mail Scan aktivieren auf Seite 7-72*. • Maßnahmen gegen Viren/Malware, die auf der OfficeScan Agent-Konsole, nicht aber auf der Webkonsole konfiguriert werden können
Unterstützte Suchtypen	Echtzeitsuche Eine Suche wird durchgeführt während E-Mail-Nachrichten vom POP3 Mail Server abgerufen werden.
Suchergebnis	• Informationen über entdeckte Sicherheitsrisiken liegen vor, sobald der Suchvorgang abgeschlossen ist • Suchergebnisse werden nicht im Fenster **Protokolle** der OfficeScan Agent-Konsole angezeigt. • Suchergenisse werden nicht an den Server gesendet
Weitere Hinweise	Teilt sich den OfficeScan NT Proxy-Dienst (`TMProxy.exe`) mit der Funktion Web Reputation

Mail Scan-Berechtigungen gewähren und POP3 Mail Scan aktivieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.

2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.

3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.

4. Navigieren Sie auf der Registerkarte **Berechtigungen** zum Abschnitt **Mail Scan**.

5. Wählen Sie **Die Mail Scan-Einstellungen auf der OfficeScan Agent-Konsole anzeigen** aus.

6. Navigieren Sie auf der Registerkarte **Andere Einstellungen** zum Bereich **POP3 E-Mail Scan Einstellungen**.

7. Wählen Sie **POP3 E-Mail durchsuchen** aus.

8. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Cache-Einstellungen für die Suche

Der OfficeScan Agent kann eine digitale Signatur erstellen und bei Bedarf Dateien aus dem Cache durchsuchen, um die Suchleistung zu verbessern. Bei einer bedarfsorientierten Suche überprüft der OfficeScan Agent zuerst die Cache-Datei mit den digitalen Signaturen und dann die Cache-Datei nach Dateien, die von der Suche ausgeschlossen werden sollen. Die Suchdauer wird reduziert, wenn viele Dateien von der Suche ausgeschlossen werden.

Digitaler Signatur-Cache

Die Cache-Datei mit den digitalen Signaturen wird während der manuellen Suche, der zeitgesteuerten Suche und der Sofortsuche verwendet. Agents durchsuchen keine Dateien, deren Signaturen zur Cache-Datei mit den digitalen Signaturen hinzugefügt wurden.

Der OfficeScan Agent verwendet das gleiche Pattern für digitale Signaturen, das bei der Verhaltensüberwachung zur Erstellung der Datei mit den digitalen Signaturen verwendet wird. Das Pattern für digitale Signaturen enthält eine Liste von Dateien, die Trend Micro als vertrauenswürdig erachtet und deshalb von der Suche ausschließt.

Hinweis

Die Verhaltensüberwachung wird auf Windows Server-Plattformen automatisch deaktiviert (64-Bit-Unterstützung für Windows XP und Windows 2003 ist nicht verfügbar). Wenn der Cache für digitale Signaturen aktiviert ist, laden OfficeScan Agents auf diesen Plattformen das Pattern für digitale Signaturen zur Verwendung im Cache herunter. Die Komponenten der Verhaltensüberwachung werden aber nicht heruntergeladen.

Agents erstellen die Cache-Datei mit den digitalen Signaturen nach einem Zeitplan, der über die Webkonsole konfiguriert werden kann. Agents gehen so vor, um:

- Die Signaturen neuer Dateien hinzuzufügen, die seit der letzten Erstellung der Cache-Datei in das System eingeführt wurden
- Die Signaturen der Dateien zu entfernen, die verändert oder aus dem System gelöscht wurden

Während der Cache-Erstellung überprüfen die Agents folgende Ordner auf vertrauenswürdige Dateien und fügen dann die Signaturen für diese Dateien zur Cache-Datei mit den digitalen Signaturen hinzu:

- `%PROGRAMFILES%`
- `%WINDIR%`

Die Cache-Erstellung hat keine Auswirkung auf die Leistung des Endpunkts, da die Agents während dieses Prozesses nur minimale Systemressourcen benötigen. Agents können auch eine bereits begonnene Cache-Erstellung wieder fortsetzen, wenn dieser Vorgang aus einem bestimmten Grund abgebrochen wurde (zum Beispiel, wenn der

Rechner von der Stromquelle getrennt wurde oder wenn das Netzteil eines Wireless-Endpunkts nicht angeschlossen ist).

Cache für die On-Demand-Suche

Die Cache-Datei für die On-Demand-Suche wird während der manuellen Suche, der zeitgesteuerten Suche und der Sofortsuche verwendet.OfficeScan Agents durchsuchen keine Dateien, deren Cache zur Cache-Datei für die On-Demand-Suche hinzugefügt wurde.

Bei jeder Suche überprüft der OfficeScan Agent die Eigenschaften der bedrohungsfreien Dateien. Wenn eine bedrohungsfreie Datei in einem bestimmten (konfigurierbaren) Zeitraum nicht verändert wurde, fügt der OfficeScan Agent den Cache der Datei zur Cache-Datei für die On-Demand-Suche hinzu. Bei der nächsten Suche wird diese Datei dann nicht durchsucht, wenn ihr Cache nicht abgelaufen ist.

Der Cache einer bedrohungsfreien Datei läuft nach einer bestimmten (ebenfalls konfigurierbaren) Anzahl von Tagen ab. Wird die Suche bei oder nach Ablauf des Caches durchgeführt, entfernt der OfficeScan Agent den abgelaufenen Cache und durchsucht die Datei nach Bedrohungen. Ist die Datei bedrohungsfrei und bleibt unverändert, wird der Cache der Datei wieder zur Cache-Datei für die bedarfsgesteuerte Suche hinzugefügt. Ist die Datei bedrohungsfrei, wurde aber vor kurzem verändert, wird der Cache nicht hinzugefügt, und die Datei wird bei der nächsten Suche wieder durchsucht.

Der Cache einer bedrohungsfreien Datei läuft ab, um den Auschluss infizierter Dateien von der Suche, wie in den folgenden Beispielen dargestellt, zu verhindern:

- Es ist möglich, dass eine stark veraltete Pattern-Datei eine infizierte, nicht veränderte Datei als bedrohungsfrei eingestuft hat. Wenn der Cache nicht abläuft, verbleibt die infizierte Datei im System, bis sie verändert und von der Echtzeitsuche entdeckt wird.
- Wenn eine gecachte Datei verändert wurde und die Echtzeitsuche zum Zeitpunkt der Dateiänderung nicht funktionsfähig war, muss der Cache ablaufen, damit die veränderte Datei nach Bedrohungen durchsucht werden kann.

Die Anzahl der Caches, die zur Cache-Datei für die bedarfsgesteuerte Suche hinzugefügt werden können, hängt von der Art der Suche und dem jeweiligen Ziel ab. Zum Beispiel

könnte die Anzahl der Caches geringer sein, wenn der OfficeScan Agent bei der manuellen Suche nur 200 anstelle der 1.000 Dateien auf dem Endpunkt durchsucht hat.

Wenn häufig bedarfsgesteuerte Suchen durchgeführt werden, reduziert die Cache-Datei für die bedarfsgesteuerte Suche den Suchzeitaufwand erheblich. Bei einer Aufgabe, bei der kein Cache abgelaufen ist, kann eine durchschnittliche Suchdauer von 12 Minuten auf 1 Minute reduziert werden. Reduziert man die Anzahl von Tagen, die eine Datei unverändert bleiben muss, und verlängert man die Ablaufzeit des Cache, erhöht sich normalerweise die Leistung. Da Dateien nur während einer relativ kurzen Zeitdauer unverändert bleiben müssen, können mehr Caches zur Cache-Datei hinzugefügt werden. Außerdem verlängert sich die Ablaufdauer der Caches, weshalb mehr Dateien von der Suche ausgeschlossen werden können.

Wenn nur selten bedarfsgesteuerte Suchen durchgeführt werden, können sie den Cache dafür deaktivieren, da die Caches ohnehin bis zur nächsten Suche abgelaufen sind.

Cache-Einstellungen für die Suche konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Klicken Sie auf die Registerkarte **Andere Einstellungen**, und gehen Sie zum Abschnitt **Cache-Einstellungen für die Suche**.
5. Konfigurieren Sie die Einstellungen für den digitalen Signatur-Cache.
   a. Wählen Sie **Digitalen Signatur-Cache aktivieren**.
   b. Unter **Cache erstellen alle __ Tage** geben Sie an, wie oft der agent den Cache erstellen soll.
6. Konfigurieren Sie die Einstellungen für den Cache der bedarfsgesteuerten Suche.
   a. Wählen Sie **Cache für die bedarfsgesteuerte Suche aktivieren**.

b. Unter **Cache für sichere Dateien hinzufügen, die unverändert sind seit __ Tagen** geben Sie Anzahl von Tagen an, die eine Datei unverändert sein muss, bevor sie gecacht wird.

c. Unter **Der Cache für eine sichere Datei läuft ab innerhalb von __ Tagen** geben Sie die Anzahl von Tagen an, die ein Cache in der Cache-Datei verbleibt.

Hinweis

Um zu verhindern, dass alle Caches, die bei einer Suche hinzugefügt wurden, am selben Tag ablaufen, laufen die Caches zufallsgesteuert innerhalb der angegebenen Anzahl von Tagen ab. Wenn zum Beispiel an einem Tag 500 Caches zum Cache hinzugefügt wurden und Sie haben als maximale Ablauffrist 10 Tage angegeben, läuft ein Bruchteil der Caches am nächsten Tag und die Mehrzahl der Caches an den darauffolgenden Tagen ab. Am zehnten Tag laufen dann alle übrigen Caches ab.

7. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Berechtigung für die Liste der vertrauenswürdigen Programme

Sie können Endbenutzern die Berechtigung zur Konfigurieren von OfficeScan gewähren, so dass die Suche für vertrauenswürdige Prozesse bei der Echtzeitsuche und der Verhaltensüberwachung übersprungen wird. Nach dem Hinzufügen eines

Programms zur Liste der vertrauenswürdigen Programme führt OfficeScan keine Echtzeitsuche für das Programm oder für vom Programm ausgeführte Prozesse aus. Fügen Sie vertrauenswürdige Programme zur Liste der vertrauenswürdigen Programme hinzu, um die Suchleistung auf Endpunkten zu verbessern.

Einstellungen für die Liste der vertrauenswürdigen Programme gewähren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Navigieren Sie auf der Registerkarte **Berechtigungen** zum Bereich **Liste der vertrauenswürdigen Programme**.
5. Wählen Sie **Die Liste der vertrauenswürdigen Programme auf der OfficeScan Agent-Konsole anzeigen** aus.
6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Allgemeine Sucheinstellungen

Es gibt mehrere Möglichkeiten, die allgemeinen Sucheinstellungen auf die agents anzuwenden.

- Eine bestimmte Sucheinstellung kann für alle agents gelten, die der Server verwaltet, oder nur für agents mit bestimmten Suchberechtigungen. Wenn Sie z. B. die Dauer für die Verschiebung der zeitgesteuerten Suche konfigurieren, wird diese Einstellung nur von agents verwendet, die über die Berechtigung verfügen, die zeitgesteuerte Suche zu verschieben.
- Eine bestimmte Sucheinstellung kann für alle oder nur einen bestimmten Suchtyp gelten. Beispielsweise können Sie auf Endpunkten, auf denen sowohl der OfficeScan Server als auch der OfficeScan Agent installiert sind, die OfficeScan Server-Datenbank von der Suche ausschließen. Diese Einstellung gilt jedoch nur während der Echtzeitsuche.
- Eine bestimmte Sucheinstellung kann zutreffen, wenn Sie entweder nach Viren/Malware oder Spyware/Grayware oder beidem suchen. Der Bewertungsmodus gilt beispielsweise nur während der Suche nach Spyware/Grayware.

Allgemeine Sucheinstellungen konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Klicken Sie auf die Registerkarte **Sicherheitseinstellungen** und konfigurieren Sie die allgemeinen Sucheinstellungen in allen verfügbaren Abschnitten.
   - *Abschnitt "Sucheinstellungen" auf Seite 7-81*
   - *Abschnitt "Einstellungen für die zeitgesteuerte Suche" auf Seite 7-87*
3. Klicken Sie auf die Registerkarte **System**.
4. Konfigurieren Sie im Abschnitt **Einstellungen für Certified Safe Software Service** die Einstellung **Certified Safe Software Service für Verhaltensüberwachung, Firewall und Virensuchen aktivieren**.

Der Certified Safe Software Service fragt Trend Micro Rechenzentren ab, um die Sicherheit eines von der Sperrung bei Malware-Verhalten, der Ereignisüberwachung, der Firewall oder der Virensuche erkannten Programms zu überprüfen. Aktivieren Sie den Certified Safe Software Service, um die Häufigkeit von Fehlalarmen zu verringern.

Hinweis

Achten Sie auf korrekte Proxy-Einstellungen für OfficeScan Agents (weitere Informationen finden Sie unter *OfficeScan Agent Proxy-Einstellungen auf Seite 15-53*), bevor Certified Safe Software Service aktiviert wird. Bei fehlerhaften Proxy-Einstellungen sowie einer Internet-Verbindung, die nicht ständig besteht, kann es zu Verzögerungen kommen, oder Antworten von Trend Micro Rechenzentren können nicht abgerufen werden, was zur Folge hat, dass überwachte Programme nicht zu antworten scheinen.

Des Weiteren können IPv6-OfficeScan Agents keine direkten Abfragen an Trend Micro Rechenzentren richten. Ein Dual-Stack-Proxy-Server wie beispielsweise DeleGate, der IP-Adressen konvertieren kann, muss ermöglichen, dass die OfficeScan Agents eine Verbindung zu Trend Micro Rechenzentren herstellen können.

5. Klicken Sie auf die Registerkarte **Netzwerk**.

6. Konfigurieren Sie im Abschnitt **Bandbreiteneinstellungen des Viren-/Malware-Protokolls** die Einstellung **OfficeScan Agent so konfigurieren, dass für erneute Funde desselben Virus/derselben Malware innerhalb einer Stunde nur ein Protokolleintrag erstellt wird**.

   OfficeScan führt Protokolleinträge zusammen, wenn innerhalb kurzer Zeit mehrere Infektionen mit demselben Virus oder derselben Malware entdeckt werden. Es kann vorkommen, dass OfficeScan denselben Virus oder dieselbe Malware mehrmals entdeckt. Da sich das Viren-/Malware-Protokoll dadurch rasch mit Einträgen füllt, erhöht sich der Verbrauch an Netzwerkbandbreite, wenn der OfficeScan Agent Protokollinformationen an den Server sendet. Mit der Aktivierung dieser Funktion werden die Anzahl der Einträge im Viren- und Malware-Protokoll und der Verbrauch von Netzwerkbandbreite für OfficeScan Agents reduziert, wenn diese dem Server Virenprotokollinformationen übermitteln.

7. Klicken Sie auf die Registerkarte **Agent Kontrolle**.

8. Konfigurieren Sie im Abschnitt **Allgemeine Einstellungen** die Einstellung **Manuelle Suche zum Windows-Kontextmenü auf Endpunkten hinzufügen**.

   Wenn diese Einstellung aktiviert ist, fügen alle OfficeScan Agents, die vom Server verwaltet werden, die Option **Suche mit OfficeScan** dem Kontextmenü in Windows Explorer hinzu. Wenn Benutzer mit der rechten Maustaste auf eine Datei oder einen Ordner auf dem Windows Desktop oder in Windows Explorer klicken und die Option auswählen, wird eine manuelle Suche in der Datei oder im Ordner nach Viren/Malware und Spyware/Grayware durchgeführt.

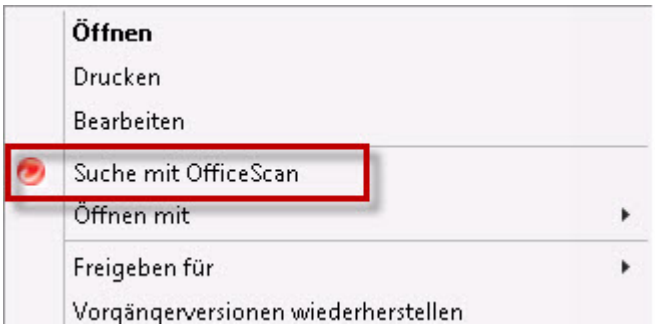


ABBILDUNG 7-6. Suche mit OfficeScan-Option

9. Klicken Sie auf **Speichern**.

Abschnitt "Sucheinstellungen"

Im Abschnitt **Sucheinstellungen** auf der Registerkarte **Sicherheitseinstellungen** des Fensters **Globale Agent-Einstellungen** können Administratoren Folgendes konfigurieren:

- *Den Ordner der OfficeScan Server-Datenbank von der Echtzeitsuche ausschließen auf Seite 7-82*
- *Ordner und Dateien des Microsoft Exchange-Servers von den Suchvorgängen ausschließen auf Seite 7-82*

- *Verzögerte Suche für Dateivorgänge aktivieren auf Seite 7-83*
- *Early Launch Anti-Malware-Schutz auf Endpunkten aktivieren auf Seite 7-83*
- *Infizierte Dateien in komprimierten Dateien säubern/löschen auf Seite 7-84*
- *Bewertungsmodus aktivieren auf Seite 7-86*
- *Nach Cookies suchen auf Seite 7-87*

Den Ordner der OfficeScan Server-Datenbank von der Echtzeitsuche ausschließen

Wenn sich der OfficeScan Agent und OfficeScan Server auf demselben Endpunkt befinden, durchsucht der OfficeScan Agent während einer Echtzeitsuche nicht die Server-Datenbank nach Viren/Malware und Spyware/Grayware.

Tipp

Aktivieren Sie diese Einstellung, um zu verhindern, dass die Datenbank während der Suche beschädigt wird.

Ordner und Dateien des Microsoft Exchange-Servers von den Suchvorgängen ausschließen

Wenn sich der OfficeScan Agent und ein Microsoft Exchange 2000/2003 Server auf demselben Endpunkt befinden, durchsucht OfficeScan nicht die folgenden Ordner und Dateien von Microsoft Exchange nach Viren/Malware und Spyware/Grayware während der manuellen Suche, Echtzeitsuche, zeitgesteuerten Suche und der Funktion "Jetzt durchsuchen":

- Die folgenden Ordner in `\Exchsrvr\Mailroot\vsi 1`:`Queue`, `PickUp` und `BadMail`
- "`.\Exchsrvr\mdbdata `", einschließlich dieser Dateien:`priv1.stm`, `priv1.edb`, `pub1.stm` und `pub1.edb`
- `.\Exchsrvr\Storage Group`

Microsoft Exchange 2007 Ordner oder höher müssen manuell zur Ausschlussliste hinzugefügt werden. Einzelheiten zu den Suchausschlüssen finden Sie auf der folgenden Website:

http://technet.microsoft.com/en-us/library/bb332342.aspx

Die einzelnen Schritte zur Konfiguration der Ausschlussliste für die Virensuche finden Sie unter *Suchausschlüsse auf Seite 7-34*.

Verzögerte Suche für Dateivorgänge aktivieren

Administratoren können einstellen, dass OfficeScan das Durchsuchen von Dateien verzögern soll.OfficeScan erlaubt den Benutzern, die Dateien zu kopieren, bevor die Dateien durchsucht werden. Diese Verzögerung steigert die Leistung beim Kopieren und Suchen.

Hinweis

Die verzögerte Suche erfordert die Version 9.713 oder höher von Viren-Scan-Engine (VSAPI). Weitere Informationen zum Aktualisieren des Servers finden Sie unter *Den OfficeScan Server manuell aktualisieren auf Seite 6-27*.

Early Launch Anti-Malware-Schutz auf Endpunkten aktivieren

OfficeScan unterstützt die Funktion Early Launch Anti-Malware (ELAM) als Teil des Sicheren Start-Standards, um Startzeitschutz an Endpunkten zu bieten. Administratoren können diese Funktion aktivieren, um OfficeScan-Agenten vor Softwaretreibern anderer Hersteller zu starten, wenn Endpunkte gestartet werden. Mit dieser Funktion werden OfficeScan Agents aktiviert, um Malware während des Betriebssystemstarts zu erkennen.

Nach dem Durchsuchen aller Softwaretreiber anderer Hersteller übermittelt der OfficeScan Agent dem Systemkernel die Informationen zur Treiberklassifizierung. Administratoren können in der Gruppenrichtlinie in Windows Aktionen basierend auf der Treiberklassifizierung festlegen und Suchergebnisse unter Verwendung der Ergebnisanzeige auf Endpunkten anzeigen.

Hinweis

ELAM wird nur unter Windows 8, Windows Server 2012 oder neueren Versionen unterstützt.

Infizierte Dateien in komprimierten Dateien säubern/löschen

Wenn die agents, die vom Server verwaltet werden, Viren/Malware innerhalb von komprimierten Dateien während einer manuellen Suche, Echtzeitsuche, zeitgesteuerten Suche und der Funktion "Jetzt durchsuchen" finden und die folgenden Bedingungen erfüllt sind, können die agents die infizierten Dateien säubern oder löschen.

- OfficeScan führt die Aktion "Säubern" oder "Löschen" durch. Sie können die Aktion von OfficeScan für infizierte Dateien auf der Registerkarte **Agents** > **Agent-Verwaltung > Einstellungen** > **Sucheinstellungen** > **{Suchtyp}** > **Aktion** prüfen.
- Diese Einstellung aktivieren Sie selbst. Die Aktivierung dieser Einstellung kann zu einer erhöhten Nutzung der Endpunktressourcen während der Suche führen und die Suchdauer verlängern. Der Grund ist, dass OfficeScan die komprimierte Datei dekomprimieren, die infizierten Dateien innerhalb der komprimierten Datei säubern/löschen und anschließend die Datei wieder komprimieren muss.
- Das komprimierte Dateiformat wird unterstützt. OfficeScan unterstützt nur bestimmte ZIP-Komprimierungsformate, wie z. B. ZIP und Office Open XML. Office Open XML ist das Standardformat für Microsoft Office 2007 Anwendungen wie Excel, PowerPoint und Word.

  Hinweis

  Eine vollständige Liste der unterstützten Komprimierungsformate erhalten Sie von Ihrem Support-Anbieter.

Beispielsweise wurde für die Echtzeitsuche festgelegt, dass Dateien, die mit einem Virus infiziert sind, gelöscht werden sollen. Nachdem die Echtzeitsuche eine komprimierte Datei mit der Bezeichnung `abc.zip` dekomprimiert hat und eine infizierte Datei `123.doc` innerhalb der komprimierten Datei gefunden hat, löscht OfficeScan die Datei `123.doc` und führt anschließend eine erneute Komprimierung von `abc.zip` durch, auf die daraufhin sicher zugegriffen werden kann.

In der folgenden Tabelle wird beschrieben, was geschieht, wenn eine der Bedingungen nicht erfüllt ist.

TABELLE 7-19. Komprimierte Dateien – Szenarien und Ergebnisse

STATUS VON "INFIZIERTE DATEIEN IN KOMPRIMIERTEN DATEIEN SÄUBERN/ LÖSCHEN"	AKTION, DIE OFFICESCAN DURCHFÜHREN SOLL	KOMPRIMIERTES DATEIFORMAT	ERGEBNIS
Aktiviert	Säubern oder Löschen	Nicht unterstützt Beispiel: `def.rar` enthält eine infizierte Datei mit dem Namen `123.doc`.	OfficeScan verschlüsselt `def.rar`. Die Datei `123.doc` wird jedoch weder gesäubert, gelöscht, noch anderweitig verarbeitet.
Deaktiviert	Säubern oder Löschen	Unterstützt/Nicht unterstützt Beispiel: `abc.zip` enthält eine infizierte Datei mit dem Namen `123.doc`.	Diese beiden Dateien (`abc.zip` und `123.doc`) werden von OfficeScan weder gesäubert, gelöscht, noch anderweitig verarbeitet.

Status von "Infizierte Dateien in komprimierten Dateien säubern/ löschen"	Aktion, die OfficeScan durchführen soll	Komprimiertes Dateiformat	Ergebnis
Aktiviert/ Deaktiviert	Nicht säubern oder löschen (also eine der folgenden Aktionen: Umbenennen, Quarantäne, Zugriff verweigern oder Übergehen)	Unterstützt/Nicht unterstützt Beispiel: `abc.zip` contains an infected file `123.doc`.	OfficeScan führt die konfigurierte Aktion (Umbennen, Quarantäne, Zugriff verweigern oder Übergehen) für die Datei `abc.zip` durch, nicht aber für die Datei `123.doc`. Bei der Aktion: **Umbenennen**: Benennt OfficeScan `abc.zip` in `abc.vir` um, nicht aber `123.doc`. **Quarantäne**: OfficeScan verschiebt `abc.zip` in Quarantäne (`123.doc` und alle nicht infizierten Dateien werden in Quarantäne verschoben). **Übergehen**: OfficeScan führt keine Aktion für die beiden Dateien `abc.zip` und `123.doc` durch, protokolliert jedoch den Virenfund. **Zugriff verweigern**: OfficeScan verweigert den Zugriff auf `abc.zip`, wenn diese geöffnet wird (`123.doc` und alle nicht infizierten Dateien können nicht geöffnet werden).

Bewertungsmodus aktivieren

Im Bewertungsmodus protokollieren alle vom Server verwalteten agents Spyware/ Grayware, die während der manuellen Suche, zeitgesteuerten Suche, Echtzeitsuche und

der Funktion "Jetzt durchsuchen" gefunden wurde. Dabei werden jedoch die Spyware-/Grayware-Komponenten nicht gesäubert. Bei der Säuberung werden Prozesse beendet oder Registrierungseinträge, Dateien, Cookies und Shortcuts gelöscht.

Mit dem Bewertungsmodus von Trend Micro können Sie Elemente überprüfen, die Trend Micro als Spyware/Grayware einstuft, und dann eine geeignete Aktion durchführen. Beispielsweise können Sie entdeckte Spyware/Grayware, die Sie als ungefährlich erachten, zur Liste der zugelassenen Spyware/Grayware hinzufügen.

Im Bewertungsmodus führt OfficeScan die folgenden Suchaktionen durch:

- **Übergehen**: Während der manuellen Suche, zeitgesteuerten Suche und der Funktion "Jetzt durchsuchen"
- **Zugriff verweigern**: Während der Echtzeitsuche

Hinweis

Der Bewertungsmodus setzt alle benutzerdefinierten Suchaktionen außer Kraft. Wenn Sie beispielsweise "Säubern" als Suchaktion für die manuelle Suche auswählen, bleibt "Übergehen" weiterhin die Suchaktion, wenn sich agent im Bewertungsmodus befindet.

Nach Cookies suchen

Wählen Sie diese Option aus, wenn Sie Cookies als potenzielle Sicherheitsrisiken einstufen. Wenn diese Option ausgewählt ist, werden alle vom Server verwalteten agents während der manuellen Suche, zeitgesteuerten Suche, Echtzeitsuche und der Funktion "Jetzt durchsuchen" nach Cookies für Spyware/Grayware durchsucht.

Abschnitt "Einstellungen für die zeitgesteuerte Suche"

Die folgenden Einstellungen werden nur von agents verwendet, die die zeitgesteuerte Suche ausführen. Die zeitgesteuerte Suche kann nach Viren/Malware und Spyware/Grayware suchen.

Im Abschnitt "Einstellungen für zeitgesteuerte Suche" der allgemeinen Sucheinstellungen können Administratoren Folgendes konfigurieren:

- *Benutzer __ Minuten vor Suchbeginn an die zeitgesteuerte Suche erinnern. auf Seite 7-88*

- *Zeitgesteuerte Suche verschieben um __ Stunden und __ Minuten auf Seite 7-88*
- *Zeitgesteuerte Suche automatisch beenden, wenn die Suche länger dauert als __ Stunden und __ Minuten auf Seite 7-89*
- *Zeitgesteuerte Suche überspringen, wenn die Akkulaufzeit eines Wireless-Endpunkts weniger als __ % beträgt und der AC-Adapter nicht angeschlossen ist auf Seite 7-89*
- *Eine übersprungene zeitgesteuerte Suche fortsetzen auf Seite 7-89*

Benutzer __ Minuten vor Suchbeginn an die zeitgesteuerte Suche erinnern.

OfficeScan zeigt eine Benachrichtigung einige Minuten vor der Durchführung der Suche an, um Benutzer an den Zeitplan der Suche (Datum und Uhrzeit) und alle Berechtigungen zu erinnern, die ihnen im Zusammenhang mit der zeitgesteuerten Suche gewährt wurden.

Über den folgenden Menüpfad kann die Benachrichtigung aktiviert bzw. deaktiviert werden: **Agents** > **Agent-Verwaltung > Einstellungen** > **Berechtigungen und andere Einstellungen** > **Andere Einstellungen (Registerkarte)** > **Zeitgesteuerte Suche - Einstellungen**. Wenn diese Option deaktiviert wurde, wird keine Erinnerung angezeigt.

Zeitgesteuerte Suche verschieben um __ Stunden und __ Minuten

Nur Benutzer mit der Berechtigung "Zeitgesteuerte Suche verschieben" können die folgenden Aktionen durchführen:

- Zeitgesteuerte Suche verschieben, bevor diese durchgeführt wird, und anschließend die Dauer der Verschiebung festlegen.
- Wenn die zeitgesteuerte Suche gerade durchgeführt wird, können Benutzer die Suche beenden und später neu starten. Der Benutzer legt anschließend fest, nach wie viel Minuten die Suche erneut durchgeführt werden soll. Wenn die Suche erneut durchgeführt wird, werden alle bereits durchsuchten Dateien nochmal durchsucht.

  Die maximale Verschiebungsdauer/abgelaufene Zeit, die Benutzer angeben können, beträgt 12 Stunden und 45 Minuten. Sie können die Dauer verkürzen,

indem Sie die Anzahl der Stunde(n) und/oder Minute(n) in den entsprechenden Feldern ändern.

Zeitgesteuerte Suche automatisch beenden, wenn die Suche länger dauert als __ Stunden und __ Minuten

OfficeScan beendet die Suche automatisch, wenn die festgelegte Zeit überschritten wurde und die Suche noch nicht abgeschlossen ist. Bei der Suche benachrichtigt OfficeScan die Benutzer sofort über die entdeckten Sicherheitsrisiken.

Zeitgesteuerte Suche überspringen, wenn die Akkulaufzeit eines Wireless-Endpunkts weniger als __ % beträgt und der AC-Adapter nicht angeschlossen ist

OfficeScan beendet den Suchvorgang sofort, wenn die zeitgesteuerte Suche gestartet und dabei festgestellt wird, dass der Akkustand eines Wireless-Endpunkts niedrig und das Netzteil nicht angeschlossen ist. Ist der Akkustand niedrig und das Netzteil angeschlossen, wird die Suche fortgesetzt.

Eine übersprungene zeitgesteuerte Suche fortsetzen

Wenn die zeitgesteuerte Suche nicht startet, weil OfficeScan zu dem entsprechenden Zeitpunkt nicht ausgeführt wird oder weil der Benutzer die zeitgesteuerte Suche unterbricht (z. B. durch Ausschalten des Endpunkts, nachdem die Suche gestartet wurde), können Sie angeben, wann OfficeScan die Suche wieder aufnehmen soll.

Geben Sie an, welche zeitgesteuerte Suche erneut gestartet werden soll:

- **Eine unterbrochene zeitgesteuerte Suche fortsetzen**: Nimmt eine zeitgesteuerte Suche wieder auf, die der Benutzer durch Ausschalten des Endpunkts unterbrochen hat
- **Eine übersprungene zeitgesteuerte Suche fortsetzen**: Nimmt eine zeitgesteuerte Suche wieder auf, die übersprungen wurde, weil der Endpunkt nicht ausgeführt wurde

Geben Sie an, wann die Suche wieder aufgenommen werden soll:

- **Gleiche Uhrzeit am nächsten Tag**: OfficeScan führt die Suche zur selben Zeit am nächsten Tag durch, wenn OfficeScan ausgeführt wird.
- **__ Minuten nach dem Start des Endpunkts**: OfficeScan setzt die Suche nach einer bestimmten Anzahl von Minuten fort, nachdem der Benutzer den Endpunkt eingeschaltet hat. Die Anzahl der Minuten liegt zwischen 10 und 120.

Hinweis

Benutzer können eine zeitgesteuerte Suche verschieben oder überspringen, wenn der Administrator diese Berechtigung aktiviert. Weitere Informationen finden Sie unter *Zeitgesteuerte Suchberechtigungen und andere Einstellungen auf Seite 7-65*.

Benachrichtigungen bei Sicherheitsrisiken

OfficeScan verfügt über zahlreiche Standardbenachrichtigungen, die Sie, andere OfficeScan Administratoren und OfficeScan Agent-Benutzer über entdeckte Sicherheitsrisiken informieren.

Weitere Informationen zu den an Administratoren gesendeten Benachrichtigungen finden Sie unter *Benachrichtigungen bei Sicherheitsrisiken für Administratoren auf Seite 7-90*.

Weitere Informationen zu den an OfficeScan Agent-Benutzer gesendeten Benachrichtigungen finden Sie unter *Benachrichtigungen bei Sicherheitsrisiken für OfficeScan Agent Benutzer auf Seite 7-97*.

Benachrichtigungen bei Sicherheitsrisiken für Administratoren

Konfigurieren Sie OfficeScan so, dass Sie oder andere OfficeScan Administratoren benachrichtigt werden, sobald ein Sicherheitsrisiko entdeckt wird oder nur dann, wenn die Aktion gegen das entdeckte Sicherheitsrisiko fehlschlägt und Ihr Eingreifen nötig ist.

OfficeScan verfügt über zahlreiche Standardbenachrichtigungen, die Sie und andere OfficeScan Administratoren über entdeckte Sicherheitsrisiken informieren. Sie können diese Benachrichtigungen ändern und zusätzliche Benachrichtigungseinstellungen konfigurieren, die Ihren Anforderungen entsprechen.

TABELLE 7-20. Typen von Sicherheitsrisiko-Benachrichtigungen

TYP	NACHSCHLAGEWERKE
Viren/Malware	*Benachrichtigungen bei Sicherheitsrisiken für Administratoren konfigurieren auf Seite 7-91*
Spyware/Grayware	*Benachrichtigungen bei Sicherheitsrisiken für Administratoren konfigurieren auf Seite 7-91*
übertragungen digitaler Assets	*Benachrichtigung zur Funktion "Prävention vor Datenverlust" für Administratoren konfigurieren auf Seite 11-59*
C&C-Callbacks	*C&C-Callback-Benachrichtigungen für Administratoren konfigurieren auf Seite 12-16*

Hinweis

OfficeScan kann Benachrichtigungen per E-Mail, SNMP-Trap und Windows NT Ereignisprotokolle versenden. Konfigurieren Sie die Einstellungen, wenn OfficeScan über diese Kanäle Benachrichtigungen versendet. Weitere Informationen finden Sie unter *Einstellungen für die Administratorbenachrichtigungen auf Seite 14-43*.

Benachrichtigungen bei Sicherheitsrisiken für Administratoren konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Administrator**.

   Das Fenster **Administratorbenachrichtigungen** wird angezeigt.

2. Auf der Registerkarte **Kriterien**:

   a. Gehen Sie zum Abschnitt **Viren/Malware** oder **Spyware/Grayware**.

   b. Geben Sie an, ob Benachrichtigungen gesendet werden sollen, wenn OfficeScan Viren/Malware und Spyware/Grayware entdeckt, oder nur dann, wenn die Aktionen gegen diese Sicherheitsrisiken fehlgeschlagen sind.

3. Auf der Registerkarte **E-Mail**:

a. Gehen Sie zum Abschnitt **Viren/Malware Fund** oder **Spyware/Grayware Fund**.

b. Wählen Sie **Benachrichtigung über E-Mail aktivieren**.

c. Wählen Sie **Benachrichtigungen an Benutzer mit Agent-Hierarchie-Domänenberechtigungen senden**.

Mit der rollenbasierten Administration können Sie Benutzern agent-Hierarchiedomänenberechtigungen gewähren. Bei einer Erkennung auf einem OfficeScan Agent, der zu einer bestimmten Domäne gehört, wird die E-Mail an die E-Mail-Adressen der Benutzer mit Domänenberechtigung gesendet. Beispiele dafür sehen Sie in der folgenden Tabelle:

TABELLE 7-21. Agent-Hierarchiedomänen und Berechtigungen

AGENT-HIERARCHIEDOMÄNE	ROLLEN MIT DOMÄNENBERECHTIGUNGEN	BENUTZERKONTO MIT DIESER ROLLE	E-MAIL-ADRESSE FÜR DAS BENUTZERKONTO
Domäne A	Administrator (integriert)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domäne B	Administrator (integriert)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

Entdeckt ein OfficeScan Agent, der zur Domäne A gehört, einen Virus, wird die E-Mail an mary@xyz.com, john@xyz.com und chris@xyz.com gesendet.

Entdeckt ein OfficeScan Agent, der zur Domäne B gehört, Spyware, wird die E-Mail an mary@xyz.com und jane@xyz.com gesendet.

Hinweis

Wenn Sie die Option aktivieren, benötigen alle Benutzer mit Domänenberechtigung eine entsprechende E-Mail-Adresse. Die E-Mail-Benachrichtigung wird nicht an Benutzer ohne E-Mail-Adresse gesendet. Benutzer und E-Mail-Adressen werden unter **Administration** > **Kontenverwaltung** > **Benutzerkonten** konfiguriert.

d. Wählen Sie **Benachrichtigungen an folgende E-Mail-Adresse(n) senden**, und geben Sie dann die E-Mail-Adressen ein.

e. Geben Sie im Feld **Betreff** den Betreff der E-Mail-Benachrichtigung ein.

f. Geben Sie im Feld **Nachricht** den Inhalt der Nachricht ein.

OfficeScan unterstützt die Verwendung von Token in den Feldern **Betreff** und **Nachricht**.

TABELLE 7-22. Token-Variablen für Benachrichtigungen über Sicherheitsrisiken

TOKEN-VARIABLE	BESCHREIBUNG
Viren-/Malware-Funde	
%v	Name der Sicherheitsbedrohung
%s	Endpunkt mit Erkennung
%i	IP-Adresse des Endpunkts
%c	MAC-Adresse des Endpunkts
%m	Domäne des Endpunkts
%p	Fundort des Virus/der Malware
%y	Datum und Uhrzeit der Erkennung
%e	Viren-Scan-Engine-Version
%r	Version der Viren-Pattern-Datei
%a	Für das Sicherheitsrisiko durchgeführte Aktionen

Token-Variable	Beschreibung
%n	Name des Benutzers, der am Endpunkt angemeldet ist
Spyware-/Grayware-Funde	
%s	Endpunkt mit Erkennung
%i	IP-Adresse des Endpunkts
%m	Domäne des Endpunkts
%y	Datum und Uhrzeit der Erkennung
%n	Name des Benutzers, der am Endpunkt angemeldet ist
%T	Spyware-/Grayware-Suchergebnis

4. Auf der Registerkarte **SNMP-Trap**:

   a. Gehen Sie zum Abschnitt **Viren/Malware Fund** oder **Spyware/Grayware Fund**.

   b. Wählen Sie **Benachrichtigung per SNMP-Trap aktivieren**.

   c. Übernehmen Sie die Standardmeldung oder ändern Sie sie. In der folgenden Tabelle können Sie Token-Variablen als Platzhalter für Daten im Feld **Nachricht** verwenden.

Tabelle 7-23. Token-Variablen für Benachrichtigungen über Sicherheitsrisiken

Variable	Beschreibung
Viren-/Malware-Funde	
%v	Name der Sicherheitsbedrohung
%s	Endpunkt mit Erkennung
%i	IP-Adresse des Endpunkts
%c	MAC-Adresse des Endpunkts

Variable	Beschreibung
%m	Domäne des Endpunkts
%p	Fundort des Virus/der Malware
%y	Datum und Uhrzeit der Erkennung
%e	Viren-Scan-Engine-Version
%r	Version der Viren-Pattern-Datei
%a	Für das Sicherheitsrisiko durchgeführte Aktionen
%n	Name des Benutzers, der am Endpunkt angemeldet ist
Spyware-/Grayware-Funde	
%s	Endpunkt mit Erkennung
%i	IP-Adresse des Endpunkts
%m	Domäne des Endpunkts
%y	Datum und Uhrzeit der Erkennung
%n	Name des Benutzers, der am Endpunkt angemeldet ist
%T	Spyware-/Grayware-Suchergebnis
%v	Name der Sicherheitsbedrohung
%a	Für das Sicherheitsrisiko durchgeführte Aktionen

5. Auf der Registerkarte **NT-Ereignisprotokoll**:

   a. Gehen Sie zum Abschnitt **Viren/Malware Fund** oder **Spyware/Grayware Fund**.

   b. Wählen Sie **Benachrichtigung über NT-Ereignisprotokoll aktivieren**.

   c. Übernehmen Sie die Standardmeldung oder ändern Sie sie. In der folgenden Tabelle können Sie Token-Variablen als Platzhalter für Daten im Feld **Nachricht** verwenden.

TABELLE 7-24. Token-Variablen für Benachrichtigungen über Sicherheitsrisiken

VARIABLE	BESCHREIBUNG
Viren-/Malware-Funde	
%v	Name der Sicherheitsbedrohung
%s	Endpunkt mit Erkennung
%i	IP-Adresse des Endpunkts
%c	MAC-Adresse des Endpunkts
%m	Domäne des Endpunkts
%p	Fundort des Virus/der Malware
%y	Datum und Uhrzeit der Erkennung
%e	Viren-Scan-Engine-Version
%r	Version der Viren-Pattern-Datei
%a	Für das Sicherheitsrisiko durchgeführte Aktionen
%n	Name des Benutzers, der am Endpunkt angemeldet ist
Spyware-/Grayware-Funde	
%s	Endpunkt mit Erkennung
%i	IP-Adresse des Endpunkts
%m	Domäne des Endpunkts
%y	Datum und Uhrzeit der Erkennung
%n	Name des Benutzers, der am Endpunkt angemeldet ist
%T	Spyware-/Grayware-Suchergebnis
%v	Name der Sicherheitsbedrohung
%a	Für das Sicherheitsrisiko durchgeführte Aktionen

6. Klicken Sie auf **Speichern**.

Benachrichtigungen bei Sicherheitsrisiken für OfficeScan Agent Benutzer

OfficeScan kann Benachrichtigungen auf OfficeScan Agent-Endpunkten anzeigen:

- Unmittelbar nachdem bei der Echtzeitsuche und der zeitgesteuerten Suche Viren/Malware oder Spyware/Grayware entdeckt wurden. Sie können die Benachrichtigung aktivieren und optional den Inhalt ändern.
- Wenn ein Endpunkt zum Säubern infizierter Dateien neu gestartet werden muss. Im Fall der Echtzeitsuche wird die Meldung angezeigt, nachdem ein bestimmtes Sicherheitsrisiko bei der Suche gefunden wurde. Im Fall der manuellen Suche, zeitgesteuerten Suche und bei der Funktion "Jetzt durchsuchen" wird die Meldung ein Mal angezeigt, nachdem OfficeScan die Durchsuchung aller Suchziele abgeschlossen hat.

TABELLE 7-25. Typen von Sicherheitsrisiko-Agent-Benachrichtigungen

TYP	NACHSCHLAGEWERKE
Viren/Malware	*Benachrichtigungen über Viren/Malware für OfficeScan Agents konfigurieren auf Seite 7-99*
Spyware/Grayware	*Spyware-/Grayware-Benachrichtigungen konfigurieren auf Seite 7-100*
Firewall-Verstöße	*Den Inhalt der Firewall-Benachrichtigung ändern auf Seite 13-32*
Verstöße gegen die Web Reputation	*Benachrichtigungen über Internet-Bedrohungen ändern auf Seite 12-15*
Verstöße gegen die Gerätesteuerung	*Gerätesteuerungsbenachrichtigungen ändern auf Seite 10-19*
Verstöße gegen eine Verhaltensüberwachungs-Richtlinie	*Inhalt der Benachrichtigung ändern auf Seite 9-24*

TYP	NACHSCHLAGEWERKE
Übertragungen digitaler Assets	*Benachrichtigung zur Funktion "Prävention vor Datenverlust" für Agents konfigurieren auf Seite 11-62*
C&C-Callbacks	*Benachrichtigungen über Internet-Bedrohungen ändern auf Seite 12-15*

Benutzer bei Viren-/Malware- oder Spyware-/Grayware-Fund benachrichtigen

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Sucheinstellungen** > **Einstellungen der Echtzeitsuche** oder **Einstellungen** > **Sucheinstellungen** > **Einstellungen für zeitgesteuerte Suche**.
4. Klicken Sie auf die Registerkarte **Aktion**.
5. Wählen Sie die folgenden Optionen:
   - **Bei Viren-/Malware-Fund eine Benachrichtigung auf dem Agent anzeigen**
   - **Bei vermutlichem Viren-/Malware-Fund eine Benachrichtigung auf dem Agent anzeigen**
6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Benachrichtigungen über Viren/Malware für OfficeScan Agents konfigurieren

Sie können den OfficeScan Agent so konfigurieren, dass Endbenutzer über das Ergebnis des Versuchs, eine Bedrohung durch Viren/Malware zu säubern oder in Quarantäne zu verschieben, benachrichtigt werden.

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Agent**.
2. Wählen Sie im Listenfeld **Typ** die Option **Viren/Malware** aus.
3. Konfigurieren Sie die Einstellungen zur Erkennung.
   a. Wählen Sie, ob Sie eine Benachrichtigung für alle Ereignisse, die von Viren/Malware stammen, oder je nach Schweregrad getrennte Benachrichtigungen anzeigen möchten:
      - **Hoch**: Der OfficeScan Agent konnte gefährliche Malware nicht beseitigen.
      - **Mittel**: Der OfficeScan Agent konnte Malware nicht beseitigen.
      - **Niedrig**: Der OfficeScan Agent konnte alle Bedrohungen beseitigen.

   b. übernehmen Sie die Standardmeldungen, oder ändern Sie sie.
4. Klicken Sie auf **Speichern**.

Spyware-/Grayware-Benachrichtigungen konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Agent**.
2. Wählen Sie im Listenfeld **Typ** die Option **Spyware/Grayware** aus.
3. Übernehmen Sie die Standardmeldung oder ändern Sie sie.
4. Klicken Sie auf **Speichern**.

Agents benachrichtigen, wenn der Computer zum Säubern infizierter Dateien neu gestartet werden muss

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Navigieren Sie auf der Registerkarte **Andere Einstellungen** zum Bereich **Aufforderung zum Neustart**.
5. Wählen Sie **Eine Benachrichtigung anzeigen, wenn der Endpunkt zum Säubern infizierter Dateien neu gestartet werden muss**.
6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Sicherheitsrisiko-Protokolle

Wenn OfficeScan Viren/Malware oder Spyware/Grayware findet oder Spyware/Grayware wiederherstellt, werden Protokolle erstellt.

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell, oder konfigurieren Sie eine zeitgesteuerte Löschung der Protokolle. Weitere Informationen zur Protokollverwaltung finden Sie unter *Protokollmanagement auf Seite 14-47*.

Viren-/Malware-Protokolle anzeigen

Der OfficeScan Agent erstellt Protokolle, wenn er Viren und Malware entdeckt, und sendet die Protokolle an den Server.

Prozedur

1. Navigieren Sie zu einer der folgenden Optionen:
   - **Protokolle** > **Agents** > **Sicherheitsrisiken**
   - **Agents** > **Agent-Verwaltung**
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Navigieren Sie zum Fenster **Kriterien für Viren-/Malware-Protokolle**:
   - Klicken Sie im Fenster **Sicherheitsrisiko-Protokolle** auf **Protokolle anzeigen** > **Viren-/Malware-Protokolle**.
   - Klicken Sie im Fenster **Agent-Verwaltung** auf **Protokolle** > **Viren-/Malware-Protokolle**.

4. Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.

5. Sehen Sie die Protokolle ein. Die Protokolle enthalten die folgenden Informationen:

VORGANG	BESCHREIBUNG
Datum/Uhrzeit	Zeitpunkt der Erkennung
Endpunkt	Endpunkt, auf dem die Erkennung erfolgte
Sicherheitsbedrohung	Der Name der Sicherheitsbedrohung
Infektionskanal	Der Kanal, aus dem die Bedrohung stammt
Infizierte(s) Datei/Objekt	Der Speicherort der Datei/des Objekts auf dem Endpunkt
Suchtyp	Die Suche, bei der die Bedrohung erkannt wurde
Ergebnis	Ergebnis der durchgeführten Aktion **Hinweis** Weitere Informationen zu Suchergebnissen finden Sie unter *Viren-/Malware-Suchergebnisse auf Seite 7-103*.
IP-Adresse	IP-Adresse und Portnummer des Quellendpunkts
MAC-Adresse	Die MAC-Adresse des infizierten Endpunkts
Details	Ein Link, der die detaillierte Analyse für eine bestimmte Erkennung anzeigt

6. Wenn Sie Protokolle als kommagetrennte Datei (CSV-Datei) speichern möchten, klicken Sie auf **Alle in CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

   Diese CSV-Datei enthält die folgenden Informationen:

   - Alle Informationen in den Protokollen

- Name des Benutzers, der zum Zeitpunkt des Fundes am Endpunkt angemeldet ist

Viren-/Malware-Suchergebnisse

Die folgenden Suchergebnisse werden in den Viren-/Malware-Protokollen angezeigt:

TABELLE 7-26. Suchergebnis

ERGEBNIS	BESCHREIBUNG
Gelöscht	• Die erste Aktion ist „Löschen“, und die infizierte Datei wurde gelöscht. • Die erste Aktion ist „Säubern“, aber die Säuberung ist fehlgeschlagen. Die zweite Aktion ist „Löschen“, und die infizierte Datei wurde gelöscht.
In Quarantäne verschoben	• Die erste Aktion ist „Quarantäne“, und die infizierte Datei wurde in Quarantäne verschoben. • Die erste Aktion ist „Säubern“, aber die Säuberung ist fehlgeschlagen. Die zweite Aktion ist „Quarantäne“, und die infizierte Datei wurde in Quarantäne verschoben.
Gesäubert	Eine infizierte Datei wurde gesäubert.
Umbenannt	• Die erste Aktion ist „Umbenennen“, und die infizierte Datei wurde umbenannt. • Die erste Aktion ist „Säubern“, aber die Säuberung ist fehlgeschlagen. Die zweite Aktion ist „Umbenennen“, und die infizierte Datei wurde umbenannt.
Zugriff verweigert	• Die erste Aktion ist „Zugriff verweigern“, und der Zugriff auf die infizierte Datei wurde verweigert, als der Benutzer versucht hat, die Datei zu öffnen. • Die erste Aktion ist „Säubern“, aber die Säuberung ist fehlgeschlagen. Die zweite Aktion ist „Zugriff verweigern“, und der Zugriff auf die infizierte Datei wurde verweigert, als der Benutzer versucht hat, die Datei zu öffnen. • "Wahrscheinlich Virus oder Malware" wurde während der Echtzeitsuche erkannt.

ERGEBNIS	BESCHREIBUNG
	• Die Echtzeitsuche verweigert den Zugriff auf Dateien, die mit einem Bootvirus infiziert sind, selbst wenn die Suchaktion „Säubern“ (erste Aktion) und „Quarantäne“ (zweite Aktion) ist. Der Grund ist, dass bei der Säuberung der MBR (Master Boot Record) des infizierten Endpunkts beschädigt werden könnte. Führen Sie eine manuelle Suche aus, damit OfficeScan die Datei säubern oder in Quarantäne verschieben kann.
Übergangen	• Die erste Aktion lautet „Übergehen“, deshalb hat OfficeScan keine Aktion für die infizierte Datei durchgeführt. • Die erste Aktion ist „Säubern“, aber die Säuberung ist fehlgeschlagen. Die zweite Aktion ist „Übergehen“, daher hat OfficeScan keine Aktion für die infizierte Datei durchgeführt.
Mögliches Sicherheitsrisiko übergangen	Dieses Suchergebnis wird nur angezeigt, wenn OfficeScan während der manuellen Suche, der zeitgesteuerten Suche und der Funktion "Jetzt durchsuchen" eine eventuelle Viren-/Malware-Infektion erkennt. Weitere Informationen über mögliche Viren/Malware und dazu, wie Sie verdächtige Dateien zur Analyse an Trend Micro senden können, finden Sie auf der folgenden Seite der Trend Micro Online Viren-Enzyklopädie. http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=POSSIBLE_VIRUS&VSect=Sn
Datei konnte nicht gesäubert oder in Quarantäne verschoben werden.	Die erste Aktion ist „Säubern“. Die zweite Aktion ist „Quarantäne“, und beide Aktionen sind fehlgeschlagen. Lösung: Siehe *Datei konnte nicht in Quarantäne verschoben/umbenannt werden auf Seite 7-105*.
Diese Datei konnte weder gesäubert noch gelöscht werden	Die erste Aktion ist „Säubern“. Die zweite Aktion ist „Löschen“, und beide Aktionen sind fehlgeschlagen. Lösung: Siehe *Datei konnte nicht gelöscht werden auf Seite 7-105*.
Datei konnte nicht gesäubert oder umbenannt werden.	Die erste Aktion ist „Säubern“. Die zweite Aktion ist „Umbenennen“, und beide Aktionen sind fehlgeschlagen. Lösung: Siehe *Datei konnte nicht in Quarantäne verschoben/umbenannt werden auf Seite 7-105*.

Ergebnis	Beschreibung
Datei konnte nicht in Quarantäne verschoben/ umbenannt werden	Erklärung 1 Die infizierte Datei ist unter Umständen von einer anderen Anwendung gesperrt, wird ausgeführt oder befindet sich auf einer CD. OfficeScan stellt die Datei unter Quarantäne oder benennt sie um, nachdem die Datei von der Anwendung freigegeben oder ausgeführt wurde. Lösung Bei infizierten Dateien auf einer CD sollten Sie die CD nicht verwenden, da der Virus andere Endpunkte im Netzwerk infizieren könnte.
	Erklärung 2 Die infizierte Datei befindet sich im Ordner "Temporary Internet Files" auf dem Agent-Endpunkt. Da der Endpunkt die Dateien während des Surfens im Internet herunterlädt, hat der Webbrowser die infizierte Datei möglicherweise gesperrt. Sobald er die Datei freigibt, verschiebt OfficeScan sie in Quarantäne oder benennt sie um. Lösung: Keine
Datei konnte nicht gelöscht werden	Erklärung 1 Die infizierte Datei befindet sich unter Umständen in einer komprimierten Datei und die Einstellung **Infizierte Dateien in komprimierten Dateien säubern/löschen** unter **Agents** > **Globale Agent-Einstellungen** auf der Registerkarte **Sicherheitseinstellungen** ist deaktiviert. Lösung Aktivieren Sie die Option **Infizierte Dateien in komprimierten Dateien säubern/löschen**. Bei Aktivierung dekomprimiert OfficeScan eine komprimierte Datei, säubert oder löscht infizierte Dateien innerhalb der komprimierten Datei und komprimiert die Datei anschließend neu.

ERGEBNIS	BESCHREIBUNG
	Hinweis Die Aktivierung dieser Einstellung kann zu einer erhöhten Nutzung der Endpunktressourcen während der Suche führen und die Suchdauer verlängern.
	Erklärung 2 Die infizierte Datei ist unter Umständen von einer anderen Anwendung gesperrt, wird ausgeführt oder befindet sich auf einer CD. OfficeScan löscht die Datei, nachdem die Datei von der Anwendung freigegeben oder ausgeführt wurde. Lösung Bei infizierten Dateien auf einer CD sollten Sie die CD nicht verwenden, da der Virus andere Endpunkte im Netzwerk infizieren könnte.
	Erklärung 3 Die infizierte Datei befindet sich im Ordner "Temporäre Internetdateien" auf dem OfficeScan Agent-Endpunkt. Da der Endpunkt die Dateien während des Surfens im Internet herunterlädt, hat der Webbrowser die infizierte Datei möglicherweise gesperrt. Sobald er die Datei freigibt, löscht OfficeScan sie. Lösung: Keine
Die Datei konnte nicht in den vorgesehenen Quarantäne-Ordner verschoben werden.	Obwohl OfficeScan eine Datei im Ordner `\Suspect` auf dem OfficeScan Agent-Endpunkt erfolgreich unter Quarantäne gestellt hat, kann sie nicht an das angegebene Quarantäneverzeichnis gesendet werden. Lösung Überprüfen Sie, bei welchem Suchtyp (manuelle Suche, Echtzeitsuche, zeitgesteuerte Suche oder "Jetzt durchsuchen") die Viren/die Malware entdeckt wurden, sowie das Quarantäneverzeichnis, das auf der Registerkarte **Agents** > **Agent-Verwaltung > Einstellungen** > **{Suchtyp}** > **Aktion** angegeben ist.

Ergebnis	Beschreibung
	Der Quarantäne-Ordner befindet sich auf dem OfficeScan Server-Computer oder auf einem anderen OfficeScan Server-Computer: 1. Überprüfen Sie die Verbindung zwischen agent und Server. 2. Bei Quarantäne-Ordnern im URL-Format: a. Vergewissern Sie sich, dass der nach `http://` angegebene Endpunktname korrekt ist. b. Überprüfen Sie die Größe der infizierten Datei. Überschreitet sie die unter **Administration** > **Einstellungen** > **Quarantäne-Manager** festgelegte maximale Dateigröße, passen Sie die Einstellung entsprechend an, damit die Datei gespeichert werden kann. Alternativ können Sie andere Aktionen, wie z. B. Löschen, ausführen. c. Überprüfen Sie, ob die Größe des Quarantäne-Ordners die unter **Administration** > **Einstellungen** > **Quarantäne-Manager** festgelegte Ordnergröße überschreitet. Sie können die Größe anpassen oder die Dateien im Quarantäne-Ordner manuell löschen. 3. Wenn Sie einen UNC-Pfad verwenden, stellen Sie sicher, dass der Quarantäne-Ordner für die Gruppe „Jeder“ freigegeben ist und dass Sie dieser Gruppe Lese- und Schreibberechtigungen zugewiesen haben. Stellen Sie außerdem sicher, dass der Quarantäne-Ordner vorhanden und der UNC-Pfad korrekt ist. Der Quarantäne-Ordner befindet sich auf einem anderen Endpunkt im Netzwerk (bei diesem Szenario können Sie den UNC-Pfad verwenden): 1. Überprüfen Sie, ob der OfficeScan Agent eine Verbindung zum Endpunkt herstellen kann. 2. Stellen Sie sicher, dass der Quarantäne-Ordner für die Gruppe „Jeder“ freigegeben ist, und dass Sie dieser Gruppe Lese- und Schreibberechtigungen zugewiesen haben. 3. Überprüfen Sie, ob der Quarantäne-Order vorhanden ist. 4. Überprüfen Sie, ob der UNC-Pfad korrekt ist. Wenn sich das Quarantäneverzeichnis in einem anderen Verzeichnis auf dem OfficeScan Agent-Endpunkt befindet (Sie

ERGEBNIS	BESCHREIBUNG
	können nur den absoluten Pfad für dieses Szenario verwenden), überprüfen Sie, ob das Quarantäneverzeichnis vorhanden ist.
Die Datei konnte nicht gesäubert werden	Erklärung 1 Die infizierte Datei befindet sich unter Umständen in einer komprimierten Datei und die Einstellung „Infizierte Dateien in komprimierten Dateien säubern/löschen“ unter **Agents** > **Globale Agent-Einstellungen** auf der Registerkarte **Sicherheitseinstellungen** ist deaktiviert. Lösung Aktivieren Sie die Option **Infizierte Dateien in komprimierten Dateien säubern/löschen**. Bei Aktivierung dekomprimiert OfficeScan eine komprimierte Datei, säubert oder löscht infizierte Dateien innerhalb der komprimierten Datei und komprimiert die Datei anschließend neu. **Hinweis** Die Aktivierung dieser Einstellung kann zu einer erhöhten Nutzung der Endpunktressourcen während der Suche führen und die Suchdauer verlängern.
	Erklärung 2 Die infizierte Datei befindet sich im Ordner `Temporäre Internetdateien` auf dem OfficeScan Agent-Endpunkt. Da der Endpunkt die Dateien während des Surfens im Internet herunterlädt, hat der Webbrowser die infizierte Datei möglicherweise gesperrt. Sobald er die Datei freigibt, säubert OfficeScan sie. Lösung: Keine
	Erklärung 3 Unter Umständen ist es nicht möglich, die Datei zu säubern. Weitere Informationen finden Sie unter *Dateien, die nicht gesäubert werden können auf Seite E-16*.
Aktion erforderlich	OfficeScan kann die konfigurierte Aktion für die infizierte Datei nicht ohne Eingreifen eines Benutzers abschließen. Bewegen Sie

ERGEBNIS	BESCHREIBUNG
	den Mauszeiger über die Spalte **Aktion erforderlich**, um die folgenden Details anzuzeigen. • „Aktion erforderlich – Wenden Sie sich an den Support, um Informationen zum Entfernen dieser Bedrohung mit dem Tool 'Clean Boot' aus dem in der OfficeScan ToolBox enthaltenen Anti-Threat Tool Kit zu erhalten.“ • „Aktion erforderlich – Wenden Sie sich an den Support, um Informationen zum Entfernen dieser Bedrohung mit dem Tool 'Rescue Disk' aus dem in der OfficeScan ToolBox enthaltenen Anti-Threat Tool Kit zu erhalten.“ • „Aktion erforderlich – Wenden Sie sich an den Support, um Informationen zum Entfernen dieser Bedrohung mit dem Tool 'Rootkit-Buster' aus dem in der OfficeScan ToolBox enthaltenen Anti-Threat Tool Kit zu erhalten.“ • „Aktion erforderlich – OfficeScan hat eine Bedrohung auf einem infizierten Agent entdeckt. Starten Sie den Endpunkt neu, um die Entfernung der Sicherheitsbedrohung abzuschließen.“ • „Aktion erforderlich – Ein vollständiger Systemscan ist erforderlich, um eine erkannte Rootkit-Bedrohung endgültig vom Endpunkt zu entfernen.“

Protokolle der zentralen Quarantänewiederherstellung anzeigen

Nach dem Säubern von Malware sichern die OfficeScan Agents die Malware-Daten. Weisen Sie einen Online-Agent an, die gesicherten Daten wiederherzustellen, wenn Sie die Daten als harmlos einstufen. In den Protokollen werden Informationen darüber aufgeführt, welche Malware-Sicherungsdaten wiederhergestellt wurden, welcher Endpunkt betroffen ist und wie das Ergebnis der Wiederherstellung war.

Prozedur

1. Navigieren Sie zu **Protokolle** > **Agents** > **Zentrale Quarantänewiederherstellung**.

2. Überprüfen Sie in den Spalten **Erfolgreich**, **Fehlgeschlagen** und **Ausstehend**, ob OfficeScan die Daten in Quarantäne wiederhergestellt hat.

3. Klicken Sie auf die Zähler-Links in jeder Spalte, um detaillierte Informationen zu jedem betroffenen Endpunkt anzuzeigen.

   Hinweis

   Für Wiederherstellungen mit dem Status **Fehlgeschlagen** können Sie versuchen, die Datei im Fenster **Details der zentralen Quarantänewiederherstellung** erneut wiederherzustellen, indem Sie auf **Alle wiederherstellen** klicken.

4. Wenn Sie das Protokoll als komma-separierte Datei im CSV-Format speichern möchten, klicken Sie auf **In CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Spyware/Grayware-Protokolle anzeigen

Der OfficeScan Agent generiert Protokolle, nachdem Spyware und Grayware erkannt wurde und sendet die Protokolle dann an den Server.

Prozedur

1. Navigieren Sie zu einer der folgenden Optionen:
   - **Protokolle** > **Agents** > **Sicherheitsrisiken**
   - **Agents** > **Agent-Verwaltung**
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Navigieren Sie zum Fenster **Kriterien für Spyware-/Grayware-Protokolle**:
   - Klicken Sie im Fenster **Sicherheitsrisiko-Protokolle** auf **Protokolle anzeigen** > **Spyware-/Grayware-Protokolle**.
   - Klicken Sie im Fenster **Agent-Verwaltung** auf **Protokolle** > **Spyware-/Grayware-Protokolle**.

4. Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.

5. Sehen Sie die Protokolle ein. Die Protokolle enthalten die folgenden Informationen:

VORGANG	BESCHREIBUNG
Datum/Uhrzeit	Zeitpunkt der Erkennung
Endpunkt	Endpunkt, auf dem die Erkennung erfolgte
Spyware/Grayware	Der Name der Sicherheitsbedrohung
Suchtyp	Die Suche, bei der die Bedrohung erkannt wurde
Ergebnis	Ergebnis der durchgeführten Aktion **Hinweis** Weitere Informationen zu Suchergebnissen finden Sie unter *Spyware-/Grayware-Suchergebnis auf Seite 7-112*.
IP-Adresse	IP-Adresse und Portnummer des Quellendpunkts
MAC-Adresse	Die MAC-Adresse des infizierten Endpunkts
Details	Ein Link, der die detaillierte Analyse für eine bestimmte Erkennung anzeigt

6. (Optional) Wählen Sie alle Spyware-/Grayware-Funde aus, die Sie als harmlos erachten, und klicken Sie auf **Zur Liste der zulässigen Programme hinzufügen**, um das Programm von der weiteren Suche auszuschließen.

7. Wenn Sie Protokolle als kommagetrennte Datei (CSV-Datei) speichern möchten, klicken Sie auf **Alle in CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

   Diese CSV-Datei enthält die folgenden Informationen:

   - Alle Informationen in den Protokollen

- Name des Benutzers, der zum Zeitpunkt des Fundes am Endpunkt angemeldet ist

Spyware-/Grayware-Suchergebnis

Die folgenden Suchergebnisse werden in den Spyware-/Grayware-Protokollen angezeigt:

TABELLE 7-27. Spyware-/Grayware-Suchergebnis auf erster Ebene

ERGEBNIS	BESCHREIBUNG
Erfolgreich, keine Aktion erforderlich	Das ist das Suchergebnis auf erster Ebene, wenn die Suchaktion erfolgreich war. Das Suchergebnis auf zweiter Ebene kann wie folgt aussehen: • *Gesäubert* • *Zugriff verweigert*
Weitere Aktionen erforderlich	Das ist das Suchergebnis auf erster Ebene, wenn die Suchaktion erfolglos war. Die Ergebnisse der zweiten Ebene enthalten mindestens eine der folgenden Benachrichtigungen: • *Übergangen* • *Spyware/Grayware kann in geschützten Systemdateien nicht gelöscht werden.* • *Suche nach Spyware/Grayware wurde manuell beendet. Führen Sie eine vollständige Suche durch.* • *Spyware/Grayware gesäubert. Neustart erforderlich. Starten Sie den Computer neu* • *Spyware/Grayware kann nicht gesäubert werden.* • *Unbekanntes Spyware-/Grayware-Suchergebnis. Wenden Sie sich an den technischen Support von Trend Micro*

TABELLE 7-28. Spyware-/Grayware-Suchergebnis auf zweiter Ebene

ERGEBNIS	BESCHREIBUNG	LÖSUNG
Gesäubert	OfficeScan beendet Prozesse oder löscht Registrierungseinträge, Dateien, Cookies und Verknüpfungen.	n. v.
Zugriff verweigert	OfficeScan hat den Zugriff (Kopieren, Öffnen) auf die entdeckten Spyware-/Grayware-Komponenten verweigert.	n. v.
Übergangen	OfficeScan hat keine Aktion durchgeführt, aber den Spyware-/Grayware-Fund zur späteren Auswertung protokolliert.	Fügen Sie der Liste der zugelassenen Spyware/Grayware die Spyware/Grayware hinzu, die Sie als harmlos erachten.
Spyware/Grayware kann in geschützten Systemdateien nicht gelöscht werden.	Mit dieser Meldung werden Sie informiert, ob die Spyware Scan Engine versucht, einen einzelnen Ordner zu löschen, und ob die folgenden Kriterien erfüllt sind: • Die zu säubernden Elemente sind größer als 250 MB. • Die Dateien im Ordner werden vom Betriebssystem verwendet. Der Ordner ist möglicherweise für den normalen Systembetrieb erforderlich. • Es handelt sich bei dem Ordner um ein Stammverzeichnis (wie z. B. `C:` oder `F:`).	Wenden Sie sich an Ihren Support-Anbieter.
Suche nach Spyware/Grayware wurde manuell beendet. Führen Sie eine vollständige Suche durch.	Ein Benutzer hat die Suche vor Abschluss beendet.	Führen Sie eine manuelle Suche aus, und warten Sie, bis die Suche abgeschlossen ist.

Ergebnis	Beschreibung	Lösung
Spyware/Grayware gesäubert. Neustart erforderlich. Starten Sie den Computer neu	OfficeScan hat die Spyware-/Grayware-Komponenten gelöscht. Um den Vorgang abzuschließen, ist ein Neustart des Endpunkts erforderlich.	Starten Sie den Endpunkt umgehend neu.
Spyware/Grayware kann nicht gesäubert werden.	Spyware/Grayware wurde auf einer CD-ROM oder einem Netzlaufwerk erkannt. OfficeScan kann an diesem Speicherort erkannte Spyware/Grayware nicht löschen.	Entfernen Sie die infizierte Datei manuell.
Unbekanntes Spyware-/Grayware-Suchergebnis. Wenden Sie sich an den technischen Support von Trend Micro	Eine neue Version der Spyware-Scan-Engine stellt ein neues Suchergebnis bereit, für dessen Umgang OfficeScan nicht konfiguriert wurde.	Wenden Sie sich an Ihren Support-Anbieter, um weitere Informationen zu erhalten.

Spyware-/Grayware-Wiederherstellungsprotokolle anzeigen

Nach dem Säubern von Spyware/Grayware sichern die OfficeScan Agents die Spyware-/Grayware-Daten. Benachrichtigen Sie einen Online-agent, die gesicherten Daten wiederherzustellen, wenn Sie die Daten als harmlos einstufen. In den Protokollen werden Informationen darüber aufgeführt, welche Spyware-/Grayware-Sicherungsdaten wiederhergestellt wurden, welcher Endpunkt betroffen und wie das Ergebnis der Wiederherstellung war.

Prozedur

1. Navigieren Sie zu **Protokolle** > **Agents** > **Spyware/Grayware-Wiederherstellung**.

2. Überprüfen Sie in der Spalte **Ergebnisse**, ob die Spyware-/Grayware-Daten von OfficeScan wiederhergestellt wurden.

3. Wenn Sie das Protokoll als komma-separierte Datei im CSV-Format speichern möchten, klicken Sie auf **In CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Protokolle zu verdächtigen Dateien anzeigen

Der OfficeScan Agent erstellt Protokolle, wenn er Dateien in der Liste der verdächtigen Dateien erkennt, und sendet die Protokolle an den Server.

Prozedur

1. Navigieren Sie zu einer der folgenden Optionen:
   - **Protokolle** > **Agents** > **Sicherheitsrisiken**
   - **Agents** > **Agent-Verwaltung**
2. Klicken Sie in der agent-Hierarchie auf das Stammsymbol ( ), um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
3. Klicken Sie auf **Protokolle** > **Protokolle zu verdächtigen Dateien** oder auf **Protokolle anzeigen** > **Protokolle zu verdächtigen Dateien**.
4. Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.
5. Sehen Sie die Protokolle ein. Die Protokolle enthalten die folgenden Informationen:
   - Datum und Uhrzeit des Funds verdächtiger Dateien
   - Endpunkt
   - Domäne
   - Infektionsquelle SHA-1-Hash-Wert der Datei
   - Dateipfad
   - Suchtyp, der die verdächtige Datei entdeckt hat

- Suchergebnis

  Hinweis

  Weitere Informationen zu Suchergebnissen finden Sie unter *Viren-/Malware-Suchergebnisse auf Seite 7-103*.

- IP-Adresse

Protokolle zu Suchvorgängen anzeigen

Wenn die manuelle Suche, die zeitgesteuerte Suche oder die Funktion "Jetzt durchsuchen" ausgeführt wird, erstellt der OfficeScan Agent ein Protokoll, das Informationen zur Suche enthält. über den OfficeScan Server oder die OfficeScan Agent-Konsolen können Sie das Suchprotokoll anzeigen.

Navigieren Sie zu einem der folgenden Speicherorte, um die Protokolle zu Suchvorgängen auf dem OfficeScan Server anzuzeigen:

- **Protokolle** > **Agents** > **Sicherheitsrisiken**. Klicken Sie dann auf **Protokolle anzeigen** > **Protokolle zu Suchvorgängen**
- **Agents** > **Agent-Verwaltung** und klicken Sie auf **Protokolle** > **Protokolle zu Suchvorgängen**

Die Protokolle zu Suchvorgängen enthalten die folgenden Informationen:

- Datum und Zeitpunkt, zu dem OfficeScan die Suche startet
- Datum und Zeitpunkt, zu dem OfficeScan die Suche beendet
- Suchstatus
  - **Abgeschlossen**: Die Suche wurde normal abgeschlossen.
  - **Unterbrochen**: Der Benutzer hat die Suche vor dem Abschluss beendet.
  - **Unerwartet beendet**: Die Suche wurde vom Benutzer, dem System oder einem unerwarteten Ereignis unterbrochen. Beispiel: Der Benutzer hat möglicherweise den Neustart des Endpunkts erzwungen oder der OfficeScan Echtzeitsuchdienst wurde unerwartet beendet.

- Suchtyp
- Anzahl der durchsuchten Objekte
- Anzahl der infizierten Viren-/Malware-Funde
- Anzahl der Spyware-/Grayware-Funde
- Version der Agent-Pattern-Datei der intelligenten Suche
- Version der Viren-Pattern-Datei
- Version des Spyware-/Grayware-Patterns

Ausbrüche von Sicherheitsrisiken

Ein Ausbruch wird angenommen, wenn die Anzahl der erkannten Viren-/Malware-, Spyware-/Grayware- oder Freigabeordner-Vorfälle über einen bestimmten Zeitraum einen bestimmten Schwellenwert überschreitet. Es gibt mehrere Möglichkeiten, um auf Ausbrüche im Netzwerk zu reagieren und sie einzudämmen. Dazu gehören folgende Maßnahmen:

- OfficeScan ermöglichen, das Netzwerk hinsichtlich verdächtiger Aktivitäten zu überwachen
- Besonders wichtige Ports und Ordner auf agent Endpunkt sperren
- Ausbruchswarnungen senden an agents
- Infizierte Endpunkte bereinigen Endpunkte

Ausbruchskriterien und Benachrichtigungen bei Sicherheitsrisiko

Konfigurieren Sie OfficeScan so, dass Sie oder andere OfficeScan Administratoren bei jedem Ausbruch eine Benachrichtigung erhalten.

TABELLE 7-29. Typen von Sicherheitsrisiko-Ausbruchsbenachrichtigungen

TYP	NACHSCHLAGEWERKE
• Viren-/Malware-Ausbruch • Spyware-/Grayware-Ausbruch • Ausbruch bei Freigabesitzung	*Ausbruchskriterien und Benachrichtigungen für Sicherheitsrisiken konfigurieren auf Seite 7-119*
Ausbruch von Firewall-Verstößen	*Kriterien für den Ausbruch von Verstößen gegen die Firewall und Benachrichtigungen konfigurieren auf Seite 13-35*
C&C-Callback-Ausbrüche	*C&C-Callback-Ausbruchskriterien und -Benachrichtigungen konfigurieren auf Seite 12-21*

Ein Ausbruch wird durch die Anzahl der Vorfälle in einem bestimmten Zeitraum definiert. OfficeScan löst eine Ausbruchswarnung aus, wenn die Anzahl der Funde während des Erkennungszeitraums den konfigurierten Wert überschreitet.

OfficeScan verfügt über zahlreiche Standardbenachrichtigungen, die Sie und andere OfficeScan Administratoren über Ausbrüche informieren. Sie können diese Benachrichtigungen ändern und nach Bedarf zusätzliche Benachrichtigungseinstellungen konfigurieren.

Hinweis

OfficeScan kann Benachrichtigungen über Sicherheitsrisiko-Ausbrüche per E-Mail, SNMP-Trap und Windows NT Ereignisprotokolle senden. Bei Ausbrüchen im Verlauf von Freigabesitzungen sendet OfficeScan Benachrichtigungen per E-Mail. Konfigurieren Sie die Einstellungen, wenn OfficeScan über diese Kanäle Benachrichtigungen versendet.

Weitere Informationen finden Sie unter *Einstellungen für die Administratorbenachrichtigungen auf Seite 14-43*.

Ausbruchskriterien und Benachrichtigungen für Sicherheitsrisiken konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Ausbruch**.
2. Auf der Registerkarte **Kriterien**:
   a. Gehen Sie zum Abschnitt **Viren/Malware** oder **Spyware/Grayware**:
   b. Geben Sie die Anzahl der eindeutigen Quellen der Vorfälle an.
   c. Geben Sie für jedes Sicherheitsrisiko die Anzahl der Vorfälle und den Entdeckungszeitraum an.

   Tipp
   Trend Micro empfiehlt, die Standardeinstellungen in diesem Fenster zu übernehmen.

   OfficeScan sendet die Benachrichtigung, wenn innerhalb von 5 Stunden 10 verschiedene Viren-/Malware-Typen entdeckt und insgesamt 101 Sicherheitsrisiken gemeldet wurden. Wenn ein Agent innerhalb von 5 Stunden 101 Sicherheitsrisiken aufgrund von irgendeinem Viren-/Malware-Typ meldet, sendet OfficeScan ebenfalls eine Ausbruchsbenachrichtigung.
3. Auf der Registerkarte **Kriterien**:
   a. Gehen Sie zum Abschnitt **Freigabesitzungen**.
   b. Wählen Sie **Freigabesitzungen im Netzwerk überwachen** aus.
   c. Klicken Sie unter **Freigabesitzungen aufgezeichnet** auf den Link mit der Anzahl, um die Endpunkte mit Freigabeordnern und die Endpunkte, die auf Freigabeordner zugreifen, anzuzeigen.
   d. Geben Sie die Anzahl der Freigabesitzungen und den Entdeckungszeitraum an.

   OfficeScan sendet eine Benachrichtigung, wenn die Anzahl der Freigabesitzungen überschritten wird.

4. Auf der Registerkarte **E-Mail**:

   a. Gehen Sie zu den Abschnitten **Viren-/Malware-Ausbrüche**, **Spyware-/Grayware-Ausbrüche** oder **Ausbrüche von Freigabesitzungen**.

   b. Wählen Sie **Benachrichtigung über E-Mail aktivieren**.

   c. Bestimmen Sie die Empfänger der E-Mail.

   d. Übernehmen oder ändern Sie die Standardbetreffzeile und -nachricht. Sie können Token-Variablen als Platzhalter für Daten in den Feldern **Betreff** und **Nachricht** verwenden.

TABELLE 7-30. Token-Variablen für Benachrichtigungen bei einem Ausbruch von Sicherheitsrisiken

VARIABLE	BESCHREIBUNG
Viren-/Malware-Ausbrüche	
%CV	Anzahl entdeckter Viren/Malware (gesamt)
%CC	Anzahl aller Endpunkte mit Viren/Malware (gesamt)
Spyware-/Grayware-Ausbrüche	
%CV	Anzahl entdeckter Spyware/Grayware (gesamt)
%CC	Anzahl aller Endpunkte mit Spyware/Grayware (gesamt)
Ausbrüche bei Freigabesitzungen	
%S	Anzahl der Freigabesitzungen
%T	Zeitraum, in dem Freigabesitzungen auftraten
%M	Zeitraum in Minuten

   e. Wählen Sie weitere Viren-/Malware- und Spyware-/Grayware-Informationen, die in der E-Mail enthalten sein sollen. Sie können den Namen des agents/der Domäne, den Namen des Sicherheitsrisikos, Datum und Uhrzeit der Erkennung, Pfad und infizierte Datei und das Suchergebnis einfügen.

   f. Den Standardtext der Benachrichtigungen akzeptieren oder ändern.

5. Auf der Registerkarte **SNMP-Trap**:

   a. Gehen Sie zu den Abschnitten **Viren-/Malware-Ausbrüche** oder **Spyware-/Grayware-Ausbrüche**.

   b. Wählen Sie **Benachrichtigung per SNMP-Trap aktivieren**.

   c. Übernehmen Sie die Standardmeldung oder ändern Sie sie. Sie können Token-Variablen als Platzhalter für Daten im Feld **Nachricht** verwenden. Weitere Informationen finden Sie unter *Tabelle 7-30: Token-Variablen für Benachrichtigungen bei einem Ausbruch von Sicherheitsrisiken auf Seite 7-120*.

6. Auf der Registerkarte **NT-Ereignisprotokoll**:

   a. Gehen Sie zu den Abschnitten **Viren-/Malware-Ausbrüche** oder **Spyware-/Grayware-Ausbrüche**.

   b. Wählen Sie **Benachrichtigung über NT-Ereignisprotokoll aktivieren**.

   c. Übernehmen Sie die Standardmeldung oder ändern Sie sie. Sie können Token-Variablen als Platzhalter für Daten im Feld **Nachricht** verwenden. Weitere Informationen finden Sie unter *Tabelle 7-30: Token-Variablen für Benachrichtigungen bei einem Ausbruch von Sicherheitsrisiken auf Seite 7-120*.

7. Klicken Sie auf **Speichern**.

Ausbruchsprävention bei Sicherheitsrisiken konfigurieren

Setzen Sie bei einem Ausbruch die Maßnahmen zur Ausbruchsprävention ein, um auf den Ausbruch zu reagieren und ihn einzudämmen. Konfigurieren Sie die Präventionseinstellungen, weil eine falsche Konfiguration unvorhergesehene Netzwerkprobleme mit sich bringt.

Prozedur

1. Navigieren Sie zu **Agents** > **Ausbruchsprävention**.

2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.

3. Klicken Sie auf **Ausbruchsprävention starten**.

4. Klicken Sie auf eine der folgenden Richtlinien für die Ausbruchsprävention und konfigurieren Sie dann die Einstellungen für die Richtlinie:

   - *Zugriff auf Freigabeordner einschränken/verweigern auf Seite 7-123*
   - *Gefährdete Ports sperren auf Seite 7-124*
   - *Schreibzugriff auf Dateien und Ordner verweigern auf Seite 7-126*
   - *Zugriff auf ausführbare komprimierte Dateien verweigern auf Seite 7-128*
   - *Mutex-Behandlung von Malware-Prozessen/-Dateien auf Seite 7-127*

5. Wählen Sie aus, welche Richtlinien durchgesetzt werden sollen.

6. Legen Sie fest, wie viele Stunden die Ausbruchsprävention aktiviert bleiben soll. Der Standardwert ist 48 Stunden. Sie können die Netzwerkeinstellungen vor dem Ablauf der Ausbruchsprävention manuell wiederherstellen.

   Warnung!

   Sie sollten keine zeitlich unbegrenzte Ausbruchsprävention zulassen. Wenn Sie den Zugriff auf bestimmte Dateien, Ordner oder Ports für unbegrenzte Zeit sperren möchten, ändern Sie stattdessen die entsprechenden Endpunkt- und Netzwerkeinstellungen direkt mit OfficeScan.

7. Den Standardtext der agent-Benachrichtigungen akzeptieren oder ändern.

   Hinweis

   Um OfficeScan so zu konfigurieren, dass Sie bei einem Ausbruch benachrichtigt werden, navigieren Sie zu **Administration** > **Benachrichtigungen** > **Ausbruch**.

8. Klicken Sie auf **Ausbruchsprävention starten**.

   Die von Ihnen ausgewählten Maßnahmen zur Ausbruchsprävention werden in einem neuen Fenster angezeigt.

9. Wenn Sie sich wieder in der agent-Hierarchie befinden, überprüfen Sie den Inhalt der Spalte **Ausbruchsprävention**.

Ein Häkchen wird auf Endpunkten angezeigt, die Maßnahmen zur Ausbruchsprävention anwenden.

OfficeScan zeichnet die folgenden Ereignisse in den Systemereignisprotokollen auf:

- Serverereignisse (die die Ausbruchsprävention einleiten und agents auffordern, die Ausbruchsprävention einzuleiten)
- OfficeScan Agent-Ereignis (das die Ausbruchsprävention aktiviert)

Ausbruchpräventionsrichtlinien

Setzen Sie bei einem Ausbruch die folgenden Richtlinien durch:

- *Zugriff auf Freigabeordner einschränken/verweigern auf Seite 7-123*
- *Gefährdete Ports sperren auf Seite 7-124*
- *Schreibzugriff auf Dateien und Ordner verweigern auf Seite 7-126*
- *Zugriff auf ausführbare komprimierte Dateien verweigern auf Seite 7-128*
- *Mutex-Behandlung von Malware-Prozessen/-Dateien auf Seite 7-127*

Zugriff auf Freigabeordner einschränken/verweigern

Bei einem Ausbruch können Sie den Zugriff auf Freigabeordner im Netzwerk einschränken oder verweigern, um die Ausbreitung von Sicherheitsrisiken über die Freigabeordner zu verhindern.

Wenn diese Richtlinie wirksam wird, können Benutzer weiterhin Ordner freigeben, aber die Richtlinie wird nicht auf die zuletzt freigegebenen Ordner angewendet. Aus diesem Grund sollten Sie die Benutzer darüber informieren, Ordner nicht während eines Ausbruchs freizugeben, oder verteilen Sie die Richtlinie erneut, damit sie auf die zuletzt freigegebenen Ordner angewendet wird.

Prozedur

1. Navigieren Sie zu **Agents** > **Ausbruchsprävention**.

2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Ausbruchsprävention starten**.
4. Klicken Sie auf **Zugriff auf Freigabeordner einschränken/verweigern**.
5. Wählen Sie dazu eine der folgenden Optionen aus:
   - **Nur Lesezugriff**: Schränkt den Zugriff auf Freigabeordner ein
   - **Zugriff verweigern**

   Hinweis

   Die Konfiguration "Nur Lesezugriff" gilt nicht für Freigabeordner, die bereits über vollständigen Zugriff verfügen.
6. Klicken Sie auf **Speichern**.

   Das Fenster **Ausbruchsprävention – Einstellungen** wird wieder angezeigt.
7. Klicken Sie auf **Ausbruchsprävention starten**.

   Die von Ihnen ausgewählten Maßnahmen zur Ausbruchsprävention werden in einem neuen Fenster angezeigt.

Gefährdete Ports sperren

Sperren Sie bei Ausbrüchen gefährdete Ports, die von Viren/Malware für den Zugriff auf OfficeScan Agent-Endpunkte verwendet werden können.

Warnung!

Gehen Sie bei der Konfiguration der Einstellungen für die Ausbruchsprävention sorgfältig vor. Wenn Sie aktive Ports sperren, stehen Netzwerkdienste, die auf diese Ports zugreifen, nicht mehr zur Verfügung. Wenn Sie beispielsweise den vertrauenswürdigen Port sperren, kann OfficeScan während der Dauer des Ausbruchs nicht mit dem Agent kommunizieren.

Prozedur

1. Navigieren Sie zu **Agents** > **Ausbruchsprävention**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Ausbruchsprävention starten**.
4. Klicken Sie auf **Ports sperren**.
5. Wählen Sie aus, ob Sie den **Vertrauenswürdigen Port sperren** möchten.
6. Wählen Sie die Ports, die Sie sperren möchten, in der Spalte **Gesperrte Ports** aus.
   a. Enthält die Tabelle keine Ports, klicken Sie auf **Hinzufügen**. Wählen Sie im daraufhin angezeigten Fenster die Ports aus, die Sie sperren möchten, und klicken Sie auf **Speichern**.
      - **Alle Ports (inkl. ICMP)**: Sperrt alle Ports außer dem vertrauenswürdigen Port. Wenn auch der vertrauenswürdige Port gesperrt werden soll, aktivieren Sie das Kontrollkästchen "Vertrauenswürdigen Port sperren" im vorherigen Fenster.
      - **Bestimmte Ports**
        - **Häufig verwendete Ports**: Wählen Sie wenigstens eine Portnummer für OfficeScan, um die Einstellungen zum Sperren von Ports zu speichern.
        - **Von Trojanern häufig verwendete Ports**: Sperrt Ports, die häufig von Trojanern verwendet werden.
        - **Alle Portnummern zwischen 1 und 65535 oder ein Portbereich**: Alternativ können Sie die Richtung des zu sperrenden Datenverkehrs zusammen mit Kommentaren angeben, wie z. B. dem Grund für das Sperren der angegebenen Ports.
        - **Ping-Protokoll (ICMP ablehnen)**: Sperrt ausschließlich ICMP-Pakete, wie z. B. Ping-Anfragen.
   b. Klicken Sie auf die Portnummer, um die Einstellungen der/des gesperrten Ports zu bearbeiten.

c. Bearbeiten Sie im daraufhin angezeigten Fenster die Einstellungen, und klicken Sie auf **Speichern**.

d. Aktivieren Sie das Kontrollkästchen neben der Portnummer, und klicken Sie dann auf **Löschen**, um einen Port aus der Liste zu entfernen.

7. Klicken Sie auf **Speichern**.

   Das Fenster **Ausbruchsprävention – Einstellungen** wird wieder angezeigt.

8. Klicken Sie auf **Ausbruchsprävention starten**.

   Die von Ihnen ausgewählten Maßnahmen zur Ausbruchsprävention werden in einem neuen Fenster angezeigt.

Schreibzugriff auf Dateien und Ordner verweigern

Viren und Malware können Dateien und Ordner auf dem Host-Endpunkten ändern oder löschen. Mit OfficeScan können Sie während eines Ausbruchs verhindern, dass Viren oder Malware Dateien und Ordner auf OfficeScan Agent-Endpunkten ändern oder löschen.

Warnung!

Der Schreibzugriff kann für zugeordnete Netzwerklaufwerke von OfficeScan nicht verweigert werden.

Prozedur

1. Navigieren Sie zu **Agents** > **Ausbruchsprävention**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Ausbruchsprävention starten**.
4. Klicken Sie auf **Schreibzugriff auf Dateien und Ordner verweigern**.
5. Geben Sie den Verzeichnispfad ein. Wenn Sie den Verzeichnispfad eingegeben haben, der geschützt werden soll, klicken Sie auf **Hinzufügen**.

Hinweis

Geben Sie den absoluten und nicht den virtuellen Verzeichnispfad ein.

6. Geben Sie die zu schützenden Dateien in den geschützten Verzeichnissen an. Dazu können Sie alle Dateien oder nur Dateien mit bestimmten Erweiterungen auswählen. Um eine Erweiterung anzugeben, die nicht in der Liste enthalten ist, geben Sie diese in das Textfeld ein, und klicken Sie auf **Hinzufügen**.

7. Um bestimmte Dateien zu schützen, geben Sie unter **Diese Dateien schützen** die vollständigen Dateinamen an, und klicken Sie auf **Hinzufügen**.

8. Klicken Sie auf **Speichern**.

   Das Fenster **Ausbruchsprävention – Einstellungen** wird wieder angezeigt.

9. Klicken Sie auf **Ausbruchsprävention starten**.

   Die von Ihnen ausgewählten Maßnahmen zur Ausbruchsprävention werden in einem neuen Fenster angezeigt.

Mutex-Behandlung von Malware-Prozessen/-Dateien

Sie können die Ausbruchsprävention so konfigurieren, dass Schutz vor Sicherheitsbedrohungen geboten wird, die Mutex-Prozesse nutzen, indem Sie die Ressourcen außer Kraft setzen, die die Sicherheitsbedrohung zum Infizieren und zum Weiterverbreiten im gesamten System benötigt. Die Ausbruchsprävention erstellt gegenseitige Ausschlüsse für Dateien und Prozesse im Zusammenhang mit bekannter Malware. Dadurch wird der Zugriff der Malware auf diese Ressourcen verhindert.

Tipp

Trend Micro empfiehlt, diese Ausschlüsse beizubehalten, bis eine Lösung für die Malware-Bedrohung implementiert werden kann. Vom technischen Support erhalten Sie die korrekten Mutex-Namen, vor denen während eines Ausbruchs geschützt werden soll.

Hinweis

Die Mutex-Behandlung erfordert den Unauthorized Change Prevention Service und unterstützt nur 32-Bit-Plattformen.

Prozedur

1. Navigieren Sie zu **Agents** > **Ausbruchsprävention**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Ausbruchsprävention starten**.
4. Klicken Sie auf **Mutex-Behandlung von Malware-Prozessen/-Dateien**.
5. Geben Sie den Mutex-Namen, vor dem Schutz angeboten werden soll, in das entsprechende Textfeld ein.

   Mit Hilfe der Schaltflächen **+** und **-** können Sie Mutex-Namen in der Liste hinzufügen oder entfernen.

   Hinweis

   Die Ausbruchsprävention unterstützt die Mutex-Behandlung für maximal sechs Mutex-Bedrohungen.

6. Klicken Sie auf **Speichern**.

   Das Fenster **Ausbruchsprävention – Einstellungen** wird wieder angezeigt.

7. Klicken Sie auf **Ausbruchsprävention starten**.

   Die von Ihnen ausgewählten Maßnahmen zur Ausbruchsprävention werden in einem neuen Fenster angezeigt.

Zugriff auf ausführbare komprimierte Dateien verweigern

Wenn Sie während Virenausbrüchen den Zugriff auf ausführbare komprimierte Dateien verweigern, können damit einhergehende potenzielle Sicherheitsrisiken an der Verbreitung im Netzwerk gehindert werden. Sie können den Zugriff auf vertrauenswürdige Dateien zulassen, die mit den unterstützten Komprimierungsprogrammen für ausführbare Dateien erstellt wurden.

Prozedur

1. Navigieren Sie zu **Agents** > **Ausbruchsprävention**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Ausbruchsprävention starten**.
4. Klicken Sie auf **Zugriff auf ausführbare komprimierte Dateien verweigern**.
5. Wählen Sie eine der Optionen aus der Liste mit den unterstützten Komprimierungsprogrammen für ausführbare Dateien aus, und klicken Sie auf **Hinzufügen**, um den Zugriff auf ausführbare komprimierte Dateien, die mit diesen Komprimierungsprogrammen erstellt wurden, zuzulassen.

   Hinweis

   Sie können nur die Verwendung von komprimierten Dateien, die mit den aufgeführten Komprimierungsprogrammen für ausführbare Dateien erstellt wurden, zulassen. Die Ausbruchsprävention verweigert den Zugriff auf jedes andere ausführbare komprimierte Dateiformat.

6. Klicken Sie auf **Speichern**.

   Das Fenster **Ausbruchsprävention – Einstellungen** wird wieder angezeigt.

7. Klicken Sie auf **Ausbruchsprävention starten**.

   Die von Ihnen ausgewählten Maßnahmen zur Ausbruchsprävention werden in einem neuen Fenster angezeigt.

Ausbruchsprävention deaktivieren

Wenn Sie sicher sind, dass ein Ausbruch eingedämmt werden konnte und alle infizierten Dateien von OfficeScan gesäubert oder in Quarantäne verschoben wurden, können Sie die Netzwerkeinstellungen wieder auf "Normal" zurücksetzen, indem Sie die Ausbruchsprävention deaktivieren.

Prozedur

1. Navigieren Sie zu **Agents** > **Ausbruchsprävention**.
2. Klicken Sie in der agent-Hierarchie auf das Stammsymbol ( ), um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
3. Klicken Sie auf **Einstellungen wiederherstellen**.
4. Um die Benutzer über das Ende des Ausbruchs zu informieren, wählen Sie **Benutzer nach dem Wiederherstellen der ursprünglichen Einstellungen benachrichtigen**.
5. Den Standardtext der agent-Benachrichtigungen akzeptieren oder ändern.
6. Klicken Sie auf **Einstellungen wiederherstellen**.

   Hinweis

   Wenn Sie die Netzwerkeinstellungen nicht manuell wiederherstellen, stellt OfficeScan diese Einstellungen automatisch nach Ablauf der unter **Netzwerkeinstellungen automatisch auf Standard zurücksetzen nach __ Stunde(n)** im Fenster **Ausbruchsprävention – Einstellungen** festgelegten Anzahl von Stunden wieder her. Die Standardeinstellung beträgt 48 Stunden.

   OfficeScan zeichnet die folgenden Ereignisse in den Systemereignisprotokollen auf:

   - Serverereignisse (die die Ausbruchsprävention einleiten und OfficeScan Agents auffordern, die Ausbruchsprävention einzuleiten)
   - OfficeScan Agent-Ereignis (das die Ausbruchsprävention aktiviert)

7. Durchsuchen Sie nach dem Deaktivieren der Ausbruchsprävention Ihre Netzwerkendpunkte nach Sicherheitsrisiken, um sicherzustellen, dass der Ausbruch eingedämmt wurde.

Kapitel 8

Schutz vor unbekannten Bedrohungen

In diesem Kapitel wird der Schutz von Endpunkten vor unbekannten Bedrohungen, die versuchen, in das Netzwerk einzudringen, beschrieben.

Es werden folgende Themen behandelt:

- *Vorausschauendes Maschinenlernen auf Seite 8-2*
- *Verdächtiger Verbindungsdienst auf Seite 8-6*
- *Exemplar Zusendung auf Seite 8-11*
- *Protokolle unbekannter Bedrohungen auf Seite 8-12*

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 vorausschauenden 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 vorausschauenden 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 OfficeScan 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 vorausschauenden 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 OfficeScan Agent versuchen, die betroffene Datei unter „Quarantäne“ zu stellen, um zu verhindern, dass sich die Bedrohung im Netzwerk verbreitet.

FUNDTYP	BESCHREIBUNG
Prozess	Nach der Erkennung eines unbekannten oder selten vorkommenden Prozesses überwacht der OfficeScan 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 vorausschauenden Maschinenlernen das Prozessverhalten mit dem Modell verglichen, ein Wahrscheinlichkeitswert zugewiesen und der mögliche Malware-Typ ermittelt, der vom Prozess ausgeführt wird. Die Prozesserkennung überwacht auch die Ausführung des Skripts. Wenn die "Maschine für kontextbezogene Intelligenz" die Ausführung eines verdächtigen Skripts erkennt, führt die Funktion "Vorausschauendes Maschinenlernen" die konfigurierte Aktion durch. Die Funktion "Vorausschauendes Maschinenlernen" führt die Sperrung von Skripts für die folgenden Arten von Skripts durch: • Cscript • JAR • PowerShell • VBS • WScript Je nach Konfiguration der Funktion "Vorausschauendes Maschinenlernen" kann OfficeScan Agent den betroffenen Prozess oder das Skript „beenden“ und die Datei bereinigen, die den Prozess oder das Skript ausgeführt hat.

Konfigurieren der Einstellungen für "Vorausschauendes Maschinenlernen"

Hinweis

Folgende Dienste müssen für "Vorausschauendes Maschinenlernen" aktiviert werden:

- Schutz vor unbefugten Änderungen
- Erweiterter Schutzdienst

Weitere Informationen finden Sie unter *Die Agent-Dienste von der Webkonsole aus aktivieren oder deaktivieren auf Seite 15-8*.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für "Vorausschauendes Maschinenlernen"**.

   Das Fenster **Einstellungen für "Vorausschauendes Maschinenlernen"** wird angezeigt.
4. Wählen Sie **Vorausschauendes Maschinenlernen aktivieren** aus.
5. Wählen Sie unter **Erkennungseinstellungen** den Erkennungstyp und die zugehörige Aktion aus, die von "Vorausschauendes Maschinenlernen" durchgeführt wird.

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.
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.

6. Konfigurieren Sie unter **Ausnahmen** die globalen Dateiausnahmen für "Vorausschauendes Maschinenlernen", um alle Agents daran zu hindern, eine Datei als böswillig zu erkennen.

   a. Klicken Sie auf **Datei-Hash hinzufügen**.

      Das Fenster **Datei zur Ausnahmeliste hinzufügen** wird angezeigt.

b. Geben Sie den Datei-Hash SHA-1 an, um ihn vom Suchvorgang auszuschließen.

c. Stellen Sie optional eine Anmerkung mit dem Grund für die Ausnahme bereit oder beschreiben Sie die dem Hash-Wert zugeordneten Dateinamen.

d. Klicken Sie auf **Hinzufügen**.

Die Funktion "Vorausschauendes Maschinenlernen" fügt den Dateihash zur Ausnahmeliste hinzu.

7. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

- **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Verdächtiger Verbindungsdienst

Der Dienst für verdächtige Verbindungen verwaltet die benutzerdefinierten und globalen C&C-IP-Listen und überwacht das Verhalten von Verbindungen, die Endpunkte zu potenziellen C&C-Servern herstellen.

- Die benutzerdefinierten Listen mit zulässigen bzw. gesperrten IP-Adressen ermöglichen die weitere Kontrolle darüber, ob Endpunkte auf bestimmte IP-Adressen zugreifen können. Konfigurieren Sie diese Liste, wenn Sie den Zugriff auf eine Adresse zulassen möchten, die durch die globale C&C-IP-Liste gesperrt ist, oder wenn Sie den Zugriff auf eine Adresse sperren möchten, die mögliche Sicherheitsrisiken darstellt.

Weitere Informationen finden Sie unter *Globale Einstellungen für die benutzerdefinierte IP-Liste konfigurieren auf Seite 8-7*.

- Zusammen mit der Prüf-Engine für Netzwerkinhalte (Network Content Inspection Engine, NCIE) sorgt die globale C&C-IP-Liste dafür, dass Netzwerkverbindungen mit von Trend Micro bestätigten C&C-Servern erkannt werden. NCIE erkennt Kontakte mit C&C-Servern in allen Netzwerkkanälen. Der Verdächtige Verbindungsdienst protokolliert alle Daten der Verbindungen mit Servern in der Globalen C&C-IP-Liste, damit sie ausgewertet werden können.

  Weitere Informationen zum Aktivieren der Globalen C&C-IP-Liste finden Sie unter *Verdächtige Verbindungseinstellungen konfigurieren auf Seite 8-9*.

- Nach der Erkennung von Malware auf einem Endpunkt mit Hilfe des Abgleichs für das Pattern der Relevanzregel in Netzwerkpaketen kann der "Verdächtige Verbindungsdienst" das Verbindungsverhalten weiter analysieren, um festzustellen, ob ein C&C-Callback aufgetreten ist. Nach der Erkennung eines C&C-Callbacks kann der "Verdächtige Verbindungsdienst" versuchen, die Quelle der Verbindung mit Hilfe von GeneriClean-Technologie zu sperren und zu säubern.

  Weitere Informationen zum Konfigurieren des Diensts für verdächtige Verbindungen finden Sie unter *Verdächtige Verbindungseinstellungen konfigurieren auf Seite 8-9*.

  Weitere Informationen zu GeneriClean finden Sie unter *GeneriClean auf Seite E-5*.

Aktivieren Sie den "Verdächtigen Verbindungsdienst" im Fenster **Zusätzliche Diensteinstellungen**, um Agents vor C&C-Server-Callbacks zu schützen. Weitere Informationen finden Sie unter *Die Agent-Dienste von der Webkonsole aus aktivieren oder deaktivieren auf Seite 15-8*.

Globale Einstellungen für die benutzerdefinierte IP-Liste konfigurieren

Administratoren können OfficeScan so konfigurieren, dass alle Verbindungen zwischen Agents und benutzerdefinierten C&C-IP-Adressen zugelassen, gesperrt oder protokolliert werden.

Hinweis

Die benutzerdefinierten IP-Listen unterstützen nur IPv4-Adressen.

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Klicken Sie auf die Registerkarte **Sicherheitseinstellungen**.
3. Navigieren Sie zum Abschnitt **Verdächtige Verbindungseinstellungen**.
4. Klicken Sie auf **Benutzerdefinierte IP-Liste bearbeiten**.
5. Fügen Sie auf der Registerkarte **Liste 'Zulässig'** oder **Liste 'Gesperrt'** die IP-Adressen hinzu, die Sie überwachen möchten.

   Tipp

   Sie können OfficeScan so konfigurieren, dass nur Verbindungen zu Adressen in der benutzerdefinierten Liste mit gesperrten IP-Adressen protokolliert werden. Informationen, wie Sie nur Verbindungen zu Adressen in der benutzerdefinierten Liste mit gesperrten IP-Adressen protokollieren, finden Sie unter *Verdächtige Verbindungseinstellungen konfigurieren auf Seite 8-9*.

   a. Klicken Sie auf **Hinzufügen**.

   b. Geben Sie in dem nun angezeigten Fenster die IP-Adresse, den IP-Adressbereich oder die IPv4-Adresse und die Subnetzmaske ein, die von OfficeScan überwacht werden sollen.

   c. Klicken Sie auf **Speichern**.

6. Aktivieren Sie das Kontrollkästchen neben einer Adresse, und klicken Sie auf **Löschen**, um IP-Adressen aus der Liste zu entfernen.
7. Klicken Sie nach der Konfiguration der Listen auf **Schließen**, um zum Fenster **Globale Agent-Einstellungen** zurückzukehren.
8. Klicken Sie auf **Speichern**, um die aktualisierte Liste auf Agents zu verteilen.

Verdächtige Verbindungseinstellungen konfigurieren

OfficeScan Agents kann alle Verbindungen zwischen Endpunkten und Adressen in der globalen C&C-IP-Liste protokollieren und sperren. Sie können IP-Adressen protokollieren, die in der benutzerdefinierten Liste mit gesperrten IP-Adressen konfiguriert sind, aber dennoch den Zugriff auf diese IP-Adressen erlauben.

OfficeScan Agents kann außerdem Verbindungen überwachen, die das Ergebnis einer Botnet- oder sonstigen Malware-Bedrohung sind. Wenn eine Malware-Bedrohung erkannt wurde, kann OfficeScan Agents versuchen, die Infektion zu beseitigen.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Verdächtige Verbindungseinstellungen**.

   Das Fenster **Verdächtige Verbindungseinstellungen** wird angezeigt.
4. Aktivieren Sie die Einstellung **Netzwerkverbindungen mit Adressen in der globalen C&C-IP-Liste erkennen**, um Verbindungen zu von Trend Micro bestätigten C&C-Servern zu überwachen, und wählen Sie für Verbindungen die Option **Nur protokollieren** oder **Sperren** aus.
   - Aktivieren Sie die Einstellung **Zugriff auf benutzerdefinierte Liste mit gesperrten IP-Adressen zulassen und protokollieren**, um Agents den Zugriff auf Adressen in der benutzerdefinierten Liste mit gesperrten IP-Adressen zu erlauben.

Hinweis

Sie müssen die Protokollierung von Netzwerkverbindungen aktivieren, damit OfficeScan Agents den Zugriff auf Adressen in der benutzerdefinierten Liste mit gesperrten IP-Adressen zulassen kann.

Weitere Informationen über die Globale C&C-IP-Liste finden Sie unter *Verdächtiger Verbindungsdienst auf Seite 8-6*.

5. Aktivieren Sie **Verbindungen mit Malware-Fingerabdruck für Netzwerk erkennen** und wählen Sie für Verbindungen die Option **Nur protokollieren** oder **Sperren** aus.

   Die Funktion "Malware-Fingerabdruck für Netzwerk" führt einen Pattern-Abgleich für Paket-Header durch. OfficeScan Agents protokollieren mit Hilfe des Patterns der Relevanzregel alle Verbindungen, die von Paketen mit Headern hergestellt werden, die mit bekannten Malware-Bedrohungen übereinstimmen.

   - Aktivieren Sie die Einstellung **Verdächtige Verbindungen säubern, wenn ein C&C-Callback erkannt wird**, damit OfficeScan Agents versuchen kann, Verbindungen zu C&C-Servern zu bereinigen. OfficeScan Agents verwenden GeneriClean, um die Malware-Bedrohung zu bereinigen und die Verbindung zum C&C-Server zu unterbrechen.

   Hinweis

   Sie müssen Verbindungen mit **Malware-Fingerabdruck für Netzwerk protokollieren** aktivieren, damit OfficeScan Agents versuchen kann, die Verbindungen zu C&C-Servern zu säubern, die vom Paketstrukturabgleich erkannt wurden.

6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Exemplar Zusendung

Sie können OfficeScan Agents so konfigurieren, dass Dateiobjekte, die unter Umständen zuvor nicht erkannte Bedrohungen enthalten, zur weiteren Analyse an Virtual Analyzer weitergeleitet werden. Nach der Bewertung der Objekte fügt Virtual Analyzer alle Objekte, in denen unbekannte Bedrohungen gefunden wurden, zu den Virtual Analyzer-Listen mit verdächtigen Objekten hinzu und verteilt die Listen über das Netzwerk an andere OfficeScan Agents.

Weitere Informationen finden Sie unter *Einstellungen für Liste der verdächtigen Objekte auf Seite 14-38*.

Die Exemplar Zusendung benötigt Folgendes:

- Sie müssen den OfficeScan Server mit einem Trend Micro Control Manager Server (6.0 SP3 Patch 2 oder höher) registrieren.
- Der Trend Micro Control Manager muss über eine aktive Verbindung zu einem Trend Micro Deep Discovery Analyzer Server (5.1 oder höher) verfügen.

Zu den verdächtigen Dateien gehören:

- Programme, die Trend Micro nicht bekannt sind (heruntergeladen über unterstützte Webbrowser oder E-Mail-Kanäle)
- Heuristische Erkennungen von Prozessen (heruntergeladen über unterstützte Webbrowser oder E-Mail-Kanäle)
- Selten vorkommende, automatisch ausgeführte Programme auf Wechselmedien

Wichtig

OfficeScan Agents kann Beispieldateien mit einer maximalen Größe von 50 MB zu Analysezwecken an Virtual Analyzer übermitteln.

Konfigurieren der Exemplar Zusendung

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für die Exemplar Zusendung**.

   Das Fenster **Einstellungen für die Exemplar Zusendung** wird angezeigt.
4. Wählen Sie **Weiterleitung verdächtiger Dateien an Virtual Analyzer aktivieren** aus.
5. Klicken Sie auf **Speichern**.

Protokolle unbekannter Bedrohungen

OfficeScan Agents protokollieren unbekannte Bedrohungen und senden die Protokolle an den Server. Standardmäßig fasst ein OfficeScan Agent, der kontinuierlich läuft, die Protokolle zusammen und sendet sie in bestimmten Zeitabständen (standardmäßig alle 60 Minuten).

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell, oder konfigurieren Sie eine zeitgesteuerte Löschung der Protokolle. Weitere Informationen zur Protokollverwaltung finden Sie unter *Protokollmanagement auf Seite 14-47*.

Anzeigen von Protokolldaten für "Vorausschauendes Maschinenlernen"

Prozedur

1. Navigieren Sie zu einer der folgenden Optionen:
   - **Protokolle** > **Agents** > **Sicherheitsrisiken**
   - **Agents** > **Agent-Verwaltung**
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Navigieren Sie zum Fenster **Protokollkriterien für "Vorausschauendes Maschinenlernen"**:
   - Klicken Sie im Fenster **Sicherheitsrisiko-Protokolle** auf **Protokolle anzeigen** > **Protokolldaten für "Vorausschauendes Maschinenlernen"**.
   - Klicken Sie im Fenster **Agent-Verwaltung** auf **Protokolle** > **Protokolldaten für "Vorausschauendes Maschinenlernen"**.
4. Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.
5. Sehen Sie die Protokolle ein. Die Protokolle enthalten die folgenden Informationen:

VORGANG	BESCHREIBUNG
Datum/Uhrzeit	Zeitpunkt der Erkennung
Endpunkt	Endpunkt, auf dem die Erkennung erfolgte
IP-Adresse	IP-Adresse und Portnummer des Quellendpunkts
Sicherheitsbedrohung	Der Name der vom Modul für "Vorausschauendes Maschinenlernen" angegebenen Sicherheitsbedrohung
Ergebnis	Ergebnis der durchgeführten Aktion

Vorgang	Beschreibung
Infizierte(s) Datei/Objekt	Der Name des Dateiobjekts oder Programms, das den Prozess ausgeführt hat
Typ	Der Objekttyp, der die Erkennung („Datei“ oder „Prozess“) ausgelöst hat
Dateipfad	Der Pfad des Dateiobjekts oder Programms, das den Prozess ausgeführt hat
Infektionskanal	Der Kanal, aus dem die Bedrohung stammt
Details	Ein Link, der die detaillierte Analyse für eine bestimmte Erkennung anzeigt Weitere Informationen finden Sie unter *Details der Protokolldaten für "Vorausschauendes Maschinenlernen" auf Seite 8-14*.

6. Wenn Sie Protokolle als kommagetrennte Datei (CSV-Datei) speichern möchten, klicken Sie auf **Alle in CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Details der Protokolldaten für "Vorausschauendes Maschinenlernen"

Sie können einen ausführlichen Bericht für jede Erkennung im Protokoll für "Vorausschauendes Maschinenlernen" anzeigen, indem Sie in der Spalte **Details** auf die Verknüpfung **Anzeigen** klicken.

Das Fenster **Protokolldetails** besteht aus zwei Abschnitten:

- Oberes Banner: Bestimmte Informationen, die sich auf diese spezielle Protokollerkennung beziehen
- Steuerelemente der unteren Registerkarten: Details, die sich auf Bedrohungen durch "Vorausschauendes Maschinenlernen" beziehen, einschließlich Einschätzungen der Bedrohungsprobabilität, Dateiinformationen und anderer Endpunkte im Netzwerk mit derselben Erkennung

In der folgenden Tabelle werden die im oberen Banner bereitgestellten Informationen erläutert.

TABELLE 8-1. Protokolldetails - Oberes Banner

ABSCHNITT	BESCHREIBUNG
Zeitpunkt der Erkennung / Aktion	Gibt an, zu welchem Zeitpunkt die jeweilige Protokollerkennung stattgefunden hat und welche Maßnahmen vom Agent gegen die Bedrohung getroffen wurden.
Dateiname	Gibt den Namen der Datei an, die die Erkennung auf dem angegebenen Endpunkt ausgelöst hat. **Tipp** Klicken Sie auf **Zur Ausnahmeliste hinzufügen**, um den Hash-Wert der betroffenen Datei schnell zur globalen Ausnahmeliste für "Vorausschauendes Maschinenlernen" hinzuzufügen. Zeigen Sie die gesamte Liste im Fenster **Einstellungen für "Vorausschauendes Maschinenlernen"** an. Weitere Informationen finden Sie unter *Konfigurieren der Einstellungen für "Vorausschauendes Maschinenlernen" auf Seite 8-4*. **Wichtig** Der erkannte Dateiname für diese Erkennung stimmt unter Umständen nicht mit dem auf anderen Agents erkannten Dateinamen überein. Bei "Vorausschauendes Maschinenlernen" werden die Erkennungen nach den Hash-Werten der Dateien und nicht nach den Dateinamen zugeordnet. überprüfen Sie auf der Registerkarte **Betroffene Endpunkte** den Dateinamen auf anderen Endpunkten.
Endpunktinformationen	Zeigt den zum Zeitpunkt der Erkennung angemeldeten Benutzer, den Namen sowie die IP-Adresse des Endpunkts an.
Kanalinformationen	Zeigt den Ursprungskanal der Bedrohung und den Speicherort des Ordners auf dem Endpunkt an, an den die Bedrohung übertragen wurde.

In der folgenden Tabelle werden die auf den unteren Registerkarten bereitgestellten Informationen erläutert.

TABELLE 8-2. Protokolldetails - Registerkarteninformationen

REGISTERKARTEN	BESCHREIBUNG
Bedrohungsindikatoren	Stellt die Analyseergebnisse von "Vorausschauendes Maschinenlernen" bereit. • **Bedrohungsprobabilität**: Gibt die übereinstimmungsgenauigkeit zwischen der Datei/dem Prozess und dem Malware-Modell an. • **Wahrscheinliche Bedrohungsart**: Gibt die wahrscheinlichste in der Datei enthaltene Bedrohungsart an, nachdem die Analyse mittels "Vorausschauendes Maschinenlernen" mit anderen Bedrohungen verglichen wurde. • **Bedrohungsidentifikation**: Stellt eine Liste mit von der Datei/vom Prozess verwendeten API-Funktionen bereit, die auf die erkannte Bedrohungsart hinweisen können. **Wichtig** Die Identifizierung von API-Funktionen stellt nur einen Faktor bei der Bestimmung der Bedrohungsart dar. "Vorausschauendes Maschinenlernen" verwendet viele andere Dateifunktionen und Analysemethoden, um die Bedrohungsprobabilität und die wahrscheinliche Bedrohungsart zu berechnen. • **ähnliche bekannte Bedrohungen**: Stellt eine Liste bekannter Bedrohungsarten bereit, die ähnliche Datei-/Prozessfunktionen für die Erkennung aufweisen.
Dateidetails	Stellt allgemeine Informationen bereit, die sich auf die Dateieigenschaften und Zertifikatsinformationen für dieses spezielle Erkennungsprotokoll beziehen.
Betroffene Endpunkte	Zeigt eine Liste der anderen Agents im Netzwerk mit derselben Erkennung durch "Vorausschauendes Maschinenlernen" an und stellt bestimmte Details zu den Erkennungen auf den anderen Agents bereit.

Protokolle zu verdächtigen Verbindungen anzeigen

Prozedur

1. Navigieren Sie zu einer der folgenden Optionen:
   - **Protokolle** > **Agents** > **Sicherheitsrisiken**
   - **Agents** > **Agent-Verwaltung**
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Navigieren Sie zum Fenster **Kriterien für das Protokoll von verdächtigen Verbindungen**:
   - Klicken Sie im Fenster **Sicherheitsrisiko-Protokolle** auf **Protokolle anzeigen** > **Protokolle zu verdächtigen Verbindungen**.
   - Klicken Sie im Fenster **Agent-Verwaltung** auf **Protokolle** > **Protokolle zu verdächtigen Verbindungen**.
4. Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.
5. Sehen Sie die Protokolle ein. Die Protokolle enthalten die folgenden Informationen:

VORGANG	BESCHREIBUNG
Datum/Uhrzeit	Zeitpunkt der Erkennung
Endpunkt	Endpunkt, auf dem die Erkennung erfolgte
Domäne	Domäne des Endpunkts, auf dem die Erkennung erfolgte
Prozess	Prozess, über den die Kontaktaufnahme versucht wurde (Pfad\Anwendungsname)
Lokale IP-Adresse und lokaler Port	IP-Adresse und Portnummer des Quellendpunkts

VORGANG	BESCHREIBUNG
Remote-IP-Adresse und Remote-Port	IP-Adresse und Portnummer des Zielendpunkts
Ergebnis	Ergebnis der durchgeführten Aktion
Listenquelle	Die C&C-Listenquelle, die den C&C-Server identifiziert hat
Richtung des Datenverkehrs	Richtung der übertragung

6. Wenn Sie das Protokoll als komma-separierte Datei im CSV-Format speichern möchten, klicken Sie auf **In CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Anzeigen von Protokollen für die Exemplar Zusendung

OfficeScan speichert Exemplar Zusendungsdaten in den Systemereignisprotokollen. Um eine detaillierte Zusammenfassung der Exemplar Zusendungsdaten zu erhalten, empfiehlt Trend Micro die Anzeige der Protokolle über die Control Manager Konsole. Control Manager stellt eine detaillierte Analyse der Verarbeitung verdächtiger Dateiobjekte bereit, wodurch Sie besseren Einblick in die Auswirkungen verdächtiger Objekte auf das Netzwerk erhalten.

Prozedur

1. Navigieren Sie zu **Protokolle** > **Systemereignisse**.
2. Überprüfen Sie unter **Ereignis** die folgenden Protokolltypen:
   - „An Virtual Analyzer weitergeleitetes Beispiel [Datei[<file_name], SHA1[<file_SHA1_value>]“
   - „Virtual Analyzer Beispielanalyse vollständig [<date_time_analysis_completed>, file[<file_name],

SHA1[<file_SHA1_value>], virus[<detection_type],
rule[<virtual_analyzer_rule_type]]“

Kapitel 9

Verhaltensüberwachung verwenden

In diesem Kapitel wird erläutert, wie Sie Computer mit der Funktion "Verhaltensüberwachung" vor Sicherheitsrisiken schützen.

Es werden folgende Themen behandelt:

- *Verhaltensüberwachung auf Seite 9-2*
- *Einstellungen der globalen Verhaltensüberwachung konfigurieren auf Seite 9-19*
- *Verhaltensüberwachungsberechtigungen auf Seite 9-21*
- *Benachrichtigungen der Verhaltensüberwachung für OfficeScan Agent-Benutzer auf Seite 9-23*
- *Verhaltensüberwachungsprotokolle auf Seite 9-24*

Verhaltensüberwachung

Die Verhaltensüberwachung überprüft regelmäßig Endpunkte auf ungewöhnliche Änderungen im Betriebssystem oder in installierter Software. Die Verhaltensüberwachung schützt Endpunkte durch **Sperrung bei Malware-Verhalten** und **Ereignisüberwachung**. Diese zwei Funktionen werden durch eine benutzerdefinierte **Ausschlussliste** und den **Certified Safe Software Service** ergänzt.

Wichtig

- Die Verhaltensüberwachung unterstützt keine Plattformen unter Windows XP (64-Bit) oder Windows Server 2003 (64-Bit).
- Die Verhaltensüberwachung ist in allen Versionen der Windows Server-Plattformen standardmäßig deaktiviert.

Sperrung bei Malware-Verhalten

Die Sperrung bei Malware-Verhalten bietet eine für zusätzlichen Schutz vor Bedrohungen durch Programme, die ein bösartiges Verhalten zeigen, erforderliche Schicht. Sie beobachtet über einen gewissen Zeitraum Systemereignisse. Während Programme verschiedene Kombinationen oder Folgen von Aktionen ausführen, erkennt die Sperrung bei Malware-Verhalten bekanntes bösartiges Verhalten und sperrt die entsprechenden Programme. Verwenden Sie diese Funktion, um einen besseren Schutz vor neuen, unbekannten und aufkommenden Bedrohungen zu gewährleisten.

Bei der Verhaltensüberwachung können schädliche von berechtigten Windows-Programmen ausgeführte Skripts sowie der effektive Nutzlastpfad der von berechtigten DLLs ausgeführten Skriptdateien erkannt werden, um Endpunkte vor Malware zu schützen, die dateilose Angriffswege nutzt.

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

- **Bekannte Bedrohungen**: Hiermit wird mit bekannten Bedrohungen verbundenes Malware-Verhalten blockiert.

- **Bekannte und mögliche Bedrohungen**: Hiermit wird mit bekannten Bedrohungen verbundenes Verhalten blockiert und es werden entsprechende Maßnahmen gegen potenziell bösartiges Verhalten ergriffen.

Nachdem das Sperren eines Programms mit Benachrichtigungen aktiviert wurde, zeigt der OfficeScan Agent eine Benachrichtigung auf dem Endpunkt an.

Weitere Informationen zu Benachrichtigungen finden Sie unter *Benachrichtigungen der Verhaltensüberwachung für OfficeScan Agent-Benutzer auf Seite 9-23*.

Ransomware-Schutz

Ransomware-Schutz verhindert die unbefugte änderung oder Verschlüsselung von Dateien auf Agents 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.

OfficeScan bietet die folgenden Methoden zum Schutz Ihrer Umgebung vor Ransomware-Bedrohungen.

Hinweis

Um zu vermeiden, dass der OfficeScan Agent einen sicheren Prozess als bösartig einstuft, stellen Sie sicher, dass der Agent Zugriff auf das Internet hat, damit weitere Verifizierungsprozesse unter Verwendung von Trend Micro Servern durchgeführt werden können.

Optionen	Beschreibung
Dokumente vor nicht autorisierter Verschlüsselung oder Veränderung schützen	Sie können Verhaltensüberwachung konfigurieren, um eine bestimmte Sequenz von Ereignissen zu erkennen, die möglicherweise auf einen Ransomware-Angriff hinweisen. Wenn die Verhaltensüberwachung alle der folgenden Kriterien erfüllt, beendet der OfficeScan Agent das böswillige Programm und versucht, es unter Quarantäne zu stellen. 1. Ein Prozess, der nicht als sicher erkannt wird, versucht, drei Dateien innerhalb eines bestimmten Zeitintervalls zu ändern, zu löschen oder umzubenennen. 2. Der Prozess hat versucht, eine Datei mit einer geschützten Erweiterung zu ändern Aktivieren Sie zusätzlich die Option **Die durch verdächtige Programme geänderten Dateien automatisch sichern**, um Kopien von auf Endpunkten verschlüsselten Dateien zu erstellen. Wenn OfficeScan nach Abschluss der Verschlüsselung eine Ransomware-Bedrohung entdeckt, fordert OfficeScan Endbenutzer dazu auf, die betroffenen Dateien ohne Datenverlust wiederherzustellen. **Hinweis** Zur automatischen Dateisicherung werden mindestens 100 MB Festplattenspeicher auf dem Agent-Endpunkt benötigt und es werden nur Dateien gesichert, die kleiner als 10 MB sind. Der Speicherort des Sicherungsordners auf den Agent-Endpunkt befindet sich unter:<Installationsordner des Agents>`\CCSF\module\DRE\data`. **Warnung!** Wenn die Option **Die durch verdächtige Programme geänderten Dateien automatisch sichern** nicht aktiviert ist, kann OfficeScan die ersten von einer Ransomware-Bedrohung betroffenen Dateien nicht wiederherstellen.

OPTIONEN	BESCHREIBUNG
Prozesse blockieren, die häufig mit Ransomware verknüpft sind	Ransomware verteilt häufig ausführbare Dateien in bestimmten Speicherorten auf Endpunkten, bevor Dateien angegriffen werden. Durch Blockieren der Prozesse, die von diesen Speicherorten aus gestartet werden, kann verhindert werden, dass die Ransomware die Dateien angreifen kann.
Programmüberprüfung zum Erkennen und Sperren gefährdeter ausführbarer Dateien aktivieren	Die Programmüberprüfung überprüft Prozesse und führt API-Hooking durch, um festzustellen, ob ein Programm unerwartetes Verhalten zeigt. Dieses Verfahren erhöht zwar den Gesamterkennungsgrad gefährdeter ausführbarer Dateien, setzt aber möglicherweise die Systemleistung herab. **Tipp** Die Programmüberprüfung stellt erhöhte Sicherheit bereit, wenn Sie **Bekannte und potenzielle Bedrohungen** im Dropdown-Menü **Zu sperrende Bedrohungen** auswählen. **Wichtig** Wird auf Windows Server 2003 ohne SP2 (oder höher) und Windows XP 64-Bit-Plattformen nicht unterstützt.

Schwachstellenschutz

Schwachstellenschutz und Programmüberprüfung arbeiten zusammen, um das Verhalten von Programmen zu überwachen und ungewöhnliches Verhalten zu erkennen, das unter Umständen darauf hinweist, dass ein Angreifer eine Programmschwachstelle ausgenutzt hat. Wird solches Verhalten erkannt, beendet die Verhaltensüberwachung die Programmprozesse.

Wichtig

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

Schutz vor neu erkannten Programmen

Zusammen mit den Web-Reputation-Diensten und der Echtzeitsuche überprüft die Verhaltensüberwachung das bisherige Vorkommen von Dateien, die über Internetkanäle, E-Mail-Anwendungen oder Microsoft Office-Makroskripts heruntergeladen wurden. Sobald eine "neu entdeckte" Datei erkannt wird können Administratoren eine Systemaufforderung an die Benutzer ausgeben, bevor sie die Datei ausführen. Trend Micro stuft ein Programm auf der Grundlage der Anzahl der Dateierkennungen oder des historischen Alters der Datei wie durch das Smart Protection Network als neu gefunden ein.

Die Verhaltensüberwachung überprüft für jeden Kanal die folgenden Dateitypen:

- Internet (HTTP/HTTPS): `.exe`-Dateien werden überprüft.
- E-Mail-Anwendungen: `.exe`-Dateien und komprimierte `.exe`-Dateien in unverschlüsselten `.zip`- und `.rar`-Dateien werden überprüft.

Hinweis

- Bevor diese Eingabeaufforderung angezeigt werden kann, müssen Administratoren die Web-Reputation-Dienste auf dem Agent aktivieren, damit der OfficeScan Agent HTTP- oder HTTPS-Datenverkehr durchsuchen kann.
- Der OfficeScan Agent führt einen Abgleich mit den Dateinamen durch, die während des Ausführungsvorgangs über E-Mail-Anwendungen heruntergeladen wurden. Wenn der Dateiname geändert wurde, erhält der Benutzer eine Eingabeaufforderung.

Ereignisüberwachung

Die Ereignisüberwachung bietet einen generischeren Ansatz zum Schutz vor nicht autorisierter Software und Malware-Angriffen. Sie überwacht Systembereiche auf bestimmte Ereignisse. Dies gibt Administratoren die Möglichkeit, Programme zu regulieren, die derartige Ereignisse auslösen. Verwenden Sie die Systemüberwachung, wenn Sie über den durch Sperrung bei Malware-Verhalten gebotenen Schutz hinaus spezielle Schutzanforderungen für das System benötigen.

Die folgende Tabelle enthält eine Liste der überwachten Systemereignisse.

TABELLE 9-1. Überwachte Systemereignisse

EREIGNISSE	BESCHREIBUNG
Duplizierte Systemdatei	Viele bösartige Programme erstellen Kopien von sich selbst oder anderen bösartigen Programmen unter Verwendung von Dateinamen, die von Windows Systemdateien verwendet werden. Dies geschieht in der Regel, um Systemdateien zu überschreiben oder zu ersetzen, sich zu verbergen oder zu verhindern, dass Benutzer die bösartigen Dateien löschen.
Änderung der Hosts-Datei	Die Hosts-Datei ordnet Domain-Namen IP-Adressen zu. Zahlreiche bösartige Programme verändern die Hosts-Datei so, dass der Webbrowser zu infizierten, nicht existierenden oder falschen Websites umgeleitet wird.
Verdächtiges Verhalten	Verdächtiges Verhalten kann sich in einer bestimmten Aktion oder einer Reihe von Aktionen zeigen, die normalerweise nicht von rechtmäßigen Programmen durchgeführt werden. Programme, die verdächtiges Verhalten aufweisen, sollten mit Vorsicht verwendet werden.
Neues Plug-in für den Internet Explorer	Spyware-/Grayware-Programme installieren oft unerwünschte Plug-ins für den Internet Explorer, wie z. B. Symbolleisten und Browser Helper Objects.
Änderungen an Einstellungen des Internet Explorers	Viele Viren-/Malware-Programme verändern die Einstellungen im Internet Explorer, einschließlich Startseite, vertrauenswürdige Websites, Proxy-Server-Einstellungen und Menü-Erweiterungen.
Änderungen der Sicherheitsrichtlinien	Durch Änderungen der Sicherheitsrichtlinien können unerwünschte Anwendungen ausgeführt und Systemeinstellungen verändert werden.
Injektion einer Programmbibliothek	Viele bösartige Programme konfigurieren Windows so, dass alle Anwendungen automatisch eine Programmbibliothek (DLL) laden. Dadurch können bösartige Routinen in der DLL bei jedem Start einer Anwendung ausgeführt werden.

Ereignisse	Beschreibung
Shell-Änderungen	Viele bösartige Programme verändern die Einstellungen der Windows Shell, um sich selbst mit bestimmten Dateitypen zu verknüpfen. Durch diese Routine können bösartige Programme automatisch gestartet werden, wenn Benutzer die verknüpften Dateien im Windows Explorer öffnen. Durch Änderungen in der Windows Shell können bösartige Programme außerdem die verwendeten Programme nachverfolgen und wie rechtmäßige Programme gestartet werden.
Neuer Dienst	Windows Dienste sind Prozesse mit speziellen Funktionen. Sie werden in der Regel dauerhaft und mit vollständigen Administratorberechtigungen im Hintergrund ausgeführt. Bösartige Programme installieren sich in manchen Fällen als versteckte Dienste selbst.
Änderung von Systemdateien	Bestimmte Windows Systemdateien legen das Systemverhalten, einschließlich der Autostart-Programme und der Bildschirmschonereinstellungen, fest. Viele bösartige Programme verändern Systemdateien so, dass sie beim Start automatisch ausgeführt werden und das Systemverhalten steuern.
Änderungen der Firewall-Richtlinien	Die Windows Firewall-Richtlinie legt die Anwendungen fest, die auf das Netzwerk zugreifen können, die Ports, die für die Kommunikation geöffnet sind und die IP-Adressen, die mit dem Computer kommunizieren können. Viele bösartige Programme verändern die Richtlinie, um sich den Zugriff auf das Netzwerk und das Internet zu ermöglichen.
Änderungen an Systemprozessen	Viele bösartige Programme führen verschiedene Aktionen an integrierten Windows Prozessen durch. So beenden oder ändern sie beispielsweise aktive Prozesse.
Neues Autostart-Programm	Bösartige Anwendungen fügen der Windows-Registrierung gewöhnlich Autostart-Einträge hinzu oder ändern diese, so dass sie bei jedem Hochfahren des Computers automatisch gestartet werden.

Wenn von der Ereignisüberwachung ein überwachtes Systemereignis erkannt wird, wird die für dieses Ereignis konfigurierte Aktion ausgeführt.

Die folgende Tabelle enthält eine Liste der möglichen Aktionen, die Administratoren bei überwachten Systemereignissen ergreifen können.

TABELLE 9-2. Aktionen bei überwachten Systemereignissen

AKTION	BESCHREIBUNG
Bewerten	Der OfficeScan Agent lässt die Ausführung von Programmen, die einem Ereignis zugeordnet sind, immer zu und protokolliert das Ereignis zwecks Bewertung. Dies ist die Standardaktion für alle überwachten Systemereignisse. **Hinweis** Diese Option wird nicht für DLL-Injektionen auf 64-Bit-Systemen unterstützt.
Zulassen	Der OfficeScan Agent lässt die Ausführungen von Programmen, die einem Ereignis zugeordnet sind, immer zu.
Bei Bedarf nachfragen	Der OfficeScan Agent fordert Benutzer auf, die Ausführung von Programmen, die einem Ereignis zugeordnet sind, zuzulassen oder abzulehnen und fügt die Programme in der Ausnahmeliste hinzu. Wenn der Benutzer nicht innerhalb eines bestimmten Zeitraums reagiert, lässt der OfficeScan Agent die Ausführung des Programms automatisch zu. Der Standardzeitraum beträgt 30 Sekunden. Informationen zur Anpassung des Zeitraums finden Sie unter *Einstellungen der globalen Verhaltensüberwachung konfigurieren auf Seite 9-19*. **Hinweis** Diese Option wird nicht für DLL-Injektionen auf 64-Bit-Systemen unterstützt.

AKTION	BESCHREIBUNG
Verweigern	Der OfficeScan Agent sperrt stets die Ausführung von Programmen, die einem Ereignis zugeordnet sind, und protokolliert das Ereignis. Nachdem das Sperren eines Programms mit Benachrichtigungen aktiviert wurde, zeigt der OfficeScan Agent eine Benachrichtigung auf dem Endpunkt an. Weitere Informationen zu Benachrichtigungen finden Sie unter *Benachrichtigungen der Verhaltensüberwachung für OfficeScan Agent-Benutzer auf Seite 9-23*.

Ausschlussliste für Verhaltensüberwachung

Die Ausnahmeliste für die Verhaltensüberwachung enthält Programme, die der OfficeScan Agent nicht mit Hilfe der Verhaltensüberwachung überwacht.

- **Zulässige Programme**: Der OfficeScan Agent gestattet allen Programmen in der Liste der zulässigen Programme, die Verhaltensüberwachung zu übergehen.

  Hinweis

  Obwohl die Verhaltensüberwachung für Programme, die der Liste der zulässigen Programme hinzugefügt wurden, keine Maßnahmen ergreift, werden die Programme weiterhin mit anderen Suchfunktionen (beispielsweise dateibasierte Suche) durchsucht, bevor die Ausführung der Programme zugelassen wird.

- **Gesperrte Programme**: Der OfficeScan Agent sperrt alle Programme in der Liste der gesperrten Programme. Zum Konfigurieren der Liste der gesperrten Programme aktivieren Sie die Ereignisüberwachung.

Sie können die Ausschlussliste über die Webkonsole konfigurieren. Sie können Benutzern auch die Berechtigung zum Konfigurieren einer eigenen Ausnahmeliste über die OfficeScan Agent-Konsole gewähren.

Weitere Informationen finden Sie unter *Verhaltensüberwachungsberechtigungen auf Seite 9-21*.

Ausnahmeliste, Unterstützung von Platzhaltern

Die zulässige Liste der OfficeScan Verhaltensüberwachung unterstützt Platzhalterzeichen beim Definieren von Ausnahmetypen für den Dateipfad, den Dateinamen und die Dateierweiterung. Verwenden Sie die folgende Tabelle für eine ordnungsgemäße Formatierung Ihrer Ausnahmelisten, um sicherzustellen, dass OfficeScan die korrekten Dateien und Ordner von der Suche ausschließt.

Unterstützte Platzhalterzeichen:

- Sternchen (*): Steht für ein beliebiges Zeichen oder eine Zeichenfolge.
- Fragezeichen (?): Steht für ein einzelnes Zeichen.

Wichtig

Die zulässige Liste der OfficeScan Verhaltensüberwachung unterstützt die Verwendung von Platzhalterzeichen zum Ersetzen von Systemlaufwerksbezeichnungen oder UNC-Adressen nicht.

Ausnahmetyp	Verwendung von Platzhalterzeichen	Übereinstimmung	Keine Übereinstimmung
Verzeichnisse	`C:\*` Schließt alle Dateien und Ordner im ausgewählten Laufwerk aus.	• `C:\sample.exe` • `C:\folder\test.doc`	• `D:\sample.exe` • `E:\folder\test.doc`
Bestimmte Dateien unter einer bestimmten Ordnerebene	`C:\*\Sample.exe` Schließt die Datei `Sample.exe` nur dann aus, wenn sich die Datei in einem Unterordner des Verzeichnisses `C:\` befindet.	• `C:\files\Sample.exe` • `C:\temp\files\Sample.exe`	• `C:\sample.exe`

AUSNAHMETYP	VERWENDUNG VON PLATZHALTERZEICHEN	ÜBEREINSTIMMUNG	KEINE ÜBEREINSTIMMUNG
UNC-Pfade	`\\<UNC-Pfad>\*\Sample.exe` Schließt die Datei `Sample.exe` nur dann aus, wenn sich die Datei in einem Unterordner des angegebenen UNC-Pfads befindet.	• `\\<UNC path>\files\Sample.exe` • `\\<UNC path>\temp\files\Sample.exe`	• `R:\files\Sample.exe` Grund: Zugeordnete Laufwerke werden nicht unterstützt. • `\\<UNC-Pfad>\Sample.exe` Grund: Die Datei ist nicht in einem Unterordner des UNC-Pfads enthalten.
Dateinamen und Erweiterungen	`C:\*.*` Schließt alle Dateien mit Erweiterungen in allen Ordnern und Unterordnern des Verzeichnisses `C:\` aus.	• `C:\Sample.exe` • `C:\temp\Sample.exe` • `C:\test.doc`	• `D:\sample.exe` • `C:\Sample` **Hinweis** `C:\Sample` hat keine Dateierweiterung und wird daher nicht aus der Suche ausgeschlossen.

Ausnahmetyp	Verwendung von Platzhalterzeichen	Übereinstimmung	Keine Übereinstimmung
Dateinamen	`C:\*.exe` Schließt alle Dateien mit der Erweiterung `.exe` in allen Ordnern und Unterordnern des Verzeichnisses `C:\` aus.	• `C:\Sample.exe` • `C:\temp\test.exe`	• `C:\Sample.doc` • `C:\temp\test.bat` • `C:\Sample` **Hinweis** `C:\Sample` hat keine Dateierweiterung und wird daher nicht aus der Suche ausgeschlossen.
Dateierweiterungen	`C:\Sample.*` Schließt alle Dateien mit dem Namen `Sample` und einer beliebigen Erweiterung in allen Ordnern und Unterordnern des Verzeichnisses `C:\` aus.	• `C:\Sample.exe` • `C:\temp\Sample.doc`	• `C:\Sample1.doc` • `C:\temp\Samples.bat` • `C:\Sample` **Hinweis** `C:\Sample` hat keine Dateierweiterung und wird daher nicht aus der Suche ausgeschlossen.

AUSNAHMETYP	VERWENDUNG VON PLATZHALTERZEICHEN	ÜBEREINSTIMMUNG	KEINE ÜBEREINSTIMMUNG
Dateien in bestimmten Verzeichnisstrukturen	`C:\*\*\Sample.exe` Schließt alle Dateien aus, die sich auf der zweiten Unterordnerebene oder in sonstigen nachfolgenden Unterordnern des Verzeichnisses `C:\` mit dem Dateinamen und der Erweiterung `Sample.exe` befinden.	• `C:\files\temp\Sample.exe` • `C:\files\temp\test\Sample.exe`	• `C:\Sample.exe` • `C:\temp\Sample.exe` • `C:\files\temp\Sample.doc`

Ausnahmetyp	Verwendung von Platzhalterzeichen	Übereinstimmung	Keine Übereinstimmung
Komplexe Pfade oder Dateinamen	`C:\Sam*e??.exe` Schließt alle Dateien mit Namen aus, die die folgenden Bedingungen erfüllen: • Sie beginnen mit den Zeichen "Sam". • Der drittletzte Buchstabe des Dateinamens muss ein "e" sein. • Zwischen der Zeichenfolge "Sam" am Anfang und der Zeichenfolge "e??" am Ende des Dateinamens muss sich mindestens ein Zeichen befinden. • Vor der Dateierweiterung und nach dem "e" im Dateinamen sind genau 2 Zeichen vorhanden. • Die Dateierweiterung ist `.exe` Wenn eine Datei alle erforderlichen Bedingungen erfüllt und sich in einem beliebigen Unterordner des Verzeichnisses `C:\` befindet, schließt OfficeScan die Datei aus Suchvorgängen aus.	• `C:\Sample12.exe` • `C:\test\SametimeAA.exe` • `C:\SamSamSample12.exe`	• `C:\SaSmple12.exe` Grund: Beginnt nicht mit "Sam". • `C:\SamSamSam12.exe` Grund: Enthält kein "e" als drittletztes Zeichen. • `C:\Same12.exe` Grund: Enthält keine Zeichen zwischen der Zeichenfolge "Sam" am Anfang und dem Buchstaben "e" an drittletzter Stelle. • `C:\Sample1.exe` Grund: Enthält keine 2 Zeichen vor der Erweiterung und nach dem Buchstaben "e". • `C:\Sample12.doc` Grund: Ungültige Erweiterung

Sperrung bei Malware-Verhalten, Ereignisüberwachung und Ausnahmeliste konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen der Verhaltensüberwachung**.
4. Klicken Sie auf die Registerkarte **Regeln**.
5. Gehen Sie im Abschnitt **Sperrung bei Malware-Verhalten** wie folgt vor:

    a. Wählen Sie **Sperren des Malware-Verhaltens aktivieren** aus und geben Sie die zu sperrenden Bedrohungstypen an:

    - **Bekannte Bedrohungen**: Sperrt Verhaltensweisen im Zusammenhang mit bekannten Malware-Bedrohungen
    - **Bekannte und potenzielle Bedrohungen**: Sperrt Verhaltensweisen im Zusammenhang mit bekannten Bedrohungen und ergreift Maßnahmen gegen potenziell bösartiges Verhalten

    b. Wählen Sie aus, welche Ransomware-Schutzfunktionen aktiviert werden sollen, um Dokumente vor Ransomware-Bedrohungen zu schützen.

    - **Dokumente vor nicht autorisierter Verschlüsselung oder Veränderung schützen**: Beendet potentielle Ransomware-Bedrohungen, sodass sie Inhalte von Dokumenten nicht verschlüsseln oder verändern können.
        - **Die durch verdächtige Programme geänderten Dateien automatisch sichern und wiederherstellen**: Erstellt zur Vermeidung von Datenverlust Sicherungskopien von auf Endpunkten verschlüsselten Dateien, nachdem eine Bedrohung durch Ransomware erkannt wurde.

Hinweis

Zur automatischen Dateisicherung werden mindestens 100 MB Festplattenspeicher auf dem Agent-Endpunkt benötigt und es werden nur Dateien gesichert, die kleiner als 10 MB sind.

- **Prozesse sperren, die häufig mit Ransomware verknüpft sind**: Sperrt Prozesse, die mit bekannten Ransomware-Bedrohungen verknüpft sind, bevor eine Verschlüsselung oder Veränderung von Dokumenten auftreten kann.
- **Programmüberprüfung zum Erkennen und Sperren gefährdeter ausführbarer Dateien aktivieren**: Die Programmüberprüfung überprüft Prozesse und führt API-Hooking durch, um festzustellen, ob ein Programm unerwartetes Verhalten zeigt. Dieses Verfahren erhöht zwar den Gesamterkennungsgrad gefährdeter ausführbarer Dateien, setzt aber möglicherweise die Systemleistung herab.

Tipp

Die Programmüberprüfung stellt erhöhte Sicherheit bereit, wenn Sie **Bekannte und potenzielle Bedrohungen** im Dropdown-Menü **Zu sperrende Bedrohungen** auswählen.

Weitere Informationen finden Sie unter *Ransomware-Schutz auf Seite 9-3*.

c. Aktivieren Sie unter **Schutz vor Schwachstellen** die Option **Programme beenden, die ungewöhnliches Verhalten im Zusammenhang mit Angriffen auf Schwachstellen zeigen**, um Schutz vor Programmen mit Sicherheitslücken bereitzustellen.

Hinweis

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

Weitere Informationen finden Sie unter *Schwachstellenschutz auf Seite 9-5*.

6. Aktivieren Sie im Abschnitt **Neu erkannte Programme** die Option **Neu erkannte Programme überwachen, die über Internet- oder E-Mail-**

Anwendungskanäle heruntergeladen wurden und wählen Sie entweder **Benutzer auffordern** aus, bevor Sie das heruntergeladene Programm ausführen, oder lassen Sie OfficeScan nur die Erkennungen protokollieren.

7. Gehen Sie im Abschnitt **Ereignisüberwachung** wie folgt vor:

   a. Wählen Sie **Ereignisüberwachung aktivieren**.

   b. Wählen Sie die zu überwachenden Systemereignisse und wählen Sie eine Aktion für die einzelnen ausgewählten Ereignisse.

      Weitere Informationen zu überwachten Systemereignissen und Aktionen finden Sie unter *Ereignisüberwachung auf Seite 9-6*.

8. Klicken Sie auf die Registerkarte **Ausnahmen**, um die Ausnahmelisten zu konfigurieren.

   a. Geben Sie unter **Geben Sie den vollständigen Programmpfad ein** den vollständigen Pfad des Programms ein, das zugelassen oder gesperrt werden soll.

   b. Klicken Sie auf **Zur Liste der zulässigen URLs hinzufügen** oder **Zur Liste der gesperrten URLs hinzufügen**.

   c. Um ein gesperrtes oder zugelassenes Programm aus der Liste zu entfernen, klicken Sie neben dem Programm auf das Papierkorbsymbol).

   Hinweis

   In OfficeScan sind insgesamt maximal 1024 zugelassene Programme und gesperrte Programme möglich.

9. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Einstellungen der globalen Verhaltensüberwachung konfigurieren

OfficeScan wendet globale Agent-Einstellungen auf alle Agents oder nur auf Agents mit bestimmten Berechtigungen an.

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Klicken Sie auf die Registerkarte **Sicherheitseinstellungen**.
3. Navigieren Sie zum Abschnitt **Einstellungen der Verhaltensüberwachung**.
4. Konfigurieren Sie die Einstellung **Automatisch Aktion ausführen, wenn keine Antwort vom Benutzer innerhalb von __ Sekunde(n)** nach Bedarf.

   Diese Einstellung wird nur unterstützt, wenn die Ereignisüberwachung aktiviert ist und die Aktion für ein überwachtes Systemereignis "Bei Bedarf nachfragen" lautet. Diese Aktion fordert einen Benutzer auf, mit dem Ereignisse verbundene Programme zuzulassen oder abzulehnen. Wenn der Benutzer nicht in einem bestimmten Zeitraum reagiert, lässt OfficeScan die Ausführung des Programms automatisch zu.

   Weitere Informationen finden Sie unter *Ereignisüberwachung auf Seite 9-6*.

5. Klicken Sie auf die Registerkarte **System**.
6. Navigieren Sie zum Abschnitt **Einstellungen für Certified Safe Software Service**, und ändern Sie ggf. den Certified Safe Software Service.

   Der Certified Safe Software Service fragt Trend Micro Rechenzentren ab, um die Sicherheit eines von der Sperrung bei Malware-Verhalten, der

Ereignisüberwachung, der Firewall oder der Virensuche erkannten Programms zu überprüfen. Aktivieren Sie den Certified Safe Software Service, um die Häufigkeit von Fehlalarmen zu verringern.

Hinweis

Achten Sie auf korrekte Proxy-Einstellungen für OfficeScan Agents (weitere Informationen finden Sie unter *OfficeScan Agent Proxy-Einstellungen auf Seite 15-53*), bevor Certified Safe Software Service aktiviert wird. Bei fehlerhaften Proxy-Einstellungen sowie einer Internet-Verbindung, die nicht ständig besteht, kann es zu Verzögerungen kommen, oder Antworten von Trend Micro Rechenzentren können nicht abgerufen werden, was zur Folge hat, dass überwachte Programme nicht zu antworten scheinen.

Des Weiteren können IPv6-OfficeScan Agents keine direkten Abfragen an Trend Micro Rechenzentren richten. Ein Dual-Stack-Proxy-Server wie beispielsweise DeleGate, der IP-Adressen konvertieren kann, muss ermöglichen, dass die OfficeScan Agents eine Verbindung zu Trend Micro Rechenzentren herstellen können.

7. Klicken Sie auf **Speichern**.

Verhaltensüberwachungsberechtigungen

Wenn agents Verhaltensüberwachungsberechtigungen haben, wird die Option "Verhaltensüberwachung" auf der OfficeScan Agent-Konsole im Fenster **Einstellungen** angezeigt. Benutzer können dann ihre eigene Ausschlussliste verwalten.

ABBILDUNG 9-1. Die Option "Verhaltensüberwachung" auf der OfficeScan Agent-Konsole

Verhaltensüberwachungsberechtigungen gewähren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Navigieren Sie auf der Registerkarte **Berechtigungen** zum Bereich **Verhaltensüberwachungsberechtigungen**.
5. Wählen Sie **Die Einstellungen für die Verhaltensüberwachung auf der OfficeScan Agent-Konsole anzeigen** aus.
6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Benachrichtigungen der Verhaltensüberwachung für OfficeScan Agent-Benutzer

OfficeScan kann auf dem OfficeScan Agent-Computer sofort eine Benachrichtigung anzeigen, wenn die Verhaltensüberwachung ein Programm sperrt. Aktivieren Sie die Benachrichtigung und ändern Sie bei Bedarf den Inhalt der Nachricht.

Senden von Benachrichtigungen aktivieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Öffnen Sie die Registerkarte **Andere Einstellungen** und gehen Sie zum Abschnitt **Einstellungen der Verhaltensüberwachung**.
5. Wählen Sie **Benachrichtigung anzeigen, wenn ein Programm gesperrt ist**.
6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option

werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Inhalt der Benachrichtigung ändern

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Agent**.
2. Wählen Sie im Listenfeld **Typ** die Option **Verstöße gegen eine Verhaltensüberwachungs-Richtlinie** aus.
3. ändern Sie die Standardnachrichten im bereitgestellten Textfeld.
   - Verstöße gegen eine Verhaltensüberwachungs-Richtlinie:Geben Sie die Nachricht an, die Endbenutzer erhalten, wenn während des Prozesses zur Sperrung bei Malware-Verhalten ein Richtlinienverstoß erkannt wird.
   - Neu erkannte Programme: Geben Sie die Nachricht an, die Endbenutzer erhalten, wenn während des Prozesses zur Verhaltenssperrung ein unbekanntes Programm erkannt wird, das über Internet- oder E-Mail-Anwendungskanäle heruntergeladen wurde.
4. Klicken Sie auf **Speichern**.

Verhaltensüberwachungsprotokolle

Die OfficeScan Agents protokollieren unbefugte Programmzugriffe und senden die Protokolle an den Server. Standardmäßig fasst ein OfficeScan Agent, der kontinuierlich läuft, die Protokolle zusammen und sendet sie in bestimmten Zeitabständen (standardmäßig alle 60 Minuten).

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell, oder konfigurieren Sie eine zeitgesteuerte Löschung der Protokolle. Weitere Informationen zur Protokollverwaltung finden Sie unter *Protokollmanagement auf Seite 14-47*.

Verhaltensüberwachungsprotokolle anzeigen

Prozedur

1. Navigieren Sie zu **Protokolle** > **Agents** > **Sicherheitsrisiken** oder **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Protokolle** > **Verhaltensüberwachungsprotokolle** oder **Protokolle anzeigen** > **Verhaltensüberwachungsprotokolle**.
4. Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.
5. Sehen Sie die Protokolle ein. Die Protokolle enthalten die folgenden Informationen:
   - Datum/Uhrzeit, als der unbefugte Prozess erkannt wurde
   - Der Endpunkt, auf dem der unbefugte Prozess erkannt wurde
   - Endpunktdomäne
   - Verstoß, bei dem es sich um die Ereignisüberwachungsregel handelt, gegen die der Prozess verstoßen hat
   - Aktion, die durchgeführt wurde, als der Verstoß erkannt wurde
   - Ereignis, bei dem es sich um den Typ des Objekts handelt, auf das das Programm zugegriffen hat
   - Die Risikostufe des unbefugten Programms
   - Das unbefugte Programm
   - Operation, bei der es sich um die Aktion handelt, die vom unbefugten Programm ausgeführt wurde
   - Das Ziel, bei dem es sich um den Prozess handelt, auf den zugegriffen wurde

- Infektionskanal, aus dem die Bedrohung stammt

6. Wenn Sie das Protokoll als komma-separierte Datei (`CSV-Datei`) speichern möchten, klicken Sie auf **In CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Zeitgesteuertes Senden des Verhaltensüberwachungsprotokolls konfigurieren

Prozedur

1. Greifen Sie auf den Ordner <*Installationsordner des Servers*>`\PCCSRV` zu.
2. Öffnen Sie die Datei `ofcscan.ini` mit einem Texteditor, wie z. B. Notepad.
3. Suchen Sie nach der Zeichenfolge "`SendBMLogPeriod`", und überprüfen Sie anschließend den daneben stehenden Wert.

   Der Standardwert beträgt 3600 Sekunden, und die Zeichenfolge erscheint als `SendBMLogPeriod=3600`.
4. Legen Sie den Wert in Sekunden fest.

   Um z. B. die Protokolldauer auf 2 Stunden zu ändern, ändern Sie den Wert auf 7200.
5. Speichern Sie die Datei.
6. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
7. Klicken Sie auf **Speichern**, ohne eine Einstellung zu ändern.
8. Starten Sie den agent neu.

Kapitel 10

Die Gerätesteuerung verwenden

In diesem Kapitel wird erläutert, wie Sie Computer mit der Funktion "Gerätesteuerung" vor Sicherheitsrisiken schützen.

Es werden folgende Themen behandelt:

- *Gerätesteuerung auf Seite 10-2*
- *Berechtigungen für Speichergeräte auf Seite 10-4*
- *Berechtigungen für Nicht-Speichergeräte auf Seite 10-11*
- *Gerätesteuerungsbenachrichtigungen ändern auf Seite 10-19*
- *Protokolle der Gerätesteuerung auf Seite 10-19*

Gerätesteuerung

Die Gerätesteuerung reguliert den Zugriff auf externe Speichergeräte und Netzwerkressourcen, die an Computer angeschlossen sind. Die Gerätesteuerung trägt dazu bei, Datenverluste und Datenlecks zu verhindern und bietet, gemeinsam mit der Virensuche, Schutz vor Sicherheitsrisiken.

Sie können Gerätesteuerungsrichtlinien für interne und externe Agents konfigurieren. In der Regel konfigurieren Administratoren eine strengere Richtlinie für externe Agents.

Bei Richtlinien handelt es sich um detaillierte Einstellungen in der OfficeScan Agent-Hierarchie. Sie können bestimmte Richtlinien für Agent-Gruppen oder einzelne Agents erzwingen. Sie können auch eine einzelne Richtlinie für alle Agents erzwingen.

Nachdem Sie die Richtlinien verteilt haben, verwenden die Agents die Standortkriterien, die Sie im Fenster **Endpunktstandort** festgelegt haben (siehe *Endpunktspeicherort auf Seite 15-2*), um deren Standort und die erforderliche Richtlinie zu bestimmen. Agents wechseln die Richtlinien mit jedem Standortwechsel.

Wichtig

- Die Gerätesteuerung ist auf allen Versionen von Windows Server 2003, Windows Server 2008, Windows Server 2012 und Windows Server 2016 standardmäßig deaktiviert. Lesen Sie vor der Aktivierung der Gerätesteuerung auf diesen Serverplattformen die Richtlinien und bewährten Methoden, die unter *OfficeScan Agent Dienste auf Seite 15-7* beschrieben werden.
- Eine Liste aller unterstützten Gerätemodelle finden Sie in der *Datenschutzliste* unter:

  http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Die Gerätearten, die OfficeScan überwachen kann, hängen davon ab, ob die Datenschutzlizenz aktiviert ist. Der Datenschutz ist ein separat lizenziertes Modul, das vor seiner Verwendung aktiviert werden muss. Weitere Informationen über die Datenschutzlizenz finden Sie unter *Datenschutzlizenz auf Seite 3-4*.

TABELLE 10-1. Die über das Modul "Unauthorized Change Prevention Service" überwachten Geräte

GERÄTETYP	GERÄTEBESCHREIBUNG
Speichergeräte	CD/DVD **Wichtig** Gerätesteuerung kann den Zugriff auf CD/DVD-Aufnahmegeräte begrenzen, die das Live-Dateisystemformat verwenden. Einige Anwendungen von Drittanbietern, die Master Format verwenden, können Lese-/Schreibvorgänge ausführen, selbst wenn Gerätesteuerung aktiviert ist. Verwenden Sie Prävention vor Datenverlust, um den Zugriff auf CD/DVD-Aufnahmegeräte zu begrenzen, die einen beliebigen Formattyp verwenden. Weitere Informationen finden Sie unter *Zugriff auf Datenspeicher (CD/DVD) blockieren auf Seite 11-37*.
	Disketten
	Netzlaufwerke
	USB-Speichergeräte

TABELLE 10-2. Mit "Prävention vor Datenverlust" überwachte Geräte

GERÄTETYP	GERÄTEBESCHREIBUNG
Mobilgeräte	Mobilgeräte
Speichergeräte	CD/DVD
	Disketten
	Netzlaufwerke
	USB-Speichergeräte

GERÄTETYP	GERÄTEBESCHREIBUNG
Nicht-Speichergeräte	Bluetooth-Adapter
	COM- und LPT-Anschlüsse
	IEEE 1394-Schnittstelle
	Bildverarbeitungsgeräte
	Infrarotgeräte
	Modems
	PCMCIA-Karten
	Druck-Taste
	Wireless-NICs

Berechtigungen für Speichergeräte

Gerätesteuerungsberechtigungen für Speichergeräte werden in folgenden Fällen verwendet:

- Erlauben Sie den Zugriff aus USB-Speichergeräte, CD/DVD, Disketten und Netzwerklaufwerke. Sie können den Zugriff auf diese Geräte entweder uneingeschränkt zulassen oder die Zugriffsstufe einschränken.
- Konfigurieren Sie die Liste der zulässigen USB-Speichergeräte. Mit der Gerätesteuerung können Sie den Zugriff auf alle USB-Speichergeräte sperren, mit Ausnahme der Geräte, die Sie in der Liste zulässiger Geräte hinzugefügt haben. Sie können den Zugriff auf die zulässigen Geräte entweder uneingeschränkt zulassen oder die Zugriffsstufe einschränken.

Die folgende Tabelle enthält eine Liste der Berechtigungen für Speichergeräte.

Tabelle 10-3. Gerätesteuerungsberechtigungen für Speichergeräte

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.
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
Lesen	Zulässige Aktionen: Kopieren, öffnen Unzulässige Aktionen: Speichern, Verschieben, Löschen, Ausführen	Unzulässige Aktionen: Speichern, Verschieben, Kopieren
Nur Geräteinhalt auflisten	Unzulässige Aktionen: Alle Aktionen Die enthaltenen Geräte und Dateien werden dem Benutzer angezeigt (beispielsweise in Windows Explorer).	Unzulässige Aktionen: Speichern, Verschieben, Kopieren

BERECHTIGUNGEN	DATEIEN AUF DEM GERÄT	EINGEHENDE DATEIEN
Sperren (nach der Installation der Funktion "Datenschutz" verfügbar)	Unzulässige Aktionen: Alle Aktionen Die enthaltenen Geräte und Dateien werden dem Benutzer nicht angezeigt (beispielsweise in Windows Explorer).	Unzulässige Aktionen: Speichern, Verschieben, Kopieren

Die dateibasierte Suche wird durch Geräteberechtigungen ergänzt und kann die Geräteberechtigungen überschreiben. Wenn die Berechtigung z. B. zulässt, dass eine Datei geöffnet werden kann, der OfficeScan Agent jedoch erkennt, dass die Datei mit Malware infiziert ist, wird eine bestimmte Suchaktion auf die Datei angewendet, um die Malware zu entfernen. Wenn als Suchaktion "Säubern" ausgewählt wird, wird die Datei nach dem Säubern geöffnet. Wird jedoch als Suchaktion "Löschen" ausgewählt, wird die Datei gelöscht.

Tipp

Die Gerätesteuerung für den Datenschutz unterstützt alle 64-Bit-Plattformen. Legen Sie für die Überwachung durch Unauthorized Change Prevention auf Systemen, die der OfficeScan Agent nicht unterstützt, die Geräteberechtigung auf **Sperren** fest, um den Zugriff auf diese Geräte einzuschränken.

Erweiterte Berechtigungen für Speichergeräte

Erweiterte Berechtigungen gelten, wenn Sie eingeschränkte Berechtigungen für die meisten Speichergeräte eingerichtet haben. Folgende Berechtigungen sind möglich:

- **Ändern**
- **Lesen und Ausführen**
- **Lesen**
- **Nur Geräteinhalt auflisten**

Sie können die Berechtigungen weiterhin eingeschränkt lassen, jedoch bestimmten Programmen auf den Speichergeräten und auf dem lokalen Endpunkt erweiterte Berechtigungen gewähren.

Um Programme zu definieren, konfigurieren Sie die folgenden Programmlisten.

TABELLE 10-4. Programmlisten

PROGRAMMLISTE	BESCHREIBUNG	GÜLTIGE EINGABEN
Programme mit Lese- und Schreibzugriff auf Geräte	Diese Liste enthält lokale Programme und Programme auf Speichergeräten, die über Lese- und Schreibzugriff auf die Geräte verfügen. Ein Beispiel für ein solches lokales Programm ist Microsoft Word (`winword.exe`), das normalerweise unter `C:\Programme\Microsoft Office\Office` gespeichert ist. Wenn die Berechtigung für die USB-Speichergeräte "Nur Geräteinhalt auflisten" lautet, `C:\Programme\Microsoft Office\Office\winword.exe`" jedoch in dieser Liste enthalten ist: • Ein Benutzer hat Lese- und Schreibzugriff auf sämtliche Dateien auf dem USB-Speichergerät, auf die über Microsoft Word zugegriffen werden kann. • Ein Benutzer kann eine Microsoft Word-Datei auf dem USB-Speichergerät speichern, sie dorthin verschieben oder kopieren.	Programmpfad und -name Weitere Informationen finden Sie unter *Unterstützung von Platzhalterzeichen für die Liste zulässiger Programme der Gerätesteuerung auf Seite 10-9*.

PROGRAMMLISTE	BESCHREIBUNG	GÜLTIGE EINGABEN
Programme auf Geräten, die ausgeführt werden dürfen	Diese Liste enthält Programme auf Speichergeräten, die von Benutzern oder vom System ausgeführt werden können. Wenn Sie beispielsweise festlegen möchten, dass Benutzer Software von einer CD installieren können, fügen Sie den Pfad und den Namen des Installationsprogramms, z. B. "`E:\Installer\Setup.exe`", zu dieser Liste hinzu.	Programmpfad und -name oder Anbieter der digitalen Signatur Weitere Informationen finden Sie unter *Unterstützung von Platzhalterzeichen für die Liste zulässiger Programme der Gerätesteuerung auf Seite 10-9* oder *Anbieter der digitalen Signatur festlegen auf Seite 10-9*.

In manchen Fällen müssen Sie ein Programm zu beiden Listen hinzufügen. Beispiel: Wenn die Funktion zum Sperren von Daten auf einem USB-Speichergerät aktiviert ist, wird der Benutzer zur Eingabe eines gültigen Benutzernamens und Kennworts aufgefordert, um das Gerät zu entsperren. Die Funktion zum Sperren der Daten verwendet ein Programm auf dem Gerät mit der Bezeichnung "`Password.exe`". Dieses Programm muss als ausführbar konfiguriert sein, damit der Benutzer das Gerät entsperren kann. "`Password.exe`" muss außerdem Lese- und Schreibzugriff auf das Gerät besitzen, damit der Benutzer den Benutzernamen oder das Kennwort ändern kann.

Jede Programmliste auf der Benutzeroberfläche kann bis zu 100 Programme enthalten.

Wenn Sie mehr Programme zu einer Programmliste hinzufügen möchten, müssen Sie diese zur Datei `ofcscan.ini` hinzufügen, die bis zu 1.000 Programme enthalten kann. Anweisungen zum Hinzufügen von Programmen zur Datei `ofcscan.ini` finden Sie unter *Programme zu Gerätesteuerungslisten mit Hilfe von ofcscan.ini hinzufügen auf Seite 10-17*.

Warnung!

Programme, die zur Datei `ofcscan.ini` hinzugefügt wurden, werden an die Root-Domäne verteilt und überschreiben Programme auf einzelnen Domänen und agents.

Anbieter der digitalen Signatur festlegen

Legen Sie einen Anbieter der digitalen Signatur fest, wenn Sie Programmen von diesem Anbieter vertrauen. Geben Sie beispielsweise Microsoft Corporation oder Trend Micro, Inc. ein. Sie können den Anbieter der digitalen Signatur über die Eigenschaften eines Programms abrufen (indem Sie beispielsweise mit der rechten Maustaste auf das Programm klicken und **Eigenschaften** auswählen).

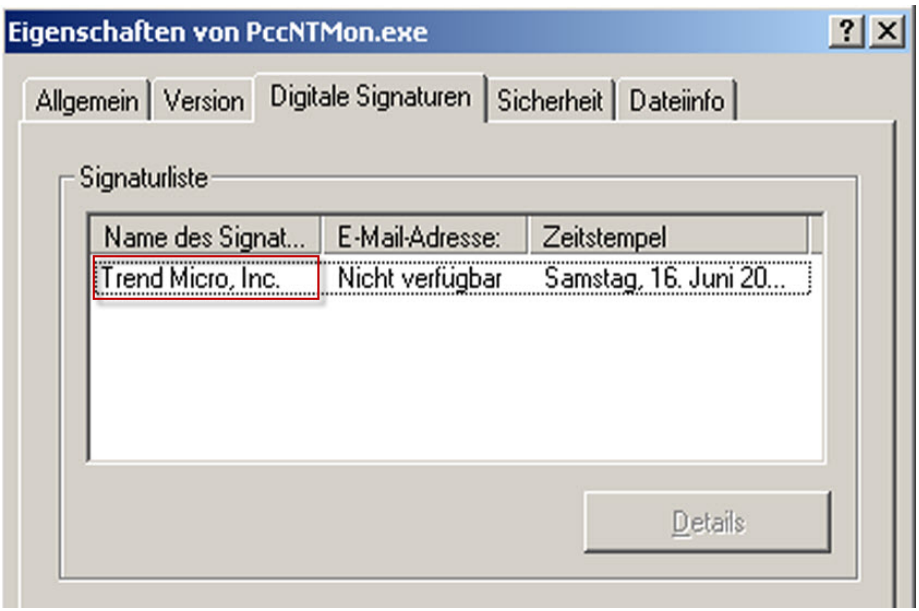


ABBILDUNG 10-1. Anbieter der digitalen Signatur für das OfficeScan Agent-Programm (`PccNTMon.exe`)

Unterstützung von Platzhalterzeichen für die Liste zulässiger Programme der Gerätesteuerung

Ein Programmpfad und -name darf maximal 259 Zeichen umfassen und nur alphanumerische Zeichen (A-Z, a-z, 0-9) enthalten. Es ist nicht möglich, nur den Programmnamen anzugeben.

Als Ersatz für Laufwerksbuchstaben und Programmnamen können Platzhalterzeichen verwendet werden. Verwenden Sie ein Fragezeichen (?), um ein einzelnes Zeichen darzustellen, z. B. einen Laufwerksbuchstaben. Verwenden Sie einen Stern (*), um mehrere Zeichen darzustellen, z. B. einen Programmnamen.

Hinweis

Platzhalter können nicht für Ordnernamen verwendet werden. Sie müssen den exakten Namen eines Ordners angeben.

In den folgenden Beispielen wurden die Platzhalter richtig verwendet:

TABELLE 10-5. Richtige Verwendung von Platzhaltern

BEISPIEL	ÜBEREINSTIMMENDE DATEN
?:\Password.exe	Die Datei "Password.exe", die sich direkt auf einem beliebigen Laufwerk befindet
C:\Programme\Microsoft*.exe	Eine beliebige Datei unter C:\Programme mit einer Dateierweiterung
C:\Programme*.*	Eine beliebige Datei unter C:\Programme mit einer Dateierweiterung
C:\Programme\a**?**c.exe	Eine beliebige .exe-Datei unter C:\Programme mit 3 Buchstaben, die mit dem Buchstaben "a" beginnt und mit dem Buchstaben "c" endet
C:*	Alle Dateien, die sich direkt auf dem Laufwerk C:\ befinden, und zwar mit oder ohne Dateierweiterung

In den folgenden Beispielen wurden die Platzhalter falsch verwendet:

TABELLE 10-6. Falsche Verwendung von Platzhaltern

BEISPIEL	GRUND
??:\Buffalo\Password.exe	?? stellt zwei Zeichen dar, und Laufwerksbuchstaben bestehen nur aus einem alphabetischen Zeichen.

BEISPIEL	GRUND
*:\Buffalo\Password.exe	* stellt mehrere Zeichen dar, und Laufwerksbuchstaben bestehen nur aus einem alphabetischen Zeichen.
C:*\Password.exe	Platzhalter können nicht für Ordnernamen verwendet werden. Sie müssen den exakten Namen eines Ordners angeben.
C:\?\Password.exe	

Berechtigungen für Nicht-Speichergeräte

Sie können den Zugriff auf Geräte, die keine Speichergeräte sind, zulassen oder sperren. Für diese Geräte gibt es keine Feineinstellungen oder erweiterten Berechtigungen.

Zugriff auf externe Geräte verwalten (Datenschutz aktiviert)

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen der Gerätesteuerung**.
4. Klicken Sie auf die Registerkarte **Externe Agents**, um Einstellungen für externe Agents zu konfigurieren, oder auf die Registerkarte **Interne Agents**, um Einstellungen für interne Agents zu konfigurieren.
5. Wählen Sie **Gerätesteuerung aktivieren**.
6. Wenden Sie die Einstellungen wie folgt an:

- Auf der Registerkarte **Externe Agents** können Sie Einstellungen auf interne Agents anwenden, indem Sie **Alle Einstellungen für interne Agents übernehmen** wählen.
- Auf der Registerkarte **Interne Agents** können Sie Einstellungen auf externe Agents anwenden, indem Sie **Alle Einstellungen für externe Agents übernehmen** wählen.

Eine Bestätigungsmeldung wird angezeigt. Warten Sie, bis der Verteilungsbefehl auf alle Agents übertragen wurde.

7. Erlauben oder sperren Sie die Autostart-Funktion (`autorun.inf`) auf USB-Speichergeräten.
8. Konfigurieren Sie die Einstellungen für Speichergeräte.
   a. Wählen Sie eine Berechtigung für jedes Speichergerät.

      Weitere Informationen zu Berechtigungen finden Sie unter *Berechtigungen für Speichergeräte auf Seite 10-4*.

   b. Wenn die Berechtigung für USB-Speichergeräte **Sperren** lautet, konfigurieren Sie eine Liste zulässiger Geräte. Benutzer können auf diese Geräte zugreifen, und Sie können die Zugriffsstufe durch Berechtigungen steuern.

      Weitere Informationen finden Sie unter *Liste der zugelassenen USB-Geräte konfigurieren auf Seite 10-14*.
9. Bei allen Geräten, die keine Speichergeräte sind, wählen Sie **Zulassen** oder **Sperren**.
10. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:
    - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
    - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option

werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Erweiterte Berechtigungen konfigurieren

Sie können zwar auf der Benutzeroberfläche erweiterte Berechtigungen und Benachrichtigungen für ein bestimmtes Speichergerät konfigurieren, die Berechtigungen und Benachrichtigungen werden dann jedoch auf alle Speichergeräte angewendet. Wenn Sie also für CD/DVD auf **Erweiterte Berechtigungen und Benachrichtigungen** klicken, definieren Sie in Wahrheit die Berechtigungen und Benachrichtigungen für alle Speichergeräte.

Hinweis

Weitere Informationen über erweiterte Berechtigungen und das richtige Definieren von Programmen mit erweiterten Berechtigungen finden Sie unter *Erweiterte Berechtigungen für Speichergeräte auf Seite 10-6*.

Prozedur

1. Klicken Sie auf **Erweiterte Berechtigungen und Benachrichtigungen**.

   Es öffnet sich ein neues Fenster.

2. Geben Sie unterhalb von **Programme mit Lese- und Schreibzugriff auf Speichergeräte** den Pfad und Dateinamen für ein Programm ein, und klicken Sie auf **Hinzufügen**.

   Anbieter der digitalen Signatur werden nicht akzeptiert.

3. Geben Sie unterhalb von **Programme auf Speichergeräten, die ausgeführt werden dürfen** den Pfad und Namen des Programms oder den Anbieter der digitalen Signatur ein, und klicken Sie auf **Hinzufügen**.

4. Wählen Sie **Benachrichtigung auf dem Endpunkt anzeigen, wenn OfficeScan unbefugten Gerätezugriff entdeckt.** aus.

- Unerlaubter Gerätezugriff bezeichnet unzulässige Geräteaktionen. Wenn die Geräteberechtigung beispielsweise "Lesen" lautet, dürfen Benutzer keine Dateien auf dem Gerät speichern, verschieben, löschen oder ausführen.
- Sie können die Benachrichtigungsmeldung ändern. Weitere Informationen finden Sie unter *Gerätesteuerungsbenachrichtigungen ändern auf Seite 10-19*.

5. Klicken Sie auf **Zurück**.

Liste der zugelassenen USB-Geräte konfigurieren

Die Liste der zulässigen USB-Geräte unterstützt die Verwendung des Sterns (*) als Platzhalter. Verwenden Sie den Stern (*) in beliebigen Feldern, um alle Geräte einzuschließen, die den Kriterien der übrigen Felder entsprechen. Beispiel: [Hersteller]-[Modell]-* platziert alle Geräte des angegebenen Herstellers und Modells in die Liste der zulässigen Geräte, unabhängig von der Seriennummer.

Prozedur

1. Klicken Sie auf **Zulässige Geräte**.
2. Geben Sie den Gerätehersteller ein.
3. Geben Sie das Gerätemodell und die Seriennummer ein.

> **Tipp**
>
> Verwenden Sie Device List, um Geräte abzufragen, die mit dem Endpunkt verbunden sind. Das Tool liefert den Hersteller, das Modell und die Seriennummer für jedes Gerät.

4. Wählen Sie die Berechtigung für dieses Gerät.

   Weitere Informationen zu Berechtigungen finden Sie unter *Berechtigungen für Speichergeräte auf Seite 10-4*.

5. Um weitere Geräte hinzuzufügen, klicken Sie auf das Plus-Symbol (**+**).

6. Klicken Sie auf **< Zurück**.

Device List

Führen Sie Device List an jedem Endpunkt lokal aus, um externe Geräte abzufragen, die mit dem Endpunkt verbunden sind. Das Tool überprüft einen Endpunkt nach externen Geräten und zeigt die entdeckten Geräte dann in einem Browser-Fenster an. Diese Informationen können Sie zur Konfiguration von Geräteeinstellungen bei der Funktion "Prävention vor Datenverlust" und der Gerätesteuerung verwenden.

Das Gerätelisten-Tool ausführen

Prozedur

1. Navigieren Sie auf dem OfficeScan Server-Computer zu <*Installationsordner des Servers auf Seite xvi*>`\PCCSRV\Admin\Utility\ListDeviceInfo`.
2. Kopieren Sie die Datei `listDeviceInfo.exe` auf den Ziel-Endpunkt.
3. Führen Sie auf dem Endpunkt `listDeviceInfo.exe` aus.
4. Es öffnet sich ein Browser-Fenster mit Informationen zu den Geräten. Die Funktion 'Prävention vor Datenverlust' und die Gerätesteuerung verwenden folgende Informationen:
   - Hersteller (erforderlich)
   - Modell (optional)
   - Seriennummer (optional)

Zugriff auf externe Geräte verwalten (Datenschutz nicht aktiviert)

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen der Gerätesteuerung**.
4. Klicken Sie auf die Registerkarte **Externe Agents**, um Einstellungen für externe Agents zu konfigurieren, oder auf die Registerkarte **Interne Agents**, um Einstellungen für interne Agents zu konfigurieren.
5. Wählen Sie **Gerätesteuerung aktivieren**.
6. Wenden Sie die Einstellungen wie folgt an:
   - Auf der Registerkarte **Externe Agents** können Sie Einstellungen auf interne Agents anwenden, indem Sie **Alle Einstellungen für interne Agents übernehmen** wählen.
   - Auf der Registerkarte **Interne Agents** können Sie Einstellungen auf externe Agents anwenden, indem Sie **Alle Einstellungen für externe Agents übernehmen** wählen.

   Eine Bestätigungsmeldung wird angezeigt. Warten Sie, bis der Verteilungsbefehl auf alle Agents übertragen wurde.
7. Erlauben oder sperren Sie die Autostart-Funktion (`autorun.inf`) auf USB-Speichergeräten.
8. Wählen Sie eine Berechtigung für jedes Speichergerät.
9. Konfigurieren Sie erweiterte Berechtigungen und Benachrichtigungen, falls eine der folgenden Berechtigungen für ein Speichergerät vorliegt: **Ändern**, **Lesen und ausführen**, **Lesen** oder **Nur Geräteinhalt auflisten**.

Weitere Informationen finden Sie unter *Erweiterte Berechtigungen konfigurieren auf Seite 10-13*.

10. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

    - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
    - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Programme zu Gerätesteuerungslisten mit Hilfe von ofcscan.ini hinzufügen

Hinweis

Weitere Informationen über Programmlisten und das richtige Definieren von Programmen, die zu diesen Listen hinzugefügt werden können, finden Sie unter *Erweiterte Berechtigungen für Speichergeräte auf Seite 10-6*.

Prozedur

1. Navigieren Sie auf dem OfficeScan Server-Computer zu <*Installationsordner des Servers*>`\PCCSRV`.
2. Öffnen Sie die Datei `ofcscan.ini` mit Hilfe eines Texteditors.
3. Programme mit Lese- und Schreibzugriff auf Speichergeräte hinzufügen:
   a. Suchen Sie die folgenden Zeilen:

      ```
      [DAC_APPROVED_LIST]
      ```

```
Count=x
```

b. Ersetzen Sie das "x" durch die Anzahl der Programme in der Programmliste.

c. Fügen Sie unterhalb von "Count=x" Programme hinzu, indem Sie Folgendes eingeben:

```
Element<Anzahl>=<Programmpfad und -name oder Anbieter
der digitalen Signatur>
```

Beispiel:

```
[DAC_APPROVED_LIST]

Count=3

Item0=C:\Programme\program.exe

Item1=?:\password.exe

Item2=Microsoft Corporation
```

4. Programme auf Speichergeräten, die ausgeführt werden dürfen, hinzufügen:

a. Suchen Sie die folgenden Zeilen:

```
[DAC_EXECUTABLE_LIST]

Count=x
```

b. Ersetzen Sie das "x" durch die Anzahl der Programme in der Programmliste.

c. Fügen Sie unterhalb von "Count=x" Programme hinzu, indem Sie Folgendes eingeben:

```
Element<Anzahl>=<Programmpfad und -name oder Anbieter
der digitalen Signatur>
```

Beispiel:

```
[DAC_EXECUTABLE_LIST]

Count=3

Item0=?:\Installer\Setup.exe
```

```
Item1=E:\*.exe

Item2=Trend Micro, Inc.
```

5. Speichern und schließen Sie die Datei `ofcscan.ini`.
6. Öffnen Sie die OfficeScan Webkonsole und navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
7. Klicken Sie auf **Speichern**, um die Programmlisten auf alle agents zu verteilen.

Gerätesteuerungsbenachrichtigungen ändern

Bei Verstößen gegen die Gerätesteuerung werden Benachrichtigungen auf den Endpunkten angezeigt. Administratoren können bei Bedarf die Standardbenachrichtigung ändern.

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Agent**.
2. Wählen Sie im Listenfeld **Typ** die Option **Verstöße gegen die Gerätesteuerung** aus.
3. Sie können die Standardmeldungen im dafür vorgesehenen Textfeld bearbeiten.
4. Klicken Sie auf **Speichern**.

Protokolle der Gerätesteuerung

Die OfficeScan Agents protokollieren unbefugte Gerätezugriffe und senden die Protokolle an den Server. Standardmäßig fasst ein agent, der kontinuierlich läuft, die Protokolle zusammen und sendet sie 1 Mal pro Stunde. Nach einem Neustart überprüft der agent, wann die Protokolle das letzte Mal an den Server gesendet wurden. Wenn seitdem mehr als 1 Stunde verstrichen ist, sendet der agent die Protokolle sofort.

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell, oder konfigurieren Sie eine zeitgesteuerte Löschung der Protokolle. Weitere Informationen zur Protokollverwaltung finden Sie unter *Protokollmanagement auf Seite 14-47*.

Protokolle der Gerätesteuerung anzeigen

Hinweis

Nur Zugriffsversuche auf **Speichergeräte** werden protokolliert. OfficeScan Agents Agents sperren oder erlauben den Zugriff auf **Nicht-Speichergeräte** gemäß Konfiguration, aber diese Aktionen werden nicht protokolliert.

Prozedur

1. Navigieren Sie zu **Protokolle** > **Agents** > **Sicherheitsrisiken** oder **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Protokolle** > **Protokolle der Gerätesteuerung** oder auf **Protokolle anzeigen** > **Protokolle der Gerätesteuerung**.
4. Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.
5. Sehen Sie die Protokolle ein. Die Protokolle enthalten die folgenden Informationen:
   - Datum/Uhrzeit, als der unbefugte Zugriff entdeckt wurde.
   - Endpunkt , mit dem das externe Gerät verbunden oder dem die Netzwerkressource zugewiesen ist.
   - Endpunkt -Domäne, mit der das externe Gerät verbunden oder der die Netzwerkressource zugewiesen ist.
   - Gerätetyp oder Netzwerkressource, auf den/die zugegriffen wurde.

- Ziel, bei dem es sich um das Element auf dem Gerät oder der Netzwerkressource handelt, auf das der Zugriff erfolgt ist
- Zugriff durch, d. h. die Angabe, wo der Zugriff initiiert wurde.
- Für das Ziel festgelegte Berechtigungen.

6. Wenn Sie das Protokoll als komma-separierte Datei (`CSV-Datei`) speichern möchten, klicken Sie auf **In CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Kapitel 11

Prävention vor Datenverlust verwenden

In diesem Kapitel wird erläutert, wie Sie die Funktion der Prävention vor Datenverlust verwenden.

Es werden folgende Themen behandelt:

- *Prävention vor Datenverlust (Data Loss Prevention, DLP) auf Seite 11-2*
- *Richtlinien für 'Prävention vor Datenverlust' auf Seite 11-3*
- *Datenbezeichnertypen auf Seite 11-6*
- *Vorlagen für 'Prävention vor Datenverlust' auf Seite 11-22*
- *DLP-Kanäle auf Seite 11-27*
- *Aktionen der Funktion "Prävention vor Datenverlust" auf Seite 11-42*
- *Ausnahmen für Prävention vor Datenverlust auf Seite 11-45*
- *Richtlinienkonfiguration der Funktion "Prävention vor Datenverlust" auf Seite 11-51*
- *Benachrichtigungen der Funktion "Prävention vor Datenverlust" auf Seite 11-58*
- *Protokolle für 'Prävention vor Datenverlust' auf Seite 11-63*

Prävention vor Datenverlust (Data Loss Prevention, DLP)

Der Schwerpunkt herkömmlicher Sicherheitslösungen liegt darin, zu verhindern, dass externe Sicherheitsbedrohungen in das Netzwerk eindringen. In der heutigen Sicherheitsumgebung deckt dies nur einen Teil der erforderlichen Aufgaben ab. Datenschutzverletzungen, die vertrauliche und sensitive Daten (digitale Assets) einer Organisation an außenstehende unbefugte Dritte weitergeben, sind heute gang und gäbe. Gründe für eine Datenschutzverletzung können Fehler oder Sorglosigkeit interner Mitarbeiter, Datenauslagerung, gestohlene oder verlegte Computer oder bösartige Angriffe sein.

Datenschutzverletzungen können:

- Das Markenimage schädigen
- Das Vertrauen der Kunden in das Unternehmen schwächen
- Unnötige Kosten für Schadenswiedergutmachung und Strafen wegen Richtlinienverstößen verursachen
- Zum Verlust von Geschäftschancen und zu Umsatzeinbußen durch entwendetes geistiges Eigentum führen

Auf Grund der Zunahme der schädlichen Auswirkungen durch Datenschutzverletzungen sehen Unternehmen mittlerweile den Schutz ihrer digitalen Assets als eine kritische Komponente in ihrer Sicherheitsinfrastruktur.

Die Funktion "Prävention vor Datenverlust" schützt die vertraulichen Daten eines Unternehmens vor versehentlichen oder beabsichtigten Lecks. Die Funktion "Prävention vor Datenverlust" ermöglicht Folgendes:

- Vertrauliche Informationen, die geschützt werden müssen, mit Hilfe von Datenbezeichnern identifizieren
- Richtlinien erstellen, die die übertragung von digitalen Assets über gemeinsam genutzte übertragungskanäle wie E-Mail und externe Geräte einschränken oder verhindern
- Die Einhaltung bewährter Datenschutzstandards durchsetzen

Um vertrauliche Informationen hinsichtlich eines potentiellen Verlusts überwachen zu können, müssen Sie die folgenden Fragen beantworten können:

- Welche Daten müssen vor unberechtigten Benutzern geschützt werden?
- Wo befinden sich die sensiblen Daten?
- Wie werden die sensiblen Daten übertragen?
- Welche Benutzer sind berechtigt, auf die sensiblen Daten zuzugreifen oder diese zu übertragen?
- Welche Maßnahmen sollten ergriffen werden, wenn eine Sicherheitsverletzung auftritt?

Diese wichtige Überprüfung betrifft in der Regel mehrere Abteilungen und Mitarbeiter, die mit den sensiblen Informationen in Ihrer Organisation vertraut sind.

Wenn Sie Ihre vertraulichen Informationen und Sicherheitsrichtlinien bereits definiert haben, können Sie damit beginnen, Datenbezeichner und Unternehmensrichtlinien zu definieren.

Richtlinien für 'Prävention vor Datenverlust'

OfficeScan überprüft eine Datei oder Daten anhand einer Reihe von Regeln, die in den DLP-Richtlinien definiert sind. Richtlinien legen die Dateien oder Daten fest, die vor einer unbefugten Übertragung geschützt werden müssen, und bestimmen die Aktion, die OfficeScan durchführt, wenn eine Übertragung erkannt wurde.

Hinweis

Datenübertragungen zwischen dem Server und OfficeScan werden von OfficeScan Agents nicht überwacht.

OfficeScan ermöglicht Administratoren die Konfiguration von Richtlinien für interne und externe OfficeScan Agents. In der Regel konfigurieren Administratoren eine strengere Richtlinie für externe agents.

Administratoren können bestimmte Richtlinien für agent-Gruppen oder einzelne agents erzwingen.

Nachdem Sie die Richtlinien verteilt haben, verwenden die agents die Standortkriterien, die Sie im Fenster **Endpunktspeicherort** festgelegt haben (siehe *Endpunktspeicherort auf Seite 15-2*), um deren Standort und die erforderliche Richtlinie zu bestimmen. Agents wechseln die Richtlinien mit jedem Standortwechsel.

Richtlinienkonfiguration

Sie definieren DLP-Richtlinien durch die Konfiguration der folgenden Einstellungen und deren Bereitstellung an ausgewählte agents:

TABELLE 11-1. Einstellungen zur Definition einer DLP-Richtlinie

EINSTELLUNGEN	BESCHREIBUNG
Regeln	Eine DLP-Regel kann aus mehreren Vorlagen, Kanälen und Aktionen bestehen. Jede Regel ist dabei eine Unterkategorie der betreffenden DLP-Richtlinie. **Hinweis** Die Prävention vor Datenverlust verarbeitet Regeln und Vorlagen anhand der Priorität. Wenn für eine Regel „Übergehen“ festgelegt ist, wird von der Prävention vor Datenverlust die nächste Regel in der Liste verarbeitet. Wenn für eine Regel „Sperren“ oder „Benutzerrechtfertigung“ festgelegt ist, wird die Benutzeraktion von der Prävention vor Datenverlust gesperrt oder akzeptiert, und diese Regel/Vorlage wird nicht weiter verarbeitet.

Einstellungen	Beschreibung
Vorlagen	Eine DLP-Vorlage verbindet Datenbezeichner mit logischen Operatoren (Und, Oder, Außer) zur Erstellung von Bedingungsanweisungen. Nur Dateien oder Daten, die einer bestimmten Bedingungsanweisung entsprechen, unterliegen einer DLP-Regel. Die Prävention vor Datenverlust verfügt bereits über mehrere vordefinierte Vorlagen, Administratoren können aber auch eigene Vorlagen erstellen. Eine DLP-Regel kann eine oder mehrere Vorlagen enthalten. Die Prävention vor Datenverlust verwendet beim Prüfen von Vorlagen die Regel der ersten Übereinstimmung. Das bedeutet, dass die Prävention vor Datenverlust keine weiteren Vorlagen prüft, sobald eine Übereinstimmung zwischen den Dateien bzw. Daten einerseits und den Datenbezeichnern in einer Vorlage andererseits vorliegt.
Kanäle	Kanäle sind Einheiten, die vertrauliche Informationen übertragen. Die Prävention vor Datenverlust unterstützt die gängigen Übertragungskanäle wie E-Mails, Wechselspeichermedien und Instant-Messaging-Anwendungen.
Aktionen	Die Prävention vor Datenverlust führt eine oder mehrere Aktionen durch, wenn der Versuch zur Übertragung vertraulicher Informationen über einen dieser Kanäle entdeckt wird.
Ausnahmen	Ausnahmen setzen konfigurierte DLP-Regeln außer Kraft. Sie können Ausnahmen konfigurieren, um nicht überwachte und überwachte Ziele sowie die Suche in komprimierten Dateien zu verwalten.
Datenbezeichner	Die Prävention vor Datenverlust verwendet Datenbezeichner zum Identifizieren vertraulicher Informationen. Datenbezeichner umfassen Ausdrücke, Dateiattribute und Schlüsselwörter, aus denen sich die DLP-Vorlagen zusammensetzen.

Datenbezeichnertypen

Digitale Assets sind Dateien und Daten, die ein Unternehmen vor unbefugter Übertragung schützen muss. Datenbezeichner können von Administratoren mit folgenden Methoden definiert werden:

- **Ausdrücke**: Daten mit einer bestimmten Struktur.

  Weitere Informationen finden Sie unter *Ausdrücke auf Seite 11-6*.

- **Dateiattribute**: Dateieigenschaften wie Dateityp und Dateigröße.

  Weitere Informationen finden Sie unter *Dateiattribute auf Seite 11-11*.

- **Schlüsselwortlisten**: Eine Liste bestimmter Wörter oder Phrasen.

  Weitere Informationen finden Sie unter *Schlüsselwörter auf Seite 11-15*.

Hinweis

Administratoren können einen Datenbezeichner nicht löschen, der in einer DLP-Vorlage verwendet wird. Löschen Sie die Vorlage, bevor Sie den Datenbezeichner löschen.

Ausdrücke

Ein Ausdruck enthält Daten mit einer bestimmten Struktur. Zum Beispiel bestehen Kreditkartennummern normalerweise aus 16 Ziffern im Format "nnnn-nnnn-nnnn-nnnn", weshalb sie sich für die ausdrucksbasierte Erkennung gut eignen.

Administratoren können vordefinierte und benutzerdefinierte Ausdrücke verwenden.

Weitere Informationen finden Sie unter *Vordefinierte Ausdrücke auf Seite 11-6* und *Benutzerdefinierte Ausdrücke auf Seite 11-7*.

Vordefinierte Ausdrücke

Im Lieferumfang der Prävention vor Datenverlust ist eine Reihe vordefinierter Ausdrücke enthalten. Diese Ausdrücke können weder geändert noch gelöscht werden.

Die Prävention vor Datenverlust überprüft diese Ausdrücke und verwendet hierfür den Pattern-Abgleich und mathematische Gleichungen. Nachdem die Prävention vor Datenverlust möglicherweise sensible Daten mit einem Ausdruck abgeglichen hat, werden für die Daten unter Umständen zusätzliche Überprüfungen durchgeführt.

Eine vollständige Liste der vordefinierten Ausdrücke finden Sie in der *Datenschutzliste* unter http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Einstellungen für vordefinierte Ausdrücke anzeigen

Hinweis

Vordefinierte Ausdrücke können weder geändert noch gelöscht werden.

Prozedur

1. Navigieren Sie zu **Agents** > **Prävention vor Datenverlust** > **Datenbezeichner**.
2. Klicken Sie auf die Registerkarte **Ausdruck**.
3. Klicken Sie auf den Namen des Ausdrucks.
4. Es öffnet sich ein Fenster mit den Einstellungen.

Benutzerdefinierte Ausdrücke

Erstellen Sie benutzerdefinierte Ausdrücke, wenn keiner der vorhandenen Ausdrücke den Anforderungen Ihres Unternehmens entspricht.

Ausdrücke sind ein mächtiges Werkzeug zum Abgleichen von Zeichenketten. Machen Sie sich mit der Syntax von Ausdrücken vertraut, bevor Sie selbst Ausdrücke erstellen. Fehlerhaft formulierte Ausdrücke können die Leistung stark beeinträchtigen.

Hinweise zum Erstellen von Ausdrücken:

- Orientieren Sie sich zum Erstellen gültiger Ausdrücke an den vordefinierten Ausdrücken. Wenn Sie zum Beispiel einen Ausdruck erstellen, in dem ein Datum enthalten ist, können Sie sich auf die Ausdrücke mit dem Präfix "Datum" beziehen.

- Beachten Sie, dass die Prävention vor Datenverlust die in der PCRE-Bibliothek (Perl-kompatible reguläre Ausdrücke) definierten Ausdrucksformate verwendet. Weitere Informationen zu PCRE finden Sie auf der folgenden Website:

  http://www.pcre.org/

- Beginnen Sie mit einfachen Ausdrücken. Verändern Sie die Ausdrücke, wenn sie Fehlarme verursachen, oder machen Sie eine Feinabstimmung, um die Erkennungsrate zu verbessern.

Administratoren stehen beim Erstellen von Ausdrücken eine Reihe von Kriterien zur Verfügung. Ein Ausdruck muss die gewählten Kriterien erfüllen, damit die Prävention vor Datenverlust ihn für eine DLP-Richtlinie akzeptiert. Weitere Informationen zu den einzelnen Kriterienoptionen finden Sie unter *Kriterien für benutzerdefinierte Ausdrücke auf Seite 11-8*.

Kriterien für benutzerdefinierte Ausdrücke

TABELLE 11-2. Kriterienoptionen für benutzerdefinierte Ausdrücke

KRITERIEN	REGEL	BEISPIEL
Keine	Keine	Alle - Namen gemäß den Angaben des Statistischen Bundesamtes der Vereinigten Staaten • Ausdruck: [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
Bestimmte Zeichen	In einem Ausdruck müssen die von Ihnen vorgegebenen Zeichen enthalten sein. Außerdem muss die Zeichenanzahl in einem Ausdruck innerhalb der vorgegebenen Mindest- und Höchstgrenzen liegen.	US - ABA-Routing-Nummer • Ausdruck: [^\d]([0123678]\d{8})[^\d] • Zeichen: 0123456789 • Mindestanzahl von Zeichen: 9 • Höchstanzahl von Zeichen: 9

Kriterien	Regel	Beispiel
Erweiterung	Als Suffix wird das letzte Segment in einem Ausdruck bezeichnet. In einem Suffix müssen die Zeichen enthalten sein, die Sie angegeben haben, und es muss aus einer bestimmten Anzahl von Zeichen bestehen. Außerdem muss die Zeichenanzahl in einem Ausdruck innerhalb der vorgegebenen Mindest- und Höchstgrenzen liegen.	Alle - Privatadresse • Ausdruck: \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave| road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\s\d{5}(-\d{4})?)[^\d-] • Suffix-Zeichen: 0123456789- • Anzahl von Zeichen: 5 • Mindestzeichenanzahl im Ausdruck: 25 • Höchstzeichenanzahl im Ausdruck: 80
Trennzeichen aus einem Zeichen	Ein Ausdruck muss aus zwei Segmenten bestehen, die mit einem Zeichen getrennt sind. Das Zeichen muss eine Länge von 1 Byte haben. Außerdem muss die Zeichenanzahl links vom Trennzeichen innerhalb der vorgegebenen Mindest- und Höchstgrenzen liegen. Die Zeichenanzahl rechts vom Trennzeichen darf die Höchstgrenze nicht überschreiten.	Alle - E-Mail-Adresse • Ausdruck: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • Trennzeichen: @ • Mindestzeichenanzahl links: 3 • Höchstzeichenanzahl links: 15 • Höchstzeichenanzahl rechts: 30

Benutzerdefinierte Ausdrücke erstellen

Prozedur

1. Navigieren Sie zu **Agents** > **Prävention vor Datenverlust** > **Datenbezeichner**.

2. Klicken Sie auf die Registerkarte **Ausdruck**.
3. Klicken Sie auf **Hinzufügen**.

   Ein neues Fenster wird geöffnet.
4. Geben Sie einen Namen für den Ausdruck ein. Der Name darf nicht länger als 100 Byte sein und folgende Zeichen dürfen nicht enthalten sein:
   - > < * ^ | & ? \ /
5. Geben Sie eine Beschreibung mit maximal 256 Byte ein.
6. Geben Sie die Daten ein, die angezeigt werden sollen.

   Wenn Sie zum Beispiel einen Ausdruck für Seriennummern erstellen, geben Sie das Muster einer Seriennummer ein. Die Daten sind nur zur Dokumentation, sie erscheinen an keiner anderen Stelle im Produkt.
7. Wählen Sie eine der folgenden Kriterien, und konfigurieren Sie zusätzliche Einstellungen für die ausgewählten Kriterien (siehe *Kriterien für benutzerdefinierte Ausdrücke auf Seite 11-8*):
   - Keine
   - Bestimmte Zeichen
   - Erweiterung
   - Trennzeichen aus einem Zeichen
8. Testen Sie den Ausdruck mit tatsächlichen Daten.

   Wenn der Ausdruck zum Beispiel für eine Personalausweisnummer steht, geben Sie eine gültige Ausweisnummer in das Textfeld **Testdaten** ein und klicken auf **Testen**; überprüfen Sie anschließend das Ergebnis.
9. Klicken Sie auf **Speichern**, wenn Sie mit dem Ergebnis zufrieden sind.

Hinweis

Speichern Sie die Einstellungen nur, wenn der Test erfolgreich war. Ein Ausdruck, der keine Daten entdeckt, verschwendet Systemressourcen und kann die Leistung beeinträchtigen.

10. Eine Meldung erinnert Sie daran, die Einstellungen auf die agents zu verteilen. Klicken Sie auf **Schließen**.

11. Wenn Sie sich wieder im Fenster **DLP-Datenbezeichner** befinden, klicken Sie auf **Auf alle Agents anwenden**.

Benutzerdefinierte Ausdrücke importieren

Verwenden Sie diese Option, wenn Sie über eine ordnungsgemäß formatierte `.DAT`-Datei verfügen, in der die Ausdrücke gespeichert sind. Sie können die Datei erzeugen, indem Sie die Ausdrücke entweder über den Server, auf den Sie gerade zugreifen, oder über einen anderen Server exportieren.

Hinweis

Die `.DAT`-Ausdrucksdateien, die von dieser Version der Prävention vor Datenverlust generiert wurden, sind mit vorherigen Versionen nicht kompatibel.

Prozedur

1. Navigieren Sie zu **Agents** > **Prävention vor Datenverlust** > **Datenbezeichner**.
2. Klicken Sie auf die Registerkarte **Ausdruck**.
3. Klicken Sie auf **Importieren**, und suchen Sie dann die `.DAT`-Datei, in der die Ausdrücke enthalten sind.
4. Klicken Sie auf **Öffnen**.

   Sie erhalten eine Nachricht, wenn der Import erfolgreich war. Wenn ein Ausdruck importiert werden soll, der bereits vorhanden ist, wird er übersprungen.
5. Klicken Sie auf **Auf alle Agents anwenden**.

Dateiattribute

Dateiattribute sind bestimmte Eigenschaften einer Datei. Sie können zwei Dateiattribute zur Definition von Datenbezeichnern verwenden: Dateityp und Dateigröße. Nehmen

wir an, ein Software-Entwickler möchte, dass sein firmeneigenes Software-Installationsprogramm nur an die R&D-Abteilung weitergegeben wird, deren Mitglieder für die Entwicklung und das Testen der Software zuständig sind. In diesen Fall kann der OfficeScan Administrator eine Richtlinie erstellen, mit der die Übertragung ausführbarer Dateien mit einer Größe von 10 bis 40 MB auf alle Abteilungen, mit Ausnahme von R&D, gesperrt wird.

Dateiattribute sind an sich schlechte Indikatoren für sensible Dateien. Wenn wir unser Beispiel von oben weiterführen, werden Software-Installationsprogramme anderer Hersteller höchstwahrscheinlich gesperrt. Trend Micro empfiehlt deshalb die Kombination von Dateiattributen mit anderen DLP-Datenbezeichnern, um eine gezieltere Erkennung sensibler Dateien zu ermöglichen.

Eine vollständige Liste der unterstützten Dateitypen finden Sie in der *Datenschutzliste* unter http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Liste vordefinierter Dateiattribute

Im Lieferumfang der Prävention vor Datenverlust ist eine Liste vordefinierter Dateiattribute enthalten. Diese Liste kann weder geändert noch gelöscht werden. Die Liste hat ihre eigenen integrierten Bedingungen, die festlegen, ob die Vorlage einen Richtlinienverstoß auslösen soll.

Mit der Liste vordefinierter Dateiattribute können Sie den Zugriff auf Datenspeicher (CD/DVD) einschränken.

Weitere Informationen finden Sie unter *Zugriff auf Datenspeicher (CD/DVD) blockieren auf Seite 11-37*.

Eine Dateiattributliste erstellen

Prozedur

1. Navigieren Sie zu **Agents** > **Prävention vor Datenverlust** > **Datenbezeichner**.
2. Klicken Sie auf die Registerkarte **Dateiattribut**.

3. Klicken Sie auf **Hinzufügen**.

   Ein neues Fenster wird geöffnet.

4. Geben Sie einen Namen für die Dateiattributliste ein. Der Name darf nicht länger als 100 Byte sein und folgende Zeichen dürfen nicht enthalten sein:

   - > < * ^ | & ? \ /

5. Geben Sie eine Beschreibung mit maximal 256 Byte ein.

6. Wählen Sie die gewünschten ursprünglichen Dateitypen aus.

7. Wenn ein Dateityp, den Sie einschließen möchten, nicht in der Liste steht, wählen Sie **Dateierweiterungen** aus, und geben Sie anschließend die Erweiterung des Dateityps ein. Die Prävention vor Datenverlust überprüft Dateien mit der angegebenen Erweiterung, prüft aber nicht deren tatsächliche Dateitypen. Richtlinien beim Festlegen von Dateierweiterungen:

   - Jede Erweiterung muss mit einem Stern (*) beginnen, gefolgt von einem Punkt (.) und danach der Erweiterung. Der Stern ist ein Platzhalter, der für den tatsächlichen Dateinamen steht. Beispiel: `*.pol` stimmt mit `12345.pol` und `test.pol` überein.

   - Sie können Platzhalter in Erweiterungen einschließen. Mit einem Fragezeichen (?) können Sie ein einzelnes Zeichen und mit einem Stern (*) zwei oder mehr Zeichen darstellen. Beispiele dafür finden Sie nachstehend:

     - `*.*m` stimmt mit den folgenden Dateien überein: `ABC.dem`, `ABC.prm`, `ABC.sdcm`

     - `*.m*r` stimmt mit den folgenden Dateien überein: `ABC.mgdr`, `ABC.mtp2r`, `ABC.mdmr`

     - `*.fm?` stimmt mit den folgenden Dateien überein: `ABC.fme`, `ABC.fml`, `ABC.fmp`

   - Gehen Sie beim Hinzufügen eines Sterns am Ende einer Erweiterung besonders sorgfältig vor, da dieser Platzhalter mit Teilen eines Dateinamens oder einer nicht zugehörigen Erweiterung übereinstimmen kann. Beispiel: `*.do*` stimmt mit `abc.doctor_john.jpg` und `abc.donor12.pdf` überein.

- Verwenden Sie Strichpunkte (;), um mehrere Dateierweiterungen zu trennen. Sie müssen nach einem Strichpunkt kein Leerzeichen einfügen.

8. Geben Sie die minimale und maximale Dateigröße in Byte ein. Beide Dateigrößen müssen ganze Zahlen größer als null sein.
9. Klicken Sie auf **Speichern**.
10. Eine Meldung erinnert Sie daran, die Einstellungen auf die agents zu verteilen. Klicken Sie auf **Schließen**.
11. Wenn Sie sich wieder im Fenster **DLP-Datenbezeichner** befinden, klicken Sie auf **Auf alle Agents anwenden**.

Eine Dateiattributliste importieren

Verwenden Sie diese Option, wenn Sie über eine ordnungsgemäß formatierte `.dat`-Datei verfügen, in der die Dateiattributlisten gespeichert sind. Sie können die Datei erzeugen, indem Sie die Dateiattributlisten entweder über den Server, auf den Sie gerade zugreifen, oder über einen anderen Server exportieren.

Hinweis

Die `.dat`-Dateiattributdateien, die von dieser Version der Prävention vor Datenverlust generiert wurden, sind mit vorherigen Versionen nicht kompatibel.

Prozedur

1. Navigieren Sie zu **Agents** > **Prävention vor Datenverlust** > **Datenbezeichner**.
2. Klicken Sie auf die Registerkarte **Dateiattribut**.
3. Klicken Sie auf **Importieren** und suchen Sie dann die `.dat`-Datei, in der die Dateiattributlisten enthalten sind.
4. Klicken Sie auf **Öffnen**.

   Sie erhalten eine Nachricht, wenn der Import erfolgreich war. Wenn eine Dateiattributliste importiert werden soll, die bereits vorhanden ist, wird sie übersprungen.

5. Klicken Sie auf **Auf alle Agents anwenden**.

Schlüsselwörter

Schlüsselwörter sind besondere Wörter oder Phrasen. Sie können miteinander verwandte Schlüsselwörter in eine Schlüsselwortliste eintragen, um bestimmte Arten von Daten zu identifizieren. Zum Beispiel sind "Prognose", "Blutgruppe", "Impfung" und "Arzt" Schlüsselwörter, die in einem Gesundheitsattest stehen könnten. Wenn Sie die Übertragung von Dateien mit Gesundheitsattesten verhindern wollen, können Sie diese Schlüsselwörter in einer DLP-Richtlinie verwenden und dann die Prävention vor Datenverlust so konfigurieren, dass Dateien mit diesen Schlüsselwörtern gesperrt werden.

Häufig benutzte Wörter können zu bedeutungsvollen Schlüsselwörtern kombiniert werden. Zum Beispiel können die Begriffe "end", "read", "if" and "at" zu Schlüsselwörtern in Quellcodes kombiniert werden, zum Beispiel als "END-IF", "END-READ" und "AT END".

Sie können vordefinierte und benutzerdefinierte Schlüsselwortlisten verwenden. Weitere Informationen finden Sie unter *Vordefinierte Schlüsselwortlisten auf Seite 11-15* und *Benutzerdefinierte Schlüsselwortlisten auf Seite 11-17*.

Vordefinierte Schlüsselwortlisten

Im Lieferumfang der Prävention vor Datenverlust ist eine Reihe vordefinierter Schlüsselwortlisten enthalten. Diese Schlüsselwortlisten können nicht geändert bzw. gelöscht werden. Jede Liste hat ihre eigenen integrierten Bedingungen, die festlegen, ob die Vorlage einen Richtlinienverstoß auslösen soll.

Weitere Informationen zu vordefinierten Schlüsselwortlisten in der Prävention vor Datenverlust finden Sie in der *Datenschutzliste* unter http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Wie funktionieren Schlüsselwortlisten?

Bedingung "Anzahl der Schlüsselwörter"

Jede Schlüsselwortliste enthält eine Bedingung, mit der eine bestimmte Anzahl an Schlüsselwörtern festgelegt wird, die in einem Dokument enthalten sein muss, bevor die Liste einen Verstoß meldet.

Die Bedingung für die Anzahl der Schlüsselwörter enthält die folgenden Werte:

- **Alle**: Alle Schlüsselwörter in der Liste müssen im Dokument vorhanden sein.
- **Beliebig**: Eines der Schlüsselwörter in der Liste muss im Dokument vorhanden sein.
- **Bestimmte Anzahl**: Es muss mindestens die angegebene Anzahl an Schlüsselwörtern im Dokument enthalten sein. Wenn das Dokument mehr Schlüsselwörter als die angegebene Anzahl enthält, meldet die Prävention vor Datenverlust einen Verstoß.

Abstandsbedingung

Einige der Listen enthalten eine Abstandsbedingung zum Ermitteln eines Verstoßes. "Abstand" bezieht sich auf die Anzahl der Zeichen zwischen dem ersten Zeichen eines Schlüsselworts und dem ersten Zeichen eines anderen Schlüsselworts. Betrachten Sie den folgenden Eintrag:

F**irst Name:_John_ L**ast Name:_Smith_

Die Liste **Formulare - Vorname, Nachname** hat eine Abstandsbedingung von 50 und enthält die häufig verwendeten Formularfelder "Vorname" und "Nachname". Im obigen Beispiel meldet die Prävention vor Datenverlust einen Verstoß, da die Anzahl der Zeichen zwischen dem "F" in "First Name" und dem "L" in "Last Name" 18 beträgt.

Nachfolgend finden Sie ein Beispiel für einen Eintrag, der keinen Verstoß darstellt:

The f**irst name of our new employee from Switzerland is John. His l**ast name is Smith.

In diesem Beispiel beträgt die Anzahl der Zeichen zwischen dem "f" in "first name" und dem "l" in "last name" 72. Dieser Wert überschreitet den Abstandsschwellenwert und stellt keinen Verstoß dar.

Benutzerdefinierte Schlüsselwortlisten

Erstellen Sie benutzerdefinierte Schlüsselwortlisten, wenn keine der vorhandenen Schlüsselwortlisten Ihren Anforderungen entspricht.

Beim Erstellen einer Schlüsselwortliste können Sie aus mehreren Kriterien wählen. Eine Schlüsselwortliste muss die gewählten Kriterien erfüllen, damit die Prävention vor Datenverlust sie für eine Richtlinie berücksichtigt. Wählen Sie eine der folgenden Kriterien für jede Schlüsselwortliste:

- **Beliebiges Schlüsselwort**
- **Alle Schlüsselwörter**
- **Alle Schlüsselwörter innerhalb von <x> Zeichen**
- **Die Gesamtbewertung für Schlüsselwörter ist größer als Grenzwert**

Details zu den Kriterienregeln finden Sie unter *Kriterien für benutzerdefinierte Schlüsselwortlisten auf Seite 11-17*.

Kriterien für benutzerdefinierte Schlüsselwortlisten

TABELLE 11-3. Kriterien für eine Schlüsselwortliste

KRITERIEN	REGEL
Beliebiges Schlüsselwort	Eine Datei muss mindestens ein Schlüsselwort aus der Schlüsselwortliste enthalten.
Alle Schlüsselwörter	Eine Datei muss alle Schlüsselwörter aus der Schlüsselwortliste enthalten.

KRITERIEN	REGEL
Alle Schlüsselwörter innerhalb von <x> Zeichen	Eine Datei muss alle Schlüsselwörter in der Schlüsselwortliste enthalten. Darüber hinaus darf jedes Schlüsselwortpaar höchstens <x> Zeichen voneinander entfernt sein. Nehmen wir an, Ihre 3 Schlüsselwörter sind WEB, DISK und USB, und die von Ihnen angegebene Anzahl von Zeichen beträgt 20. Wenn die Funktion 'Prävention vor Datenverlust' alle Schlüsselwörter in der Reihenfolge DISK, WEB und USB erkennt, darf die Anzahl der Zeichen von "D" (in DISK) bis "W" (in WEB) und von "W" bis "U" (in USB) höchstens 20 betragen. Die folgenden Daten entsprechen den Kriterien:DISK####WEB############USB Die folgenden Daten entsprechen nicht den Kriterien:DISK**********WEB****USB (23 Zeichen zwischen "D" und "W") Denken Sie beim Festlegen der Zeichenanzahl daran, dass sich durch eine kleine Anzahl, wie z. B. 10, die Suchgeschwindigkeit erhöht, aber nur ein relativ kleiner Bereich abgedeckt wird. Dadurch verringert sich die Wahrscheinlichkeit, dass sensible Daten entdeckt werden, vor allem in großen Dateien. Bei Verwendung einer größeren Anzahl an Zeichen wird der abgedeckte Bereich größer, es kann aber sein, dass sich dadurch die Suchzeiten verlängern

KRITERIEN	REGEL
Die Gesamtbewertung für Schlüsselwörter ist größer als Grenzwert	Eine Datei muss ein oder mehrere Schlüsselwörter aus der Schlüsselwortliste enthalten. Wird nur ein Schlüsselwort entdeckt, muss seine Bewertung höher sein als der Grenzwert. Werden mehrere Schlüsselwörter entdeckt, muss die Gesamtbewertung höher sein als der Grenzwert. Weisen Sie jedem Schlüsselwort eine Punktezahl von 1 bis 10 zu. Streng vertrauliche Wörter oder Formulierungen, wie etwa "Gehaltserhöhung" in Zusammenhang mit der Personalabteilung, sollten eine relativ hohe Punktezahl haben. Wörter oder Phrasen, denen an sich keine besondere Bedeutung zukommt, können niedrigere Punktezahlen haben. Berücksichtigen Sie bei der Konfiguration des Grenzwerts die Punktezahl, die Sie den Schlüsselwörtern zugewiesen haben. Wenn Sie zum Beispiel fünf Schlüsselwörter haben und drei dieser Schlüsselwörter haben hohe Priorität, kann der Grenzwert gleich oder niedriger sein als die Gesamtpunktezahl der drei Schlüsselwörter mit hoher Priorität. Das bedeutet, dass die Entdeckung dieser drei Schlüsselwörter ausreicht, um die Datei als sensibel einzustufen.

Schlüsselwortlisten erstellen

Prozedur

1. Navigieren Sie zu **Agents** > **Prävention vor Datenverlust** > **Datenbezeichner**.
2. Klicken Sie auf die Registerkarte **Schlüsselwort**.
3. Klicken Sie auf **Hinzufügen**.

   Ein neues Fenster wird geöffnet.
4. Geben Sie einen Namen für die Schlüsselwortliste ein. Der Name darf nicht länger als 100 Byte sein und folgende Zeichen dürfen nicht enthalten sein:
   - > < * ^ | & ? \ /
5. Geben Sie eine Beschreibung mit maximal 256 Byte ein.
6. Wählen Sie eines der folgenden Kriterien und konfigurieren Sie zusätzliche Einstellungen für die ausgewählten Kriterien:

- **Beliebiges Schlüsselwort**
- **Alle Schlüsselwörter**
- **Alle Schlüsselwörter innerhalb von <x> Zeichen**
- **Die Gesamtbewertung für Schlüsselwörter ist größer als Grenzwert**

7. Schlüsselwörter manuell zur Liste hinzufügen:

   a. Geben Sie ein Schlüsselwort ein, das zwischen 3 und 40 Byte lang ist, und bestimmen Sie, ob zwischen Groß- und Kleinschreibung unterschieden werden soll.

   b. Klicken Sie auf **Hinzufügen**.

8. Schlüsselwörter mit der Option "Importieren" hinzufügen:

   Hinweis

   Verwenden Sie diese Option, wenn Sie über eine ordnungsgemäß formatierte `.csv`-Datei verfügen, in der die Schlüsselwörter gespeichert sind. Sie können die Datei erzeugen, indem Sie die Schlüsselwörter entweder über den Server, auf den Sie gerade zugreifen, oder über einen anderen Server exportieren.

   a. Klicken Sie auf **Importieren**, und suchen Sie die `.csv`-Datei, die die Schlüsselwörter enthält.

   b. Klicken Sie auf **Öffnen**.

   Sie erhalten eine Nachricht, wenn der Import erfolgreich war. Wenn ein Schlüsselwort importiert werden soll, das bereits vorhanden ist, wird es übersprungen.

9. Um Schlüsselwörter zu löschen, wählen Sie die Schlüsselwörter aus und klicken auf **Löschen**.

10. Schlüsselwörter exportieren:

Hinweis

Verwenden Sie die "Export"-Funktion, um die Schlüsselwörter zu sichern oder um sie in einen anderen Server zu importieren. Alle Schlüsselwörter in der Schlüsselwortliste werden exportiert. Das Exportieren einzelner Schlüsselwörter ist nicht möglich.

a. Klicken Sie auf **Exportieren**.

b. Speichern Sie die exportierte `.CSV`-Datei am gewünschten Speicherort.

11. Klicken Sie auf **Speichern**.

12. Eine Meldung erinnert Sie daran, die Einstellungen auf die agents zu verteilen. Klicken Sie auf **Schließen**.

13. Wenn Sie sich wieder im Fenster **DLP-Datenbezeichner** befinden, klicken Sie auf **Auf alle Agents anwenden**.

Schlüsselwortlisten importieren

Verwenden Sie diese Option, wenn Sie über eine ordnungsgemäß formatierte `.dat`-Datei verfügen, in der die Schlüsselwortlisten gespeichert sind. Sie können die Datei erzeugen, indem Sie die Schlüsselwortlisten entweder über den Server, auf den Sie gerade zugreifen, oder über einen anderen Server exportieren.

Hinweis

Die `.dat`-Schlüsselwort-Listendateien, die von dieser Version der Prävention vor Datenverlust generiert wurden, sind mit vorherigen Versionen nicht kompatibel.

Prozedur

1. Navigieren Sie zu **Agents** > **Prävention vor Datenverlust** > **Datenbezeichner**.

2. Klicken Sie auf die Registerkarte **Schlüsselwort**.

3. Klicken Sie auf **Importieren** und suchen Sie dann die `.dat`-Datei, die die Schlüsselwortlisten enthält.

4. Klicken Sie auf **Öffnen**.

   Sie erhalten eine Nachricht, wenn der Import erfolgreich war. Wenn eine Schlüsselwortliste importiert werden soll, die bereits vorhanden ist, wird sie übersprungen.

5. Klicken Sie auf **Auf alle Agents anwenden**.

Vorlagen für 'Prävention vor Datenverlust'

Eine DLP-Vorlage verbindet DLP-Datenbezeichner mit logischen Operatoren (Und, Oder, Außer) zur Erstellung von Bedingungsanweisungen. Nur Dateien oder Daten, die einer bestimmten Bedingungsanweisung entsprechen, unterliegen einer DLP-Richtlinie.

Zum Beispiel muss eine Datei eine Microsoft Word-Datei (Dateiattribut) sein UND bestimmte rechtliche Begriffe (Schlüsselwörter) UND Identifikationsnummern (Ausdrücke) enthalten, damit sie einer Richtlinie für "Anstellungsverträge" unterliegt. Auf Grund dieser Richtlinie können Mitarbeiter der Personalabteilung eine Datei an einen Drucker übertragen, damit die ausgedruckte Datei von einem Mitarbeiter unterschrieben werden kann. Die Übertragung über alle anderen möglichen Kanäle, wie etwa E-Mail, ist gesperrt.

Erstellen Sie Ihre eigenen Vorlagen, wenn Sie bereits über konfigurierte DLP-Datenbezeichner verfügen. Sie können auch vordefinierte Vorlagen verwenden. Weitere Informationen finden Sie unter *Benutzerdefinierte DLP-Vorlagen auf Seite 11-23* und *Vordefinierte DLP-Vorlagen auf Seite 11-22*.

Hinweis

Das Löschen einer Vorlage, die in einer DLP-Richtlinie verwendet wird, ist nicht möglich. Entfernen Sie die Vorlage aus der Richtlinie, bevor Sie sie löschen.

Vordefinierte DLP-Vorlagen

Die Prävention vor Datenverlust verfügt bereits über mehrere vordefinierte Vorlagen, die Sie zur Einhaltung verschiedener Regulierungsstandards verwenden können. Diese Vorlagen können weder geändert noch gelöscht werden.

- **GLBA**: Gramm-Leach-Billey Act
- **HIPAA**: Health Insurance Portability and Accountability Act
- **PCI-DSS**: PCI (Payment Card Industry Data Security Standard)
- **SB-1386**: US Senate Bill 1386
- **US PII**: Personenbezogene Daten (USA)

Eine detaillierte Liste zum Gebrauch aller vordefinierten Vorlagen und Beispiele zu den geschützten Daten finden Sie in der *Datenschutzliste* unter http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Benutzerdefinierte DLP-Vorlagen

Erstellen Sie Ihre eigenen Vorlagen, wenn Sie bereits Datenbezeichner konfiguriert haben. Eine Vorlage verbindet Datenbezeichner mit logischen Operatoren (Und, Oder, Außer) zur Erstellung von Bedingungsanweisungen.

Weitere Informationen und Beispiele zur Funktionsweise von Bedingungsanweisungen und logischen Operatoren finden Sie unter *Bedingungsanweisungen und logische Operatoren auf Seite 11-23*.

Bedingungsanweisungen und logische Operatoren

Die Prävention vor Datenverlust überprüft Bedingungsanweisungen von links nach rechts. Seien Sie vorsichtig im Umgang mit logischen Operatoren bei der Konfiguration von Bedingungsanweisungen. Falscher Gebrauch von Operatoren führt zu einer fehlerhaften Bedingungsanweisung und zu eventuell unerwarteten Ergebnissen.

Die folgende Tabelle enthält einige Beispiele.

TABELLE 11-4. Beispiel für Bedingungsanweisungen

BEDINGUNGSANWEISUNG	INTERPRETATION UND BEISPIEL
[Datenbezeichner 1] **Und** [Datenbezeichner 2] **Außer** [Datenbezeichner 3]	Eine Datei muss [Datenbezeichner 1] und [Datenbezeichner 2], aber nicht [Datenbezeichner 3] erfüllen. Beispiel: Eine Datei muss [ein Adobe PDF-Dokument] sein und muss [eine E-Mail-Adresse] enthalten, aber sollte kein [Schlüsselwort in der Liste der Schlüsselwörter] enthalten.
[Datenbezeichner 1] **Oder** [Datenbezeichner 2]	Eine Datei muss [Datenbezeichner 1] oder [Data Identifier 2] erfüllen. Beispiel: Eine Datei muss [ein Adobe PDF-Dokument] oder [ein Microsoft Word-Dokument] sein.
Außer [Datenbezeichner 1]	Eine Datei muss nicht [Datenbezeichner 1] erfüllen. Beispiel: Eine Datei muss keine [Multimedia-Datei] sein.

Wie das letzte Beispiel in der Tabelle zeigt, darf der erste Datenbezeichner in der Bedingungsanweisung den Operator "Außer" enthalten, wenn eine Datei nicht alle Datenbezeichner in der Anweisung erfüllen muss. In den meisten Fällen enthält der erste Datenbezeichner jedoch keinen Operator.

Vorlagen erstellen

Prozedur

1. Navigieren Sie zu **Agents** > **Prävention vor Datenverlust** > **DLP-Vorlagen**.
2. Klicken Sie auf **Hinzufügen**.

   Ein neues Fenster wird geöffnet.
3. Geben Sie einen Namen für die Vorlage ein. Der Name darf nicht länger als 100 Byte sein und folgende Zeichen dürfen nicht enthalten sein:

- > < * ^ | & ? \ /

4. Geben Sie eine Beschreibung mit maximal 256 Byte ein.

5. Wählen Sie die Datenbezeichner aus, und klicken Sie dann auf das Symbol "Hinzufügen".

   Zur Auswahl von Definitionen:

   - Wählen Sie mehrere Einträge aus, indem Sie die Strg-Taste gedrückt halten und dann die Datenbezeichner auswählen.
   - Verwenden Sie die Suchfunktion, wenn Sie nach einer bestimmten Definition suchen. Sie können den Namen des Datenbezeichners vollständig oder teilweise eingeben.
   - Jede Vorlage darf nur maximal 30 Datenbezeichner enthalten.

6. Um einen neuen Ausdruck zu erstellen, klicken Sie auf **Ausdrücke**, und klicken Sie anschließend auf **Neuen Ausdruck hinzufügen**. Konfigurieren Sie die Einstellungen für den Ausdruck im Fenster, das angezeigt wird.

7. Um eine neue Dateiattributliste zu erstellen, klicken Sie auf **Dateiattribute**, und klicken Sie anschließend auf **Neues Dateiattribut hinzufügen**. Konfigurieren Sie die Einstellungen für die Dateiattributliste im Fenster, das angezeigt wird.

8. Um eine neue Schlüsselwortliste zu erstellen, klicken Sie auf **Schlüsselwörter**, und klicken Sie anschließend auf **Neues Schlüsselwort hinzufügen**. Konfigurieren Sie die Einstellungen für die Schlüsselwortliste im Fenster, das angezeigt wird.

9. Wenn Sie einen Ausdruck ausgewählt haben, geben Sie die Anzahl der Vorkommen ein, das heißt die Anzahl, wie oft ein Ausdruck vorkommen muss, damit die Prävention vor Datenverlust ihn für eine Richtlinie berücksichtigt.

10. Wählen Sie einen logischen Operator für jede Definition.

Hinweis

Seien Sie vorsichtig im Umgang mit logischen Operatoren bei der Konfiguration von Bedingungsanweisungen. Falscher Gebrauch von Operatoren führt zu einer fehlerhaften Bedingungsanweisung und zu eventuell unerwarteten Ergebnissen. Beispiele für die richtige Verwendung finden Sie unter *Bedingungsanweisungen und logische Operatoren auf Seite 11-23*.

11. Um einen Datenbezeichner aus der Liste der ausgewählten Bezeichner zu entfernen, klicken Sie auf das Papierkorbsymbol.

12. Überprüfen Sie unterhalb der **Vorschau** die Bedingungsanweisung, und nehmen Sie Änderungen vor, wenn die Anweisung nicht Ihre Anforderungen erfüllt.

13. Klicken Sie auf **Speichern**.

14. Eine Meldung erinnert Sie daran, die Einstellungen auf die agents zu verteilen. Klicken Sie auf **Schließen**.

15. Wenn Sie sich wieder im Fenster **DLP-Vorlagen** befinden, klicken Sie auf **Auf alle Agents anwenden**.

Vorlagen importieren

Verwenden Sie diese Option, wenn Sie über eine ordnungsgemäß formatierte `.dat`-Datei verfügen, in der die Vorlagen gespeichert sind. Sie können die Datei erzeugen, indem Sie die Vorlagen entweder über den Server, auf den Sie gerade zugreifen, oder über einen anderen Server exportieren.

Hinweis

Um DLP-Vorlagen von OfficeScan 10.6 zu importieren, müssen Sie zuerst die zugeordneten Datenbezeichner (früher Definitionen genannt) importieren. Die Prävention vor Datenverlust kann keine Vorlagen importieren, deren zugeordnete Datenbezeichner fehlen.

Prozedur

1. Navigieren Sie zu **Agents** > **Prävention vor Datenverlust** > **DLP-Vorlagen**.

2. Klicken Sie auf **Importieren** und suchen Sie dann die `.dat`-Datei, in der die Vorlagen enthalten sind.

3. Klicken Sie auf **Öffnen**.

   Sie erhalten eine Nachricht, wenn der Import erfolgreich war. Wenn eine Vorlage importiert werden soll, die bereits vorhanden ist, wird sie übersprungen.

4. Klicken Sie auf **Auf alle Agents anwenden**.

DLP-Kanäle

Benutzer können vertrauliche Informationen über verschiedene Kanäle übertragen. OfficeScan kann folgende Kanäle überwachen:

- **Netzwerkkanäle**: Vertrauliche Informationen werden mit Hilfe von Netzwerkprotokollen wie HTTP und FTP übertragen.
- **System- und Anwendungskanäle**: Vertrauliche Informationen werden mit Hilfe der Anwendungen und Peripheriegeräte eines lokalen Endpunkt übertragen.

Netzwerkkanäle

Die Funktion "Prävention vor Datenverlust" kann die Datenübertragung über die folgenden Netzwerkkanäle überwachen:

- E-Mail-Clients
- FTP
- HTTP und HTTPS
- IM-Anwendungen
- SMB-Protokoll
- Webmail

Um festzulegen, welche Datenübertragungen überwacht werden sollen, überprüft die Funktion "Prävention vor Datenverlust" den Übertragungsumfang, den Sie konfigurieren müssen. Abhängig vom ausgewählten Umfang überwacht die Funktion "Prävention vor Datenverlust" alle Datenübertragungen oder nur Übertragungen außerhalb des lokalen Netzwerks (LAN).

Weitere Informationen über den übertragungsbereich finden Sie unter *Übertragungsumfang und -ziele für Netzwerkkanäle auf Seite 11-32*.

E-Mail-Clients

Die Funktion "Prävention vor Datenverlust" überwacht E-Mails, die über unterschiedlichste E-Mail-Clients übertragen werden. Die Funktion "Prävention vor Datenverlust" überprüft den Betreff der E-Mail, den Text und die Anhänge auf Datenbezeichner. Eine Liste der unterstützten E-Mail-Clients finden Sie in der *Datenschutzliste* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Die überwachung findet dann statt, wenn der Benutzer versucht, eine E-Mail zu versenden. Enthält die E-Mail Datenbezeichner, wird das Versenden der E-Mail von der Funktion "Prävention vor Datenverlust" zugelassen oder gesperrt.

Sie können nicht überwachte interne E-Mail-Domänen und überwachte Subdomänen festlegen.

- **Nicht überwachte E-Mail-Domänen**: Die Funktion "Prävention vor Datenverlust" gestattet die unmittelbare Übertragung von E-Mails, die an nicht überwachte Domänen gesendet werden.

  Hinweis

  Datenübertragungen an nicht überwachte E-Mail-Domänen und an überwachte E-Mail-Subdomänen, bei denen die Aktion "überwachen" gilt, sind insofern vergleichbar, als die übertragung zulässig ist. Der einzige Unterschied besteht darin, dass die Funktion "Prävention vor Datenverlust" bei nicht überwachten E-Mail-Domänen die Übertragung nicht protokolliert, während die Übertragung bei überwachten E-Mail-Subdomänen immer protokolliert wird.

- **Überwachte E-Mail-Subdomänen**: Wenn die Funktion "Prävention vor Datenverlust" die Übertragung einer E-Mail an eine überwachte Subdomäne erkennt, wird die Aktion hinsichtlich der Richtlinie überprüft. Je nach Aktion wird die übertragung zugelassen oder gesperrt.

Hinweis

Wenn Sie E-Mail-Clients als überwachten Kanal auswählen, muss eine E-Mail mit einer Richtlinie übereinstimmen, damit sie überwacht wird. Im Gegensatz dazu wird eine E-Mail, die an überwachte E-Mail-Subdomänen gesendet wird, selbst dann automatisch überwacht, wenn sie nicht mit einer Richtlinie übereinstimmt.

Geben Sie Domänen in einem der folgenden Formate an. Trennen Sie mehrere Domänen durch Kommas:

- X400-Format, z. B. /O=Trend/OU=USA, /O=Trend/OU=China
- E-Mail-Domänen, z. B. `example.com`

Bei E-Mail-Nachrichten, die über das SMTP-Protokoll gesendet werden, überprüft die Funktion "Prävention vor Datenverlust", ob der Ziel-SMTP-Server in den folgenden Listen enthalten ist:

1. überwachte Ziele
2. Nicht überwachte Ziele

Hinweis

Weitere Informationen über Benachrichtigungen finden Sie unter *Nicht überwachte und überwachte Ziele definieren auf Seite 11-45*.

3. Nicht überwachte E-Mail-Domänen
4. überwachte E-Mail-Subdomänen

Wenn also eine E-Mail an einen SMTP-Server auf der Liste der überwachten Ziele gesendet wird, wird die E-Mail überwacht. Wenn sich der SMTP-Server nicht auf der Liste überwachter Ziele befindet, überprüft die Funktion "Prävention vor Datenverlust" die anderen Listen.

Bei E-Mails, die über andere Protokolle gesendet werden, überprüft die Funktion "Prävention vor Datenverlust" nur die folgenden Listen:

1. Nicht überwachte E-Mail-Domänen
2. überwachte E-Mail-Subdomänen

FTP

Wenn OfficeScan entdeckt, dass ein FTP-Client versucht, Dateien auf einen FTP-Server hochzuladen, wird überprüft, ob die Dateien Datenbezeichner enthalten. Bis zu diesem Zeitpunkt wurden keine Dateien hochgeladen. Je nach DLP-Richtlinie erlaubt oder sperrt OfficeScan den Upload.

Wenn Sie eine Richtlinie zum Sperren von Datei-Uploads erstellen, beachten Sie bitte Folgendes:

- Wenn OfficeScan einen Upload sperrt, versuchen einige FTP-Clients diese Dateien erneut hochzuladen. In diesem Fall beendet OfficeScan den FTP-Client, um einen erneuten Upload zu verhindern. Die Benutzer werden über die Beendigung des FTP-Clients nicht informiert. Informieren Sie die Benutzer darüber, wenn Sie DLP-Richtlinien einführen.
- Wenn beim Upload einer Datei eine andere Datei auf dem FTP-Server überschrieben wird, wird die Datei auf dem FTP-Server eventuell gelöscht.

Eine Liste aller unterstützten FTP-Clients finden Sie in der *Datenschutzliste* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

HTTP und HTTPS

OfficeScan überwacht Daten, die über HTTP und HTTPS übertragen werden. Bei HTTPS überprüft OfficeScan die Daten, bevor sie verschlüsselt und übertragen werden.

Eine Liste aller unterstützten Webbrowser und Anwendungen finden Sie in der *Datenschutzliste* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

IM-Anwendungen

OfficeScan überwacht Nachrichten und Dateien, die Benutzer über IM-Anwendungen (Instant Messaging) versenden. Nachrichten und Dateien, die Benutzer erhalten, werden nicht überwacht.

Eine Liste aller unterstützten IM-Anwendungen finden Sie in der *Datenschutzliste* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Wenn OfficeScan eine Nachricht oder Datei sperrt, die über AOL Instant Messenger, MSN, Windows Messenger oder Windows Live Messenger versendet wird, beendet es auch die Anwendung. Falls OfficeScan die Anwendung nicht beendet, muss sie vom Benutzer beendet werden, da sie nicht mehr reagiert. Die Benutzer werden über die Beendigung der Anwendung nicht informiert. Informieren Sie die Benutzer darüber, wenn Sie DLP-Richtlinien einführen.

SMB-Protokoll

OfficeScan überwacht Datenübertragungen über das SMB-Protokoll (Server Message Block), das den Zugriff auf frei gegebene Dateien ermöglicht. Wenn ein anderer Benutzer versucht, eine freigegebene Datei zu kopieren oder zu lesen, überprüft OfficeScan, ob die Datei selbst ein Datenbezeichner ist oder einen enthält, und erlaubt oder sperrt dann den Vorgang.

Hinweis

Die Aktion der Gerätesteuerung hat Vorrang vor der DLP-Aktion. Wenn zum Beispiel die Gerätesteuerung das Verschieben von Dateien auf verbundenen Netzlaufwerken nicht erlaubt, werden keine vertraulichen Daten übertragen, auch wenn DLP es erlaubt.

Weitere Informationen zu Aktionen der Gerätesteuerung finden Sie unter *Berechtigungen für Speichergeräte auf Seite 10-4*.

Eine Liste aller Anwendungen, die OfficeScan für den Zugriff auf freigegebene Dateien überwacht, finden Sie in der *Datenschutzliste* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Webmail

Webbasierte E-Mail-Services übertragen Daten über HTTP. Wenn OfficeScan bemerkt, dass Daten über unterstützte Geräte versendet werden, überprüft es die Daten nach Datenbezeichnern.

Eine Liste aller unterstützten webbasierten E-Mail-Dienste finden Sie in der *Datenschutzliste* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Übertragungsumfang und -ziele für Netzwerkkanäle

Mit dem Übertragungsumfang und den Übertragungszielen werden die Datenübertragungen in Netzwerkkanälen definiert, die die Funktion "Prävention vor Datenverlust" überwachen muss. Bei zu überwachenden Übertragungen überprüft die Funktion "Prävention vor Datenverlust", ob Datenbezeichner vorhanden sind, bevor die Übertragung zugelassen oder gesperrt wird. Bei nicht zu überwachenden Übertragungen überprüft die Funktion "Prävention vor Datenverlust" nicht, ob Datenbezeichner vorhanden sind, und lässt die Übertragung sofort zu.

übertragungsumfang: Alle übertragungen

Mit der Funktion "Prävention vor Datenverlust" werden Daten überwacht, die an ein Ziel außerhalb des Hostcomputers übertragen werden.

Hinweis

Trend Micro empfiehlt die Wahl dieses Bereichs für externe Agents

Wenn Datenübertragungen zu bestimmten Zielen außerhalb des Host-Computers nicht überwacht werden sollen, definieren Sie folgende Punkte:

- **Nicht überwachte Ziele**: Die Funktion "Prävention vor Datenverlust" überwacht keine an diese Ziele übertragenen Daten.

Hinweis

Datenübertragungen an nicht überwachte Ziele und an überwachte Ziele, bei denen die Aktion "überwachen" gilt, sind insofern vergleichbar, als die übertragung zulässig ist. Der einzige Unterschied besteht darin, dass die Funktion "Prävention vor Datenverlust" die Übertragung nicht protokolliert, während die Übertragung bei überwachten Zielen immer protokolliert wird.

- **Überwachte Ziele**: Dies sind spezielle Ziele innerhalb der nicht überwachten Ziele, die überwacht werden sollten. überwachte Ziele sind:
  - Optional, wenn Sie nicht überwachte Ziele definiert haben.
  - Nicht konfigurierbar, wenn Sie keine nicht überwachten Ziele festgelegt haben.

Beispiel:

Die folgenden IP-Adressen wurden der Rechtsabteilung Ihrer Firma zugewiesen:

- `10.201.168.1` bis `10.201.168.25`

Sie erstellen eine Richtlinie, mit der die Übertragung von Beschäftigungsnachweisen an alle Mitarbeiter mit Ausnahme der Vollzeitmitarbeiter der Rechtsabteilung überwacht wird. Wählen Sie hierzu als übertragungsumfang **Alle übertragungen** aus, und gehen Sie anschließend wie folgt vor:

OPTIONEN	SCHRITTE
Option 1	1. Fügen Sie `10.201.168.1-10.201.168.25` zu den nicht überwachten Zielen hinzu. 2. Fügen Sie die IP-Adressen der Teilzeitmitarbeiter der Rechtsabteilung zu den überwachten Zielen hinzu. Angenommen, es gibt 3 IP-Adressen, `10.201.168.21-10.201.168.23`.
Option 2	Fügen Sie die IP-Adressen der Vollzeitmitarbeiter der Rechtsabteilung zu den nicht überwachten Zielen hinzu: • `10.201.168.1-10.201.168.20` • `10.201.168.24-10.201.168.25`

Richtlinien zur Definition überwachter und nicht überwachter Ziele finden Sie unter *Nicht überwachte und überwachte Ziele definieren auf Seite 11-45*.

übertragungsumfang: Nur übertragungen außerhalb des lokalen Netzwerks

Die Funktion "Prävention vor Datenverlust" überwacht Daten, die an ein beliebiges Ziel außerhalb des lokalen Netzwerks (LAN) übertragen werden.

Hinweis

Trend Micro empfiehlt die Wahl dieses Bereichs für interne Agents.

"Netzwerk" bezieht sich auf das Unternehmens- oder lokale Netzwerk. Dazu gehören das aktuelle Netzwerk (IP-Adresse des Endpunkts und Netzmaske) und die folgenden standardmäßigen privaten IP-Adressen:

- Klasse A: `10.0.0.0` bis `10.255.255.255`
- Klasse B: `172.16.0.0` bis `172.31.255.255`
- Klasse C: `192.168.0.0` bis `192.168.255.255`

Wenn Sie diesen übertragungsumfang auswählen, können Sie folgende Elemente definieren:

- **Nicht überwachte Ziele**: Definieren Sie Ziele außerhalb des LAN, die Sie für sicher halten und die deshalb nicht überwacht werden müssen.

  Hinweis

  Datenübertragungen an nicht überwachte Ziele und an überwachte Ziele, bei denen die Aktion "überwachen" gilt, sind insofern vergleichbar, als die übertragung zulässig ist. Der einzige Unterschied besteht darin, dass die Funktion "Prävention vor Datenverlust" die Übertragung nicht protokolliert, während die Übertragung bei überwachten Zielen immer protokolliert wird.

- **Überwachte Ziele**: Definieren Sie Ziele innerhalb des LAN, die Sie überwachen möchten.

Richtlinien zur Definition überwachter und nicht überwachter Ziele finden Sie unter *Nicht überwachte und überwachte Ziele definieren auf Seite 11-45*.

Konflikte auflösen

Wenn bei den Einstellungen für den Übertragungsumfang, für überwachte Ziele und für nicht überwachte Ziele Konflikte auftreten, erkennt OfficeScan die folgenden Prioritäten von der höchsten bis zur niedrigsten Priorität:

- Überwachte Ziele
- Nicht überwachte Ziele
- Übertragungsumfang

System- und Anwendungskanäle

Die Funktion "Prävention vor Datenverlust" kann folgende System- und Anwendungskanäle überwachen:

- Cloud Storage Services
- Datenspeicher (CD/DVD)
- Peer-to-Peer-Anwendungen
- PGP-Verschlüsselung
- Drucker
- Wechseldatenträger
- Synchronisierungssoftware (ActiveSync)
- Windows-Zwischenablage

Cloud Storage Service

OfficeScan überwacht Dateien, auf die Benutzer mit Cloud Storage Services zugreifen. Eine Liste der unterstützten Cloud Storage Services finden Sie im Dokument *Datenschutzlisten* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Hinweis

Prävention gegen Datenverlust unterstützt die Verschlüsselung von Cloud Storage Services, wenn Endpoint Encryption auf dem Agent-Endpunkt installiert ist.

Datenspeicher (CD/DVD)

OfficeScan überwacht Daten, die auf CD oder DVD gespeichert werden. Eine Liste aller unterstützten Datenspeichergeräte und -programme finden Sie in der *Datenschutzliste* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Wenn OfficeScan entdeckt, dass eines der unterstützten Geräte oder Programme einen Brenn-Befehl gibt und als Aktion "Übergehen" gewählt wurde, werden die Daten gespeichert. Wenn als Aktion "Sperren" gewählt wurde, überprüft OfficeScan, ob eine der Dateien, die gespeichert werden soll, selbst ein Datenbezeichner ist oder einen enthält. Wenn OfficeScan mindestens einen Datenbezeichner erkennt, werden keine Dateien – auch nicht solche, die selbst kein Datenbezeichner sind oder einen enthalten – gespeichert. OfficeScan kann möglicherweise verhindern, dass eine CD oder DVD ausgeworfen wird. Falls dieses Problem auftritt, sollen die Benutzer die Software neu starten oder das Gerät zurücksetzen.

OfficeScan wendet zusätzliche CD-/DVD-Speicherungsregeln an:

- Um Fehlalarme zu reduzieren, überwacht OfficeScan die folgenden Dateien nicht:

`.bud`	`.dll`	`.gif`	`.gpd`	`.htm`	`.ico`	`.ini`
`.jpg`	`.lnk`	`.sys`	`.ttf`	`.url`	`.xml`	

- Zwei Dateitypen, die von Roxio Datenspeichern verwendet werden (`*.png` und `*.skn`) werden nicht überwacht, um die Leistung zu erhöhen.
- OfficeScan überwacht keine Dateien in den folgenden Verzeichnissen:

*:\autoexec.bat	*:\Windows
..\Application Data	..\Cookies
..\Local Settings	..\ProgramData
..\Programme	..\Users*\AppData
..\WINNT	

- ISO-Images, die von diesen Dateien oder Programmen erstellt werden, werden nicht überwacht.

Zugriff auf Datenspeicher (CD/DVD) blockieren

Gerätesteuerung kann den Zugriff auf CD/DVD-Aufnahmegeräte begrenzen, die das Live-Dateisystemformat verwenden. Einige Anwendungen von Drittanbietern, die Master Format verwenden, können Lese-/Schreibvorgänge ausführen, selbst wenn Gerätesteuerung aktiviert ist. Verwenden Sie Prävention vor Datenverlust, um den Zugriff auf CD/DVD-Aufnahmegeräte zu begrenzen, die einen beliebigen Formattyp verwenden.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **DLP-Einstellungen**.
4. Klicken Sie auf die Registerkarte **Externe Agents**, um eine Richtlinie für externe agents zu konfigurieren, oder auf die Registerkarte **Interne Agents**, um eine Richtlinie für interne agents zu konfigurieren.

Hinweis

Konfigurieren Sie die Einstellungen zum agent-Standort, wenn dies noch nicht vorgenommen wurde. Agents verwenden diese Standorteinstellungen, um die richtige Richtlinie für die Funktion "Prävention vor Datenverlust" festzulegen. Weitere Informationen finden Sie unter *Endpunktspeicherort auf Seite 15-2*.

5. Wählen Sie eine der folgenden Optionen aus:

   - Auf der Registerkarte **Externe Agents** können Sie alle Einstellungen für die Funktion "Prävention vor Datenverlust" auf interne agents anwenden, indem Sie die Option **Alle Einstellungen für interne Agents übernehmen** auswählen.

   - Auf der Registerkarte **Interne Agents** können Sie alle Einstellungen für die Funktion "Prävention vor Datenverlust" auf externe agents anwenden, indem Sie die Option **Alle Einstellungen für externe Agents übernehmen** auswählen.

6. Klicken Sie auf der Registerkarte **Regeln** auf **Hinzufügen**.

7. Wählen Sie **Diese Regel aktivieren**.

8. Geben Sie einen Namen für diese Regel an.

9. Klicken Sie auf die Registerkarte **Vorlage**.

10. Wählen Sie die Vorlage **All File Extension** aus der Liste aus und klicken Sie auf **Hinzufügen**.

11. Klicken Sie auf die Registerkarte **Kanal**.

12. Wählen Sie im Abschnitt **System- und Anwendungskanäle** den Eintrag **Datenrecorder (CD/DVD)** aus.

13. Klicken Sie auf die Registerkarte **Aktion**.

14. Wählen Sie die Aktion **Blockieren** aus.

15. Klicken Sie auf **Speichern**.

16. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

    - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Peer-to-Peer-Anwendungen

OfficeScan überwacht Dateien, die Benutzer über Peer-to-Peer-Anwendungen mit anderen teilen.

Eine Liste aller unterstützten Peer-to-Peer-Anwendungen finden Sie in der *Datenschutzliste* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

PGP-Verschlüsselung

OfficeScan überwacht Daten, die mit PGP-Verschlüsselungssoftware verschlüsselt werden sollen. OfficeScan überprüft die Daten, bevor sie verschlüsselt werden.

Eine Liste der unterstützten PGP-Verschlüsselungssoftware finden Sie in der *Datenschutzliste* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Drucker

OfficeScan überwacht Druckvorgänge, die von verschiedenen Anwendungen ausgelöst werden.

OfficeScan überwacht keine Druckvorgänge bei neuen Dateien, die noch nicht gespeichert wurden, da sich die Druckdaten bis zu diesem Zeitpunkt nur im Arbeitsspeicher befinden.

Eine Liste aller unterstützten Anwendungen, die Druckvorgänge auslösen können, finden Sie in der *Datenschutzliste* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Wechseldatenträger

OfficeScan überwacht Datenübertragungen auf oder innerhalb von Wechseldatenträgern. Die Datenübertragung umfasst folgende Aktivitäten:

- Erstellen einer Datei auf einem Gerät
- Kopieren einer Datei vom Host-Rechner auf das Gerät
- Schließen einer Datei auf einem Gerät
- Verändern von Dateiinformationen (etwa der Dateierweiterung) auf einem Gerät

Wenn eine zu übertragende Datei einen Datenbezeichner enthält, sperrt oder erlaubt OfficeScan die Übertragung.

Hinweis

- Die Aktion der Gerätesteuerung hat Vorrang vor der DLP-Aktion. Wenn zum Beispiel die Gerätesteuerung das Kopieren von Dateien auf ein Wechselspeichermedium nicht erlaubt, wird die Übertragung vertraulicher Informationen nicht fortgesetzt, selbst wenn DLP dies zulässt.
- Prävention vor Datenverlust unterstützt die Verschlüsselung von Wechselspeichermedien, wenn Endpoint Encryption auf dem Agent-Endpunkt installiert ist.

Eine Liste der unterstützten Wechselspeichermedien und Anwendungen, die die Datenübertragung ermöglichen, finden Sie in der *Datenschutzliste* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Die Handhabung von Dateiübertragungen auf einen Wechseldatenträger ist relativ einfach. Zum Beispiel möchte ein Benutzer, der eine Microsoft Word-Datei erstellt, diese auf eine SD-Karte speichern (der Dateityp spielt dabei keine Rolle). Wenn die Datei einen Datenbezeichner enthält, der nicht übertragen werden soll, verhindert OfficeScan, dass diese Datei gespeichert wird.

Zur Dateiübertragung innerhalb des Mediums erstellt OfficeScan zunächst eine Sicherungskopie der Datei (nur bei Dateien bis 75 MB) unter `%WINDIR%\system32\dgagent\temp`, bevor sie übertragen wird. OfficeScan entfernt die Sicherungskopie, wenn es die Dateiübertragung erlaubt. Wenn OfficeScan die Übertragung gesperrt hat, könnte es sein, dass die Datei dabei gelöscht wurde. In diesem Fall kopiert OfficeScan die Sicherungskopie in den Ordner, in dem sich die Originaldatei befindet.

Mit OfficeScan können Sie Ausnahmen definieren. OfficeScan lässt Datenübertragungen zu diesen oder innerhalb dieser Geräte immer zu. Identifizieren Sie die Geräte nach ihrem Hersteller, und geben Sie optional die Gerätemodelle und Seriennummern an.

Tipp

Verwenden Sie Device List, um Geräte abzufragen, die mit dem Endpunkt verbunden sind. Das Tool liefert den Hersteller, das Modell und die Seriennummer für jedes Gerät. Weitere Informationen finden Sie unter *Device List auf Seite 10-15*.

Synchronisierungssoftware (ActiveSync)

OfficeScan überwacht Daten, die über Synchronisierungssoftware auf ein mobiles Gerät übertragen werden.

Eine Liste der unterstützten Synchronisierungs-Software finden Sie in der *Datenschutzliste* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Wenn die Daten die Quell-IP-Adresse 127.0.0.1 haben und entweder über Port 990 oder 5678 versendet werden (die zur Synchronisierung verwendeten Ports), überprüft OfficeScan, ob die Datei ein Datenbezeichner ist, bevor es die Übertragung erlaubt oder sperrt.

Wenn OfficeScan eine Datei sperrt, die auf Port 990 übertragen wird, könnte trotzdem eine Datei mit gleichem Namen, aber defekten Zeichen, am Zielordner auf dem mobilen Gerät erstellt werden. Das liegt daran, dass Teile der Datei auf das Gerät kopiert wurden, bevor OfficeScan die Übertragung gesperrt hat.

Windows-Zwischenablage

OfficeScan überwacht Daten, die in die Windows-Zwischenablage übertragen werden sollen, bevor es die Übertragung erlaubt oder sperrt.

OfficeScan kann auch Übertragungen in die Zwischenablage zwischen dem Host-Rechner und VMWare bzw. Remote Desktop überwachen. Die Überwachung erfolgt auf der Einheit, die mit dem OfficeScan Agent verbunden ist. Zum Beispiel kann der OfficeScan Agent auf einer virtuellen VMware-Maschine verhindern, dass Daten im Zwischenspeicher auf den Host-Rechner übertragen werden. Ebenso kann ein Host-Rechner mit dem OfficeScan Agent eventuell keine Daten im Zwischenspeicher auf einen Endpunkt übertragen, auf den per Remote-Desktop zugegriffen wird.

Aktionen der Funktion "Prävention vor Datenverlust"

Wenn die Prävention vor Datenverlust die Übertragung von Datenbezeichnern entdeckt, überprüft es, ob die entsprechenden Richtlinien eingehalten werden, und führt dann den Vorgang richtliniengemäß durch.

Die folgende Tabelle enthält eine Liste der Aktionen für die Funktion "Prävention vor Datenverlust".

TABELLE 11-5. Aktionen der Funktion "Prävention vor Datenverlust"

AKTION	BESCHREIBUNG
Aktionen	
Übergehen	Die Prävention vor Datenverlust erlaubt und protokolliert die Übertragung.
Sperren	Die Prävention vor Datenverlust sperrt und protokolliert die Übertragung.
Zusätzliche Aktionen	

AKTION	BESCHREIBUNG
Agent-Benutzer benachrichtigen	Die Prävention vor Datenverlust benachrichtigt den Benutzer, ob die Datenübertragung stattgefunden hat oder gesperrt wurde.
Daten aufzeichnen	Unabhängig von der primären Aktion zeichnet die Prävention vor Datenverlust die vertraulichen Informationen im Ordner `<Installationsordner des Clients>\DLPLite\Forensic` auf. Wählen Sie diese Aktion, um vertrauliche Informationen zu überprüfen, die von der Funktion "Prävention vor Datenverlust" gekennzeichnet werden. Aufgezeichnete vertrauliche Informationen können zu viel Festplattenspeicherplatz verbrauchen. Daher empfiehlt Trend Micro dringend, dass Sie diese Option nur für hochsensible Informationen wählen.

Aktion	Beschreibung
Verschlüsselt unterstützte Kanäle mit dem angegebenen Schlüssel/ Kennwort (nur verfügbar, wenn Endpoint Encryption installiert ist) **Hinweis** Diese Option ist nur für Wechseldatenträger- und Cloud-Speicher-Kanäle und bei Auswahl der Aktion **übergehen** verfügbar.	Wenn Trend Micro Endpoint Encryption neben dem OfficeScan Agent installiert ist, kann Prävention vor Datenverlust Dateien automatisch verschlüsseln, bevor diese von einem Benutzer an einen anderen Speicherort weitergegeben werden können. Wenn Endpoint Encryption nicht installiert ist, führt Prävention vor Datenverlust eine Aktion zum Sperren der Dateien durch. Wählen Sie einen der folgenden Verschlüsselungsschlüssel oder ein festes Kennwort aus: • **Benutzerschlüssel**: Dieser auch als **lokaler Schlüssel** bezeichneter Schlüssel ist eindeutig für jeden Benutzer und beschränkt den Zugriff auf die verschlüsselte Datei für den Benutzer, der die Datei erstellt hat. • **Gemeinsamer Schlüssel**: Dieser Schlüssel bezieht sich auf den **Gruppenschlüssel** oder **Unternehmensschlüssel** und der Endpoint Encryption Administrator konfiguriert den Typ unter Verwendung der PolicyServer MMC. • **Festgelegtes Kennwort**: Benutzer geben manuell ein festes Kennwort an, wenn Sie auf dem Bildschirm dazu aufgefordert werden. Endpoint Encryption erstellt ein selbstextrahierendes Paket, auf das Benutzer nach Eingabe des Verschlüsselungskennworts von allen Endpunkten aus zugreifen können. **Wichtig** • Auf dem Ziel-Endpunkt muss Endpoint Encryption installiert sein und der Benutzer muss sich bei Endpoint Encryption anmelden, um die Daten zu verschlüsseln. • Verschlüsselte Dateien auf USB-Geräten werden auf die Prävention vor Datenverlust hin durchsucht, wenn Benutzer die Dateien zu entschlüsseln versuchen. Wenn Sie auf einem USB-Gerät Dateien entschlüsseln, die vertrauliche Daten enthalten, wird das USB-Verschlüsselungsprotokoll ausgelöst. Die vertraulichen Daten müssen dann (erneut) verschlüsselt werden. Um zu verhindern, dass die Daten durch die Funktion zur Prävention vor Datenverlust erneut verschlüsselt werden, verschieben Sie die verschlüsselten Dateien auf ein lokales Laufwerk, bevor Sie versuchen, auf die Daten zuzugreifen.

AKTION	BESCHREIBUNG
Benutzerrechtfertigung **Hinweis** Diese Option steht nur nach der Auswahl der Aktion **Sperren** zur Verfügung.	Die Prävention vor Datenverlust fordert den Benutzer zur Bestätigung auf, bevor die Aktion „Sperren“ ausgeführt wird. Der Benutzer kann die Aktion „Sperren“ überschreiben, indem er erläutert, weshalb die vertraulichen Daten sicher sind. Es gibt die folgenden Rechtfertigungsgründe: • **Dies ist Bestandteil eines etablierten Geschäftsvorgangs.** • **Mein Vorgesetzter hat die Datenübertragung genehmigt.** • **Die Daten in dieser Datei sind nicht vertraulich.** • **Andere**: Die Benutzer geben in das entsprechende Textfeld eine andere Erklärung ein.

Ausnahmen für Prävention vor Datenverlust

DLP-Ausnahmen gelten für die gesamte Richtlinie, einschließlich aller darin definierten Regeln. Die Prävention vor Datenverlust wendet die Ausnahmeeinstellungen auf alle Übertragungen an, bevor nach digitalen Assets gesucht wird. Wenn eine Übertragung mit einer der Ausnahmeregeln übereinstimmt, wird die Übertragung je nach Ausnahmetyp sofort zugelassen oder durchsucht.

Nicht überwachte und überwachte Ziele definieren

Definieren Sie die nicht überwachten und die überwachten Ziele anhand des Übertragungsbereichs, der auf der Registerkarte **Kanal** konfiguriert ist. Details zur Definition nicht überwachter und überwachter Ziele für **Alle Übertragungen** finden Sie unter *übertragungsumfang: Alle übertragungen auf Seite 11-32*. Details zur Definition nicht überwachter und überwachter Ziele für **Nur Übertragungen an Ziele außerhalb des lokalen Netzwerks** finden Sie unter *übertragungsumfang: Nur übertragungen außerhalb des lokalen Netzwerks auf Seite 11-34*.

Befolgen Sie die nachstehenden Richtlinien, wenn Sie überwachte und nicht überwachte Ziele definieren:

1. Definieren Sie jedes Ziel nach:

   - IP-Adresse
   - Host-Name
   - FQDN
   - Netzwerkadresse und Subnetzmaske, z. B. 10.1.1.1/32

   Hinweis

   Bei der Subnetzmaske unterstützt die Prävention vor Datenverlust nur einen Port vom Typ klassenloses Inter-Domänen-Routing (CIDR). Das heißt, Sie können nur eine Zahl wie 32 anstelle von 255.255.255.0 eingeben.

2. Um bestimmte Kanäle anzusteuern, geben Sie die Standard- oder die vom Benutzer bzw. Unternehmen festgelegten Portnummern für diese Kanäle an. Port 21 ist z. B. typischerweise für FTP-, Port 80 für HTTP- und Port 443 für HTTPS-Datenverkehr bestimmt. Verwenden Sie einen Doppelpunkt, um das Ziel von den Portnummern zu trennen.

3. Sie können auch Portbereiche angeben. Um alle Ports einzubeziehen, ignorieren Sie den Portbereich.

   Nachstehend finden Sie einige Beispiele für Zieladressen mit Portnummern und Portbereichen:

   - 10.1.1.1:80
   - host:5-20
   - host.domain.com:20
   - 10.1.1.1/32:20

4. Fügen Sie zwischen den einzelnen Zielen jeweils ein Komma ein.

Dekomprimierungsregeln

Dateien, die komprimierte Dateien enthalten, können nach digitalen Assets durchsucht werden. Um die zu durchsuchenden Dateien zu ermitteln, wendet die Prävention vor Datenverlust folgende Regeln auf eine komprimierte Datei an:

- **Die dekomprimierte Datei ist größer als: __ MB (1-512MB)**
- **Komprimierungsebenen sind höher als: __ (1-20)**
- **Anzahl der zu durchsuchenden Dateien ist höher als: __ (1-2000)**

Regel 1: Maximale Größe einer dekomprimierten Datei

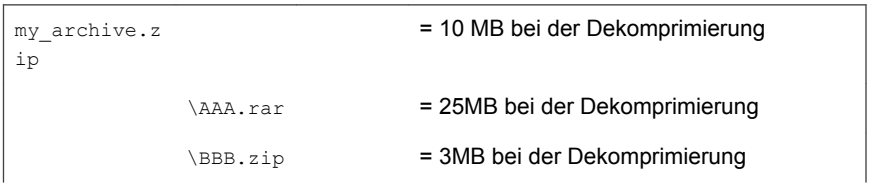
Eine komprimierte Datei muss bei ihrer Dekomprimierung den angegebenen Grenzwert einhalten.

Beispiel: Sie haben den Grenzwert auf 20 MB gesetzt.

Szenario 1: Wenn die Größe der Datei `archive.zip` bei der Dekomprimierung 30 MB, beträgt, wird keine der in der Datei `archive.zip` enthaltenen Dateien durchsucht. Die anderen beiden Regeln werden nicht mehr überprüft.

Szenario 2: Wenn die Größe der Datei `my_archive.zip` bei der Dekomprimierung 10 MB beträgt:

- Wenn die Datei `my_archive.zip` keine komprimierten Dateien enthält, überspringt OfficeScan Regel 2 und fährt direkt mit Regel 3 fort.
- Wenn die Datei `my_archive.zip` komprimierte Dateien enthält, muss die Größe aller dekomprimierten Dateien unterhalb des Grenzwerts liegen. Beispiel: Die Datei `my_archive.zip` enthält die Dateien `AAA.rar`, `BBB.zip` und `EEE.zip`, und `EEE.zip` enthält `222.zip`:



```
                \EEE.zip            = 1MB bei der Dekomprimierung
                        \222.zip    = 2MB bei der Dekomprimierung
```

Für die Dateien `my_archive.zip`, `BBB.zip`, `EEE.zip` und `222.zip` wird eine Überprüfung hinsichtlich der Regel 2 durchgeführt, weil die kombinierte Größe dieser Dateien unterhalb des Grenzwerts von 20 MB liegt. `AAA.rar` wird übersprungen.

Regel 2: Maximale Komprimierungsebenen

Dateien innerhalb der angegebenen Anzahl Ebenen werden zum Durchsuchen markiert.

Beispiel:

```
my_archive.zip
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
                                        \222.zip            \333.txt
```

Wenn Sie den Grenzwert auf zwei Ebenen festlegen:

- OfficeScan ignoriert `333.txt`, da sich diese Datei auf der dritten Ebene befindet.
- OfficeScan markiert die folgenden Dateien zum Durchsuchen und überprüft dann Regel 3:
  - `DDD.txt` (auf der ersten Ebene)
  - `CCC.xls` (auf der zweiten Ebene)
  - `111.pdf` (auf der zweiten Ebene)

Regel 3: Maximale Anzahl an zu durchsuchenden Dateien

OfficeScan durchsucht Dateien bis zum angegebenen Grenzwert. OfficeScan durchsucht Dateien und Ordner erst in numerischer, dann in alphabetischer Reihenfolge.

Ausgehend vom Beispiel in Regel 2 hat OfficeScan die hervorgehobenen Dateien zum Durchsuchen markiert:

```
my_archive.zip
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
                                        \222.zip            \333.txt
```

Darüber hinaus enthält `my_archive.zip` einen Ordner namens `7Folder`, der nicht auf Regel 2 überprüft wurde. Dieser Ordner enthält die Dateien `FFF.doc` und `GGG.ppt`. Dadurch erhöht sich die Gesamtzahl der zu durchsuchenden Dateien auf 5, wie nachstehend hervorgehoben:

```
my_archive.zip
                    \7Folder            \FFF.doc
                    \7Folder            \GGG.ppt
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
                                        \222.zip            \333.txt
```

Wenn Sie den Grenzwert auf 4 Dateien festlegen, werden die folgenden Dateien durchsucht:

- `FFF.doc`
- `GGG.ppt`

- `CCC.xls`
- `DDD.txt`

Hinweis

Bei Dateien, die eingebettete Dateien enthalten, extrahiert OfficeScan den Inhalt der eingebetteten Dateien.

Wenn es sich beim extrahierten Inhalt um Text handelt, werden die Hostdatei (z. B. `123.doc`) und die eingebetteten Dateien (z. B.`abc.txt` und `xyz.xls`) als eine Datei gezählt.

Wenn es sich beim extrahierten Inhalt nicht um Text handelt, werden die Hostdatei (z. B. `123.doc`) und die eingebetteten Dateien (z. B. `abc.exe`) separat gezählt.

Ereignisse, die Dekomprimierungsregeln auslösen

Die folgenden Ereignisse lösen Dekomprimierungsregeln aus:

TABELLE 11-6. Ereignisse, die Dekomprimierungsregeln auslösen

Eine komprimierte Datei, die übertragen werden soll, stimmt mit einer Richtlinie überein, und die Aktion für die komprimierte Datei lautet "Übergehen" (Datei übertragen).	Um beispielsweise .ZIP-Dateien zu überwachen, die Benutzer übertragen, haben Sie ein Dateiattribut (.ZIP) definiert, zu einer Vorlage hinzugefügt, die Vorlage in einer Richtlinie verwendet und anschließend die Aktion auf **Übergehen** gesetzt. **Hinweis** Wenn die Aktion "Sperren" lautet, wird die gesamte komprimierte Datei nicht übertragen. Daher müssen die darin enthaltenen Dateien nicht durchsucht werden.

Eine komprimierte Datei, die übertragen werden soll, stimmt nicht mit einer Richtlinie überein.	In diesem Fall wendet OfficeScan trotzdem die Dekomprimierungsregeln auf die komprimierte Datei an, um festzustellen, welche der darin enthaltenen Dateien auf digitale Assets durchsucht werden sollen und ob die gesamte komprimierte Datei übertragen werden soll.

Beide Ereignisse haben dasselbe Ergebnis. Wenn OfficeScan eine komprimierte Datei findet:

- Wenn Regel 1 nicht erfüllt wird, lässt OfficeScan die Übertragung der gesamten komprimierten Datei zu.
- Wenn Regel 1 erfüllt wird, werden die anderen beiden Regeln überprüft. OfficeScan lässt die Übertragung der gesamten komprimierten Datei zu, wenn die folgenden Punkte erfüllt sind:
  - Alle durchsuchten Dateien stimmen nicht mit einer Richtlinie überein.
  - Alle durchsuchten Dateien stimmen mit einer Richtlinie überein, und die Aktion lautet **Übergehen**.

    Die Übertragung der gesamten komprimierten Datei wird gesperrt, wenn mindestens eine durchsuchte Datei mit einer Richtlinie übereinstimmt und die Aktion **Sperren** lautet.

Richtlinienkonfiguration der Funktion "Prävention vor Datenverlust"

Nachdem Sie Datenbezeichner konfiguriert und in Vorlagen kategorisiert haben, können Sie damit beginnen, Richtlinien für die Funktion "Prävention vor Datenverlust" zu erstellen.

Zusätzlich zu den Datenbezeichnern und Vorlagen müssen Sie bei der Erstellung einer Richtlinie Kanäle und Aktionen konfigurieren. Weitere Informationen über Richtlinien finden Sie unter *Richtlinien für 'Prävention vor Datenverlust' auf Seite 11-3*.

Richtlinie für Prävention vor Datenverlust erstellen

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **DLP-Einstellungen**.
4. Klicken Sie auf die Registerkarte **Externe Agents**, um eine Richtlinie für externe agents zu konfigurieren, oder auf die Registerkarte **Interne Agents**, um eine Richtlinie für interne agents zu konfigurieren.

   Hinweis

   Konfigurieren Sie die Einstellungen zum agent-Standort, wenn dies noch nicht vorgenommen wurde. Agents verwenden diese Standorteinstellungen, um die richtige Richtlinie für die Funktion "Prävention vor Datenverlust" festzulegen. Weitere Informationen finden Sie unter *Endpunktspeicherort auf Seite 15-2*.

5. Wählen Sie**'Prävention vor Datenverlust' aktivieren**.
6. Wählen Sie eine der folgenden Optionen aus:

   - Auf der Registerkarte **Externe Agents** können Sie alle Einstellungen für die Funktion "Prävention vor Datenverlust" auf interne agents anwenden, indem Sie die Option **Alle Einstellungen für interne Agents übernehmen** auswählen.
   - Auf der Registerkarte **Interne Agents** können Sie alle Einstellungen für die Funktion "Prävention vor Datenverlust" auf externe agents anwenden, indem Sie die Option **Alle Einstellungen für externe Agents übernehmen** auswählen.

7. Klicken Sie auf der Registerkarte **Regeln** auf **Hinzufügen**.

   Eine Richtlinie darf maximal 40 Regeln enthalten.

8. Konfigurieren Sie die Regeleinstellungen.

   Einzelheiten zum Erstellen von DLP-Regeln finden Sie unter *Regeln für Prävention vor Datenverlust erstellen auf Seite 11-53*.

9. Klicken Sie auf die Registerkarte **Ausnahmen**, und konfigurieren Sie die erforderlichen Ausnahmeeinstellungen.

   Einzelheiten zu den verfügbaren Ausnahmeeinstellungen finden Sie unter *Ausnahmen für Prävention vor Datenverlust auf Seite 11-45*.

10. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

    - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
    - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Regeln für Prävention vor Datenverlust erstellen

Hinweis

Die Prävention vor Datenverlust verarbeitet Regeln und Vorlagen anhand der Priorität. Wenn für eine Regel „Übergehen“ festgelegt ist, wird von der Prävention vor Datenverlust die nächste Regel in der Liste verarbeitet. Wenn für eine Regel „Sperren“ oder „Benutzerrechtfertigung“ festgelegt ist, wird die Benutzeraktion von der Prävention vor Datenverlust gesperrt oder akzeptiert, und diese Regel/Vorlage wird nicht weiter verarbeitet.

Prozedur

1. Wählen Sie **Diese Regel aktivieren**.
2. Geben Sie einen Namen für diese Regel an.

   Konfigurieren Sie die Vorlageneinstellungen:
3. Klicken Sie auf die Registerkarte **Vorlage**.
4. Wählen Sie Vorlagen aus der Liste **Verfügbare Vorlagen**, und klicken Sie dann auf **Hinzufügen**.

   Zur Auswahl von Vorlagen:

   - Durch Klicken auf die Vorlagennamen können Sie mehrere Einträge auswählen. Der Name wird hervorgehoben.
   - Verwenden Sie die Suchfunktion, wenn Sie nach einer bestimmten Vorlage suchen. Sie können den Namen der Vorlage vollständig oder teilweise eingeben.

   Hinweis

   Jede Regel darf maximal 200 Vorlagen enthalten.
5. Wenn Ihre gewünschte Vorlage in der Liste **Verfügbare Vorlagen** nicht gefunden wird:

   a. Klicken Sie auf **Neue Vorlage hinzufügen**.

      Das Fenster **Vorlagen für 'Prävention vor Datenverlust'** wird angezeigt.

      Weitere Hinweise zum Hinzufügen von Vorlagen zum Fenster **Vorlagen für 'Prävention vor Datenverlust'** finden Sie unter *Vorlagen für 'Prävention vor Datenverlust' auf Seite 11-22*.

   b. Nachdem Sie eine Vorlage erstellt haben, wählen sie diese aus und klicken auf **Hinzufügen**.

Hinweis

OfficeScan verwendet beim Prüfen von Vorlagen die Regel der ersten Übereinstimmung. Das bedeutet, dass OfficeScan keine weiteren Vorlagen prüft, wenn eine Datei oder Daten mit der Definition in einer Vorlage übereinstimmen. Die Priorität basiert auf der Reihenfolge der Vorlagen in der Liste.

Konfigurieren Sie die Kanaleinstellungen:

6. Klicken Sie auf die Registerkarte **Kanal**.

7. Wählen Sie die Kanäle für die Richtlinie aus.

   Weitere Informationen über Kanäle finden Sie unter *Netzwerkkanäle auf Seite 11-27* und *System- und Anwendungskanäle auf Seite 11-35*.

8. Wenn Sie einen der Netzwerkkanäle ausgewählt haben, wählen Sie den Übertragungsbereich:

   - **Alle Übertragungen**
   - **Nur Übertragungen außerhalb des lokalen Netzwerks**

   Unter *Übertragungsumfang und -ziele für Netzwerkkanäle auf Seite 11-32* finden Sie weitere Informationen über den Übertragungsumfang, wie Ziele abhängig vom Übertragungsumfang funktionieren und wie Ziele korrekt definiert werden.

9. Wenn Sie **E-Mail-Clients** ausgewählt haben:

   a. Klicken Sie auf **Ausnahmen**.

   b. Geben Sie überwachte und nicht-überwachte interne E-Mail-Domänen an.

      Informationen über überwachte und nicht-überwachte E-Mail-Domänen finden Sie unter *E-Mail-Clients auf Seite 11-28*.

10. Wenn Sie **Wechseldatenträger** ausgewählt haben:

    a. Klicken Sie auf **Ausnahmen**.

    b. Fügen Sie nicht-überwachte Wechseldatenträger hinzu, indem Sie sie anhand der jeweiligen Hersteller ermitteln. Die Modellbezeichnung und die serielle ID des Geräts sind optional.

Die Liste der zulässigen USB-Geräte unterstützt die Verwendung des Sterns (*) als Platzhalter. Verwenden Sie den Stern (*) in beliebigen Feldern, um alle Geräte einzuschließen, die den Kriterien der übrigen Felder entsprechen.

Beispiel: [Hersteller]-[Modell]-* platziert alle Geräte des angegebenen Herstellers und Modells in die Liste der zulässigen Geräte, unabhängig von der Seriennummer.

c. Um weitere Geräte hinzuzufügen, klicken Sie auf das Plus-Symbol (**+**).

Tipp

Verwenden Sie Device List, um Geräte abzufragen, die mit dem Endpunkt verbunden sind. Das Tool liefert den Hersteller, das Modell und die Seriennummer für jedes Gerät. Weitere Informationen finden Sie unter *Device List auf Seite 10-15*.

Konfigurieren Sie die Aktionseinstellungen:

11. Klicken Sie auf die Registerkarte **Aktion**.

12. Wählen Sie eine primäre Aktion und weitere zusätzliche Aktionen.

Weitere Informationen über Aktionen finden Sie unter *Aktionen der Funktion "Prävention vor Datenverlust" auf Seite 11-42*.

Hinweis

Die Funktion 'Prävention gegen Datenverlust' unterstützt nur die Verschlüsselung von vertraulichen Informationen auf Wechselmedien oder in Cloud Storage Services. Die Funktion "Prävention vor Datenverlust" führt die Aktion „Übergehen“ ohne Verschlüsselung auf allen Kanälen durch, auf denen die Verschlüsselung nicht unterstützt wird. Auf dem Ziel-Endpunkt muss Endpoint Encryption installiert sein und der Benutzer muss sich bei Endpoint Encryption anmelden, um die Daten zu verschlüsseln.

13. Nach der Konfiguration der Einstellungen für **Vorlage**, **Kanal** und **Aktion** klicken Sie auf **Speichern**.

Regeln für Prävention vor Datenverlust importieren, exportieren und kopieren

Administratoren können bereits definierte (und in einer korrekt formatierten `.dat`-Datei enthaltene) Regeln importieren oder eine Liste der konfigurierten DLP-Regeln exportieren. Durch Kopieren einer DLP-Regel kann ein Administrator zeitsparend den Inhalt einer bereits definierten Regel anpassen.

In der folgenden Tabelle wird die Funktionsweise der einzelnen Funktionen beschrieben.

TABELLE 11-7. Import-, Export- und Kopierfunktionen für DLP-Regeln

FUNKTION	BESCHREIBUNG
Importieren	Beim Importieren einer Regelliste werden nicht vorhandene Regeln an die Liste der bestehenden DLP-Regeln angefügt. Die Prävention vor Datenverlust überspringt alle Regeln, die in der Zielliste bereits vorhanden sind. Die Prävention vor Datenverlust behält alle vorkonfigurierten Einstellungen der einzelnen Regeln bei, auch den Status "Aktiviert" oder "Deaktiviert".
Exportieren	Beim Exportieren einer Regelliste wird die gesamte Liste in eine `.dat`-Datei exportiert, die Administratoren anschließend importieren und anderen Domänen oder agents bereitstellen können. Die Prävention vor Datenverlust speichert alle Regeleinstellungen auf Grundlage der aktuellen Konfiguration. **Hinweis** • Administratoren müssen vor dem Listenexport alle neuen oder geänderten Regeln speichern oder anwenden. • Die Prävention vor Datenverlust exportiert keine für die Richtlinie konfigurierten Ausnahmen, sondern nur die Einstellungen jeder einzelnen Regel.
Kopieren	Beim Kopieren einer Regel wird ein exaktes Abbild der aktuellen Konfigurationseinstellungen der Regel erstellt. Administratoren müssen der Regel einen neuen Namen geben und können alle erforderlichen Konfigurationsänderungen daran vornehmen.

Benachrichtigungen der Funktion "Prävention vor Datenverlust"

OfficeScan verfügt über zahlreiche Standardbenachrichtigungen, die Sie und andere OfficeScan Administratoren und agent-Benutzer über die Übertragung digitaler Assets informieren.

Weitere Informationen zu den an Administratoren gesendeten Benachrichtigungen finden Sie unter *Benachrichtigungen der Funktion "Prävention vor Datenverlust" für Administratoren auf Seite 11-58*.

Weitere Informationen zu den an agent-Benutzer gesendeten Benachrichtigungen finden Sie unter *Benachrichtigungen zur Funktion "Prävention vor Datenverlust" für Agent-Benutzer auf Seite 11-62*.

Benachrichtigungen der Funktion "Prävention vor Datenverlust" für Administratoren

Konfigurieren Sie OfficeScan so, dass eine Benachrichtigung versendet wird, wenn eine Übertragung digitaler Assets entdeckt wird, oder nur dann, wenn eine Übertragung gesperrt wird.

OfficeScan verfügt über zahlreiche Standardbenachrichtigungen, die Sie und andere Administratoren über die Übertragung digitaler Assets informieren. Sie können die Benachrichtigungen ändern und zusätzliche Benachrichtigungseinstellungen konfigurieren, die den Anforderungen des Unternehmens entsprechen.

Hinweis

OfficeScan kann Benachrichtigungen per E-Mail, SNMP-Trap und Windows NT Ereignisprotokolle versenden. Konfigurieren Sie die Einstellungen, wenn OfficeScan über diese Kanäle Benachrichtigungen versendet. Weitere Informationen finden Sie unter *Einstellungen für die Administratorbenachrichtigungen auf Seite 14-43*.

Benachrichtigung zur Funktion "Prävention vor Datenverlust" für Administratoren konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Administrator**.
2. Auf der Registerkarte **Kriterien**:
   a. Gehen Sie zum Abschnitt **Übertragungen digitaler Assets**.
   b. Bestimmen Sie, ob die Benachrichtigungen versendet werden, wenn die Übertragung digitaler Assets entdeckt wird (diese Aktion kann gesperrt oder zugelassen sein) oder wenn die Übertragung gesperrt wird.
3. Auf der Registerkarte **E-Mail**:
   a. Gehen Sie zum Abschnitt **Übertragungen digitaler Assets**.
   b. Wählen Sie **Benachrichtigung über E-Mail aktivieren**.
   c. Wählen Sie **Benachrichtigungen an Benutzer mit Agent-Hierarchie-Domänenberechtigungen senden**.

      Mit der rollenbasierten Administration können Sie Benutzern agent-Hierarchie-Domänenberechtigungen gewähren. Wenn eine Übertragung auf einem agent stattfindet, der zu einer bestimmten Domäne gehört, werden die E-Mails an die E-Mail-Adressen der Benutzer mit Domänenberechtigungen gesendet. Beispiele dafür sehen Sie in der folgenden Tabelle:

TABELLE 11-8. Agent-Hierarchiedomänen und Berechtigungen

AGENT-HIERARCHIEDOMÄNE	ROLLEN MIT DOMÄNENBERECHTIGUNGEN	BENUTZERKONTO MIT DIESER ROLLE	E-MAIL-ADRESSE FÜR DAS BENUTZERKONTO
Domäne A	Administrator (integriert)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domäne B	Administrator (integriert)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

Entdeckt ein OfficeScan Agent, der zur Domäne A gehört, eine Übertragung digitaler Assets, wird die E-Mail an mary@xyz.com, john@xyz.com und chris@xyz.com versendet.

Entdeckt ein OfficeScan Agent, der zur Domäne B gehört, die Übertragung, wird die E-Mail an mary@xyz.com und jane@xyz.com versendet.

Hinweis

Wenn Sie die Option aktivieren, benötigen alle Benutzer mit Domänenberechtigung eine entsprechende E-Mail-Adresse. Die E-Mail-Benachrichtigung wird nicht an Benutzer ohne E-Mail-Adresse gesendet. Benutzer und E-Mail-Adressen werden unter **Administration** > **Kontenverwaltung** > **Benutzerkonten** konfiguriert.

d. Wählen Sie **Benachrichtigungen an folgende E-Mail-Adresse(n) senden**, und geben Sie dann die E-Mail-Adressen ein.

e. Übernehmen oder ändern Sie die Standardbetreffzeile und -nachricht. Verwenden Sie Token-Variablen als Platzhalter für Daten in den Feldern **Betreff** und **Nachricht**.

TABELLE 11-9. Token-Variablen für Benachrichtigungen zur Funktion "Prävention vor Datenverlust"

VARIABLE	BESCHREIBUNG
%USER%	Benutzer, der am Endpunkt angemeldet war, als die Übertragung entdeckt wurde
%COMPUTER%	Endpunkt, bei dem eine Übertragung erkannt wurde
%DOMAIN%	Domäne des Endpunkts
%DATETIME%	Datum/Uhrzeit, als die Übertragung entdeckt wurde
%CHANNEL%	Der Kanal, über den die Übertragung entdeckt wurde
%TEMPLATE%	Die Vorlage für digitale Assets, durch welche die Entdeckung ausgelöst wurde
%RULE%	Name der Regel, die die Erkennung ausgelöst hat **Hinweis** Fügen Sie zur Anzeige des Regelnamens in der Nachricht diese Variable im Feld **Nachricht** hinzu.

4. Auf der Registerkarte **SNMP-Trap**:

   a. Gehen Sie zum Abschnitt **Übertragungen digitaler Assets**.

   b. Wählen Sie **Benachrichtigung per SNMP-Trap aktivieren**.

   c. Übernehmen Sie die Standardmeldung oder ändern Sie sie. Sie können Token-Variablen als Platzhalter für Daten im Feld **Nachricht** verwenden. Weitere Informationen finden Sie unter *Tabelle 11-9: Token-Variablen für Benachrichtigungen zur Funktion "Prävention vor Datenverlust" auf Seite 11-61*.

5. Auf der Registerkarte **NT Ereignisprotokoll**:

   a. Gehen Sie zum Abschnitt **Übertragungen digitaler Assets**.

   b. Wählen Sie **Benachrichtigung über NT-Ereignisprotokoll aktivieren**.

   c. Übernehmen Sie die Standardmeldung oder ändern Sie sie. Sie können Token-Variablen als Platzhalter für Daten im Feld **Nachricht** verwenden. Weitere

Informationen finden Sie unter *Tabelle 11-9: Token-Variablen für Benachrichtigungen zur Funktion "Prävention vor Datenverlust" auf Seite 11-61*.

6. Klicken Sie auf **Speichern**.

Benachrichtigungen zur Funktion "Prävention vor Datenverlust" für Agent-Benutzer

OfficeScan kann auf den agent-Computern, nachdem es die Übertragung digitaler Assets erlaubt oder gesperrt hat, sofort Benachrichtigungsmeldungen anzeigen.

Um die Benutzer darüber zu informieren, dass die Übertragung digitaler Assets gesperrt oder zugelassen wurde, wählen Sie die Option **Client-Benutzer benachrichtigen**, wenn Sie eine Richtlinie zur Prävention vor Datenverlust erstellen. Weitere Anweisungen zum Erstellen einer Richtlinie finden Sie unter *Richtlinienkonfiguration der Funktion "Prävention vor Datenverlust" auf Seite 11-51*.

Benachrichtigung zur Funktion "Prävention vor Datenverlust" für Agents konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Agent**.
2. Wählen Sie im Listenfeld **Typ** die Option **Übertragungen von digitalen Assets** aus.
3. Übernehmen Sie die Standardmeldung oder ändern Sie sie.
4. Klicken Sie auf **Speichern**.

Protokolle für 'Prävention vor Datenverlust'

Agents protokollieren Übertragungen digitaler Assets (gesperrte oder zulässige Übertragungen) und senden die Protokolle sofort an den Server. Wenn der agent die Protokolle nicht versenden kann, wiederholt er den Versuch nach 5 Minuten.

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell, oder konfigurieren Sie eine zeitgesteuerte Löschung der Protokolle. Weitere Informationen zur Protokollverwaltung finden Sie unter *Protokollmanagement auf Seite 14-47*.

Protokolle der Funktion "Prävention vor Datenverlust" anzeigen

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung** oder zu **Protokolle** > **Agents** > **Sicherheitsrisiken**.
2. Klicken Sie in der agent-Hierarchie auf das Stammsymbol ( ), um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
3. Klicken Sie auf **Protokolle** > **Protokolle für 'Prävention vor Datenverlust'**oder **Protokolle anzeigen** > **DLP-Protokolle**.
4. Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.
5. Sehen Sie die Protokolle ein.

   Die Protokolle enthalten die folgenden Informationen:

   TABELLE 11-10. Protokolldaten für Prävention vor Datenverlust

SPALTE	BESCHREIBUNG
Datum/Uhrzeit	Datum und Uhrzeit der Protokollierung des Vorfalls durch die Prävention vor Datenverlust

SPALTE	BESCHREIBUNG
Benutzer	Name des am Endpunkt angemeldeten Benutzers
Endpunkt	Name des Endpunkts, auf dem die Prävention vor Datenverlust die Übertragung entdeckt hat
Domäne	Domäne des Endpunkts
IP	Die IP-Adresse auf dem Endpunkt
Regelname	Namen der Regeln, die den Vorfall ausgelöst haben **Hinweis** Bei Regeln, die in einer früheren Version von OfficeScan erstellt wurden, wird der Standardname LEGACY_DLP_Policy angezeigt.
Kanal	Kanal, über den die Übertragung stattfand
Prozess	Prozess, der die Übertragung des digitalen Assets ermöglichte (hängt vom Kanal ab) Weitere Informationen finden Sie unter *Prozesse bezogen auf den Kanal auf Seite 11-65*.
Adresse	Adresse der Datei, in der das digitale Asset enthalten ist (oder Kanal, wenn keine Adresse verfügbar ist)
Ziel	Beabsichtigtes Ziel der Datei, in der das digitale Asset enthalten ist (oder Kanal, wenn keine Quelle verfügbar ist)
Aktion	Hinsichtlich der Übertragung ergriffene Maßnahme
Details	Link mit zusätzlichen Einzelheiten zur Übertragung Weitere Informationen finden Sie unter *Protokolle für Prävention vor Datenverlust auf Seite 11-67*.

6. Wenn Sie das Protokoll als komma-separierte Datei (`CSV-Datei`) speichern möchten, klicken Sie auf **In CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Prozesse bezogen auf den Kanal

Die folgende Tabelle enthält eine Liste mit Prozessen, die in der Spalte **Prozess** in den Protokollen der Funktion "Prävention vor Datenverlust" angezeigt werden.

TABELLE 11-11. Prozesse bezogen auf den Kanal

KANAL	PROZESS
Synchronisierungssoftware (ActiveSync)	Vollständiger Pfad- und Prozessname der Synchronisierungssoftware Beispiel: `C:\Windows\system32\WUDFHost.exe`
Datenrecorder (CD/DVD)	Vollständiger Pfad und Prozessname des Datenrecorders Beispiel: `C:\Windows\Explorer.exe`
Windows-Zwischenablage	Nicht zutreffend
E-Mail-Client - Lotus Notes	Vollständiger Pfad und Prozessname von Lotus Notes Beispiel: `C:\Programme\IBM\Lotus\Notes\nlnotes.exe`
E-Mail-Client - Microsoft Outlook	Vollständiger Pfad und Prozessname von Microsoft Outlook Beispiel: `C:\Programme\Microsoft Office\Office12\OUTLOOK.EXE`
E-Mail-Client - Alle Clients, die das SMTP-Protokoll verwenden	Vollständiger Pfad und Prozessname des E-Mail-Clients Beispiel: `C:\Programme\Mozilla Thunderbird\thunderbird.exe`
Wechseldatenträger	Prozessname der Anwendung, die Daten auf das Speichergerät oder innerhalb des Speichergeräts übertragen hat. Beispiel: `explorer.exe`

KANAL	PROZESS
FTP	Vollständiger Pfad und Prozessname des FTP-Clients Beispiel: `D:\Programme\FileZilla FTP Client\filezilla.exe`
HTTP	"HTTP-Anwendung"
HTTPS	Vollständiger Pfad und Prozessname des Browsers oder der Anwendung Beispiel: `C:\Programme\Internet Explorer\iexplore.exe`
IM-Anwendung	Vollständiger Pfad und Prozessname der IM-Anwendung Beispiel: `C:\Programme\Skype\Phone\Skype.exe`
IM-Anwendung - MSN	• Vollständiger Pfad und Prozessname von MSN Beispiel: `C:\Programme\Windows Live\Messenger\msnmsgr.exe` • "HTTP-Anwendung", wenn Daten von einem Chat-Fenster übertragen werden
Peer-to-Peer-Anwendung	Vollständiger Pfad und Prozessname der Peer-to-Peer-Anwendung Beispiel: `D:\Programme\BitTorrent\bittorrent.exe`
PGP-Verschlüsselung	Vollständiger Pfad und Prozessname der PGP-Verschlüsselungssoftware Beispiel: `C:\Programme\PGP Corporation\PGP Desktop\PGPmnApp.exe`

KANAL	PROZESS
Drucker	Vollständiger Pfad und Prozessname der Anwendung, die einen Druckervorgang initiiert hat. Beispiel: `C:\Programme\Microsoft Office\Office12\WINWORD.EXE`
SMB-Protokoll	Vollständiger Pfad und Prozessname der Anwendung, von der aus der Zugriff auf freigegebene Dateien (Kopieren oder Erstellen einer neuen Datei) erfolgt ist. Beispiel: `C:\Windows\Explorer.exe`
Webmail (HTTP-Modus)	"HTTP-Anwendung"
Webmail (HTTPS-Modus)	Vollständiger Pfad und Prozessname des Browsers oder der Anwendung Beispiel: `C:\Programme\Mozilla Firefox\firefox.exe`

Protokolle für Prävention vor Datenverlust

Der Bildschirm **Protokolle für Prävention vor Datenverlust** enthält zusätzliche Details zur Übertragung digitaler Assets. Die Übertragungsdetails hängen vom Kanal und vom Prozess ab, in dem der Vorfall von OfficeScan entdeckt wurde.

Die folgende Tabelle enthält eine Liste aller angezeigten Informationen.

TABELLE 11-12. Protokolle für Prävention vor Datenverlust

DETAIL	BESCHREIBUNG
Datum/Uhrzeit	Datum und Uhrzeit der Protokollierung des Vorfalls durch die Prävention vor Datenverlust
Verstoß-ID	Eindeutige ID des Vorfalls
Benutzer	Name des am Endpunkt angemeldeten Benutzers

Detail	Beschreibung
Endpunkt	Name des Endpunkts, auf dem die Prävention vor Datenverlust die Übertragung entdeckt hat
Domäne	Domäne des Endpunkts
IP	Die IP-Adresse auf dem Endpunkt
Kanal	Kanal, über den die Übertragung stattfand
Prozess	Prozess, der die Übertragung des digitalen Assets ermöglichte (hängt vom Kanal ab) Weitere Informationen finden Sie unter *Prozesse bezogen auf den Kanal auf Seite 11-65*.
Adresse	Adresse der Datei, in der das digitale Asset enthalten ist (oder Kanal, wenn keine Adresse verfügbar ist)
E-Mail-Absender	E-Mail-Adresse, von der die Übertragung ausging
E-Mail-Betreff	Betreffzeile der E-Mail-Nachricht, in der das digitale Asset enthalten ist
E-Mail-Empfänger	Zieladresse(n) der E-Mail-Nachricht
URL	URL einer Website oder Webseite
FTP-Benutzer	Der zum Anmelden am FTP-Server verwendete Benutzername
Dateiklasse	Typ der Datei, in der das digitale Asset durch die Prävention vor Datenverlust entdeckt wurde
Regel/Vorlage	Liste der genauen Regelnamen und Vorlagen, durch die die Erkennung ausgelöst wurde; **Hinweis** jede Regel kann mehrere Vorlagen enthalten, die zur Auslösung des Ereignisses führten. Vorlagennamen werden durch Kommas getrennt.
Aktion	Hinsichtlich der Übertragung ergriffene Maßnahme

DETAIL	BESCHREIBUNG
Benutzerrechtfertigungsgrund	Grund des Benutzers zum Fortsetzen der Übertragung der vertraulichen Daten

Debug-Protokollierung für das Datenschutzmodul aktivieren

Prozedur

1. Beziehen Sie die Datei `logger.cfg` von Ihrem Support-Anbieter.
2. Fügen Sie die folgenden Daten zu `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite` (für 32-Bit-Systeme) oder `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\DlpLite` (für 64-Bit-Systeme):
   - **Typ**: `String`
   - **Name**: `debugcfg`
   - **Wert**: `C:\Log\logger.cfg`
3. Erstellen Sie einen Ordner mit dem Namen „Protokoll“ im Verzeichnis `C:\`.
4. Kopieren Sie `logger.cfg` in den Ordner „Protokoll“.
5. Verteilen Sie die Einstellungen für die Funktion "Prävention vor Datenverlust" und die Gerätesteuerung über die Webkonsole, um mit dem Sammeln der Protokolle zu beginnen.

Hinweis

Deaktivieren Sie die Debug-Protokollierung für das Datenschutzmodul, indem Sie `debugcfg` im Registrierungsschlüssel löschen und den Endpunkt neu starten.

Kapitel 12

Verwenden von Web Reputation

In diesem Kapitel werden Internet-Bedrohungen beschrieben, und es wird erläutert, wie Ihr Netzwerk und Ihre Computer mit Hilfe von OfficeScan vor diesen Bedrohungen geschützt werden können.

Es werden folgende Themen behandelt:

- *Info über Internet-Bedrohungen auf Seite 12-2*
- *Command & Control-Kontaktalarmdienste auf Seite 12-2*
- *Web Reputation auf Seite 12-4*
- *Web-Reputation-Richtlinien auf Seite 12-5*
- *Benachrichtigungen über Internet-Bedrohungen für Agent-Benutzer auf Seite 12-14*
- *C&C-Callback-Benachrichtigungen für Administratoren auf Seite 12-15*
- *C &C-Callback-Ausbrüche auf Seite 12-20*
- *Protokolle für Internet-Bedrohungen auf Seite 12-23*

Info über Internet-Bedrohungen

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 Endpunkt befindet, wird der Code ständig verändert, um einer Entdeckung zu entgehen.

In den vergangenen Jahren nannte man sie Hacker, Viren-Schreiber, Spammer oder Spyware-Autoren – heute heißen sie Cyber-Kriminelle. Internet-Bedrohungen helfen diesen Personen bei der Erreichung eines von zwei Zielen. Eines der Ziele ist der Diebstahl von Informationen für den anschließenden Verkauf. Dies führt zum Durchsickern vertraulicher Informationen in Form von Identitätsverlust. Infizierte Endpunkt können außerdem als Überträger für Phishing-Angriffe eingesetzt oder anderweitig zur Informationsbeschaffung missbraucht werden. Neben anderen Auswirkungen hat diese Bedrohung ein Potenzial, das Vertrauen in den Internet-Handel zu untergraben und so die Grundlage für Transaktionen im Internet zu korrumpieren. Das zweite Ziel ist die Fremdsteuerung der Prozessorkapazität eines Computers, um diese für profitable Aktivitäten zu missbrauchen. Die Aktivitäten reichen vom Spam-Versand über Erpressung in Form des Versands von Denial-of-Service-Angriffen bis hin zu Aktivitäten mit Klickvergütung (Pay per Click).

Command & Control-Kontaktalarmdienste

Trend Micro Command & Control (C&C)-Kontaktalarmdienste bieten verbesserte Erkennungs- und Warnungsfunktionen zur Minderung des Schadens infolge von erweiterten permanenten Bedrohungen und gezielten Angriffen. C&C-Kontaktalarmdienste sind in die Web-Reputation-Dienste integriert, wodurch die durchzuführende Aktion der erkannten Callback-Adresse basierend auf der Sicherheitsstufe der Web Reputation ermittelt wird.

Die C&C-IP-Liste verbessert die C&C-Callback-Erkennungen weiter, indem die Prüf-Engine für Netzwerkinhalte (Network Content Inspection Engine, NCIE) verwendet wird, um C&C-Kontakte durch jeden Netzwerkkanal zu erkennen.

Weitere Informationen zur Konfiguration der Sicherheitsstufe der Web-Reputation-Dienste finden Sie unter *Eine Web-Reputation-Richtlinie konfigurieren auf Seite 12-5*.

TABELLE 12-1. Funktionen der C&C-Kontaktalarmdienste

FUNKTION	BESCHREIBUNG
Global Intelligence-Liste	Trend Micro Smart Protection Network stellt die Global Intelligence-Liste anhand von Quellen auf der ganzen Welt zusammen und testet und bewertet die Risikostufe jeder C&C-Callback-Adresse. Web-Reputation-Dienste nutzen die Global Intelligence-Liste zusammen mit den Reputationsbewertungen bösartiger Websites, um für erhöhten Schutz vor erweiterten Bedrohungen zu sorgen. Die Web-Reputation-Sicherheitsstufe legt anhand zugewiesener Risikostufen die Maßnahme fest, die bei bösartigen Websites oder C&C-Servern ergriffen wird.
Virtual Analyzer Liste	Smart Protection Servers können mit Virtual Analyzer integriert werden, um die Virtual Analyzer C&C-Serverliste zu erhalten. Virtual Analyzer wertet potenzielle Risiken in einer sicheren Umgebung aus und weist den analysierten Bedrohungen mit Hilfe leistungsfähiger heuristischer Verfahren und Verhaltenstests eine Risikostufe zu. Virtual Analyzer füllt die Virtual Analyzer Liste mit allen Bedrohungen, die versuchen, eine Verbindung mit einem möglichen C&C-Server herzustellen. Die Virtual Analyzer Liste ist hochgradig firmenspezifisch und bietet eine anpassbare Verteidigungsmöglichkeit gegen gezielte Angriffe. OfficeScan ruft die Liste von Virtual Analyzer ab und kann alle denkbaren C&C-Bedrohungen sowohl mit der Global Intelligence Liste als auch der lokalen Virtual Analyzer Liste abgleichen. Einzelheiten zum Einbinden der Virtual Analyzer Listen der verdächtigen Objekte finden Sie unter *Einstellungen für Liste der verdächtigen Objekte konfigurieren auf Seite 14-39*.
Verdächtiger Verbindungsdienst	Der Dienst für verdächtige Verbindungen verwaltet die benutzerdefinierten und globalen C&C-IP-Listen und überwacht das Verhalten von Verbindungen, die Endpunkte zu potenziellen C&C-Servern herstellen. Weitere Informationen finden Sie unter *Verdächtiger Verbindungsdienst auf Seite 8-6*.

FUNKTION	BESCHREIBUNG
Administratorbenachrichtigungen	Administratoren können nach Erkennung eines C&C-Callbacks nach Bedarf detaillierte und anpassbare Benachrichtigungen erhalten. Weitere Informationen finden Sie unter *C&C-Callback-Benachrichtigungen für Administratoren konfigurieren auf Seite 12-16*.
Agent-Benachrichtigungen	Administratoren können nach Erkennung eines C&C-Callbacks auf einem Endpunkt nach Bedarf detaillierte und anpassbare Benachrichtigungen an Endbenutzer versenden. Weitere Informationen finden Sie unter *C&C-Kontaktalarmbenachrichtigungen für Agent-Benutzer auf Seite 12-19*.
Ausbruchsbenachrichtigungen	Administratoren können Ausbruchsbenachrichtigungen für spezifische C&C-Callback-Ereignisse anpassen und angeben, ob ein Ausbruch auf einem einzelnen Endpunkt oder im ganzen Netzwerk auftritt. Weitere Informationen finden Sie unter *C &C-Callback-Ausbrüche auf Seite 12-20*.
C&C-Callback-Protokolle	Protokolle enthalten detaillierte Angaben zu allen C&C-Callback-Ereignissen. Weitere Informationen finden Sie unter *C&C Callback-Protokolle anzeigen auf Seite 12-25*.

Web Reputation

Die Web-Reputation-Technologie bewertet die Glaubwürdigkeit von Webdomänen nach einem Scoring-Verfahren, indem Informationen wie das Alter einer Website, historische Änderungen des Speicherorts und Anzeichen von verdächtigen Aktivitäten zurückverfolgt werden, die durch die Malware-Verhaltensanalyse entdeckt wurden. Trend Micro analysiert ständig Websites und aktualisiert Web-Reputation-Bewertungen, um zu verhindern, dass Benutzer auf potenziell bösartige Inhalte zugreifen.

Wenn ein Benutzer versucht, auf eine Website zuzugreifen, fragt der OfficeScan Agent eine Smart Protection Quelle ab, um die Risikostufe des Inhalts zu ermitteln. Die konfigurierte Web-Reputation-Richtlinie für den OfficeScan Agent bestimmt, ob der Zugriff auf die Website zulässig ist.

Hinweis

Weitere Informationen zu Smart Protection Quellen finden Sie unter *Liste der Smart Protection Quellen auf Seite 4-23*.

Web Reputation ermöglicht Ihnen das Hinzufügen von Websites zu Listen zulässiger oder gesperrter Websites, die Sie als sicher oder gefährlich erachten. Der OfficeScan Agent fragt keine Web-Reputation-Bewertungen für Websites ab, die den Listen hinzugefügt wurden, sondern sperrt stattdessen den Zugriff automatisch oder lässt ihn zu.

Web-Reputation-Richtlinien

Web-Reputation-Richtlinien bestimmen, ob OfficeScan den Zugriff auf eine Website zulässt oder sperrt.

Sie können Richtlinien für interne und externe agents konfigurieren. OfficeScan Administratoren konfigurieren in der Regel eine strengere Richtlinie für externe agents.

Richtlinien sind detaillierte Einstellungen in der OfficeScan agent-Hierarchie. Sie können bestimmte Richtlinien für agent-Gruppen oder einzelne agents erzwingen. Sie können auch eine einzelne Richtlinie für alle agents erzwingen.

Nachdem Sie die Richtlinien verteilt haben, verwenden die agents die Standortkriterien, die Sie im Fenster **Endpunktspeicherort** festgelegt haben, (siehe *Endpunktspeicherort auf Seite 15-2*), um deren Standort und die erforderliche Richtlinie zu bestimmen. Agents Agents wechseln die Richtlinien mit jedem Standortwechsel.

Eine Web-Reputation-Richtlinie konfigurieren

Legen Sie die Anmeldedaten zur Proxy-Server-Authentifizierung fest, wenn die HTTP-Kommunikation in Ihrem Unternehmen über den Proxy-Server erfolgt und eine Authentifizierung vor dem Internet-Zugriff erforderlich ist.

Weitere Informationen finden Sie unter *Proxy-Einstellungen für externen Agent konfigurieren auf Seite 15-57*.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Wählen Sie die Ziele in der Agent-Hierarchie aus.
   - Um Richtlinien für Agents zu konfigurieren, auf denen Windows Desktop-Plattformen ausgeführt werden, wählen Sie das Symbol der Root-Domäne ( ), bestimmte Domänen oder Agents aus.

     Hinweis

     Wenn Sie die Root-Domäne oder bestimmte Domänen auswählen, gilt die Einstellung nur für agents unter Windows Desktop-Plattformen. Diese Einstellung gilt nicht für Agents unter einer beliebigen Windows Server-Plattform, selbst wenn sie zu den Domänen gehören.

   - Wählen Sie zum Konfigurieren einer Richtlinie für Agents unter Windows Server-Plattformen einen bestimmten Agent aus.
3. Klicken Sie auf **Einstellungen** > **Web-Reputation-Einstellungen**.
4. Klicken Sie auf die Registerkarte **Externe Agents**, um eine Richtlinie für externe Agents zu konfigurieren, oder auf die Registerkarte **Interne Agents**, um eine Richtlinie für interne Agents zu konfigurieren.

   Tipp

   Konfigurieren Sie die Einstellungen zum Agent-Standort, soweit dies noch nicht geschehen ist. Agents verwenden diese Einstellungen, um ihren Standort zu bestimmen und die richtige Web-Reputation-Richtlinie anzuwenden. Weitere Informationen finden Sie unter *Endpunktspeicherort auf Seite 15-2*.
5. Wählen Sie unter **Web Reputation unter den folgenden Betriebssystemen aktivieren** die Arten der zu schützenden Windows-Plattformen aus (**Windows Desktop-Plattformen** und **Windows Server-Plattformen**).

   Welche Betriebssysteme in diesem Fenster aufgelistet werden, hängt davon ab, welche Ziele Sie in Schritt 1 gewählt haben.

Tipp

Trend Micro empfiehlt, Web Reputation für interne Agents zu deaktivieren, wenn Sie bereits ein Trend Micro Produkt mit einer Web-Reputation-Funktion (z. B. InterScan Web Security Virtual Appliance) verwenden.

Wenn eine Web-Reputation-Richtlinie aktiviert ist:

- Externe Agents senden Web-Reputation-Abfragen an das Smart Protection Network.
- Interne Agents senden Web-Reputation-Abfragen an:
  - Smart Protection Server, wenn die Option **Anfragen an Smart Protection Server senden** aktiviert ist. Weitere Informationen über diese Option finden Sie unter Schritt 7.
  - Smart Protection Network, wenn die Option **Anfragen an Smart Protection Server senden** deaktiviert ist.

6. Wählen Sie **Bewertungsmodus aktivieren** aus.

Hinweis

Gestatten Sie OfficeScan Agents den Zugriff auf alle Websites, wenn Sie sich im Bewertungsmodus befinden. Für alle besuchten Websites, die gegen die konfigurierte Einstellung für die **Sicherheitsstufe** verstoßen, protokolliert der OfficeScan Agent das Ereignis. Im Bewertungsmodus können Sie den Websitezugriff überwachen und die Sicherheit von Websites bewerten, bevor Sie den Benutzerzugriff aktiv sperren. Anhand der Bewertung in den Zugriffsprotokollen können Sie vertrauenswürdige Websites zur Liste der zulässigen URLs hinzufügen, bevor Sie den Bewertungsmodus deaktivieren.

7. Wählen Sie **HTTPS-URLs prüfen** aus.

HTTPS-Kommunikation verwendet Zertifikate zum Identifizieren von Webservern. Sie verschlüsselt Daten, um Datendiebstahl und Abhörvorgänge zu verhindern. Obwohl HTTPS beim Zugriff auf Websites mehr Schutz bietet, verbleiben bei der Nutzung Risiken. Sites, die von Hackern übernommen wurden, können trotz gültiger Zertifikate Malware anbieten und persönliche Daten stehlen. Außerdem sind Zertifikate relativ einfach zu beschaffen, wodurch sich das Einrichten bösartiger Webserver, die HTTPS nutzen, einfach gestaltet.

Aktivieren Sie das Prüfen von HTTPS-URLs, um die Gefährdung durch infizierte und bösartige Websites, die HTTPS verwenden, zu verringern. Web Reputation kann HTTPS-Datenverkehr auf den folgenden Browsern überwachen:

TABELLE 12-2. Browser, die den HTTPS-Datenverkehr unterstützen

BROWSER	VERSION
Microsoft Internet Explorer	• 8.x • 9.x • 10.x • 11.x
Mozilla Firefox	3.5 oder höher
Chrome	Aktuelle Version
Microsoft Edge	Aktuelle Version

Wichtig

- Die HTTPS-Suchfunktion unterstützt nur Windows 8-, Windows 8.1-, Windows 10- und Windows 2012-Plattformen im Desktop-Modus.
- Firefox, Microsoft Edge und Chrome (die HTTPS-Suchfunktion in diesen Browsern wird nicht auf Windows XP-, Server 2003/2003 R2- oder Server 2008-Plattformen unterstützt)

  Sie müssen den Unauthorized Change Prevention Service und die Funktion **Programmüberprüfung zum Erkennen und Sperren gefährdeter ausführbarer Dateien** der Verhaltensüberwachung auf Agents aktivieren, um den HTTPS-Datenverkehr zu durchsuchen.
- Nachdem die HTTPS-Suchfunktion zum ersten Mal auf OfficeScan Agents aktiviert wurde, müssen die Benutzer das erforderliche Add-On im Browser aktivieren. Erst dann ist die HTTPS-Suchfunktion betriebsbereit.
  - Internet Explorer 9, 10 und 11

    Bei OfficeScan Agents mit Windows 7, 8, 8.1, 10, Server 2008 R2 oder Server 2012 müssen die Benutzer das Add-On `Trend Micro Osprey Plugin Class` im Browser-Popup-Fenster aktivieren.

    Bei OfficeScan Agents mit Windows XP, Server 2003 oder Server 2008 müssen die Benutzer das Add-On `TmIEPlugInBHO Class` im Browser-Popup-Fenster aktivieren.

  Weitere Informationen zum Konfigurieren der Internet Explorer-Einstellungen für Web Reputation finden Sie in den folgenden Knowledge Base-Artikeln:

  - http://esupport.trendmicro.com/solution/en-us/1060643.aspx
  - http://esupport.trendmicro.com/solution/en-us/1095350.aspx

8. Wählen Sie **Nur gängige HTTP-Ports durchsuchen**, um die Web-Reputation-Suche auf die Ports 80, 81 und 8080 zu beschränken. Standardmäßig durchsucht Web Reputation den gesamten Datenverkehr auf allen Ports.

Hinweis

Nicht unterstützt unter Windows 7, 8, 8.1, 10 oder Windows Server 2008 R2, 2012 oder höheren Plattformen.

9. Wählen Sie für interne OfficeScan Agents die Option **Abfragen an Smart Protection Server senden** aus, wenn OfficeScan Agents Web-Reputation-Abfragen an Smart Protection Server senden sollen.

   - Wenn Sie diese Option aktivieren:

     - Agents ermitteln anhand der Liste der Smart Protection Quelle den Smart Protection Server, an den sie ihre Abfragen senden.

       Weitere Informationen über die Liste der Smart Protection Quellen finden Sie unter *Liste der Smart Protection Quellen auf Seite 4-23*.

     - Stellen Sie sicher, dass die Smart Protection Server verfügbar sind. Wenn kein Smart Protection Server verfügbar ist, senden die Agents keine Abfragen an das Smart Protection Network. Die einzig verbleibenden Quellen der Web-Reputation-Daten für Agents sind die Listen zulässiger und gesperrter URLs.

     - Wenn agents eine Verbindung zu Smart Protection Servern über einen Proxy-Server herstellen können sollen, geben Sie die Proxy-Einstellungen im Abschnitt **Interner Proxy** auf der Registerkarte **Administration** > **Einstellungen** > **Proxy > Agent** an.

     - Aktualisieren Sie die Smart Protection Server regelmäßig, damit der Schutz stets aktuell ist.

     - Nicht getestete Websites werden von den Agents nicht gesperrt. Die Smart Protection Server speichern keine Web-Reputation-Daten für diese Websites.

   - Wenn Sie diese Option deaktivieren:

     - Agents senden Web-Reputation-Abfragen an das Smart Protection Network. Endpunkte benötigen eine Internetverbindung für den erfolgreichen Versand von Abfragen.

     - Wenn für die Verbindung mit dem Smart Protection Network Proxy-Server-Authentifizierung erforderlich ist, müssen Sie die Authentifizierungsdaten unter **Administration** > **Einstellungen** > **Proxy > Agent (Registerkarte)** > **Externer Proxy**.

- Nicht getestete Websites werden von Agents gesperrt, wenn Sie **Seiten sperren, die nicht von Trend Micro getestet wurden** auswählen.

10. Wählen Sie unter den vorhandenen Web-Reputation-Sicherheitsstufen aus: **Hoch**, **Mittel** oder **Niedrig**

Hinweis

Die Sicherheitsstufen legen fest, ob Web Reputation den Zugriff auf eine URL zulässt oder sperrt. Wenn zum Beispiel die Sicherheitsstufe auf "Niedrig" festgelegt ist, sperrt Web Reputation nur URLs, die als Internetbedrohung bekannt sind. Bei einer Erhöhung der Sicherheitsstufe verbessert sich die Erkennungsrate von Internet-Bedrohungen, doch gleichzeitig steigt auch die Wahrscheinlichkeit von Fehlalarmen.

11. Wenn Sie die Option **Abfragen an Smart Protection Server senden** deaktiviert haben, können Sie **Seiten sperren, die nicht von Trend Micro getestet wurden** auswählen.

Hinweis

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.

12. Wählen Sie **Seiten mit bösartigem Skript sperren**, um Webbrowser-Schwachstellen und bösartige Skripts zu identifizieren und die Gefährdung des Webbrowsers durch diese Bedrohungen zu verhindern.

    Web Reputation verwendet sowohl das Pattern zur Erkennung von Browser-Schwachstellen als auch das Pattern der Skriptanalyse, um Webseiten zu identifizieren und zu sperren, bevor das System gefährdet wird.

TABELLE 12-3. Unterstützte Browser für die Verhinderung von Browser-Schwachstellen

BROWSER	VERSION
Microsoft Internet Explorer	• 7.x • 8.x • 9.x • 10.x • 11.x

Wichtig

Für die Funktion zur Verhinderung von Browser-Schwachstellen müssen Sie den erweiterten Schutzdienst aktivieren.

Navigieren Sie zu **Agents** > **Agent-Verwaltung**, klicken Sie auf **Einstellungen** > **Zusätzliche Diensteinstellungen**, um den "Erweiterten Schutzdienst" zu aktivieren.

Nachdem die Funktion zur Verhinderung von Browser-Schwachstellen das erste Mal auf OfficeScan Agents aktiviert wurde, müssen die Benutzer das erforderliche Add-On im Browser aktivieren, damit die Verhinderung von Browser-Schwachstellen funktioniert. Bei OfficeScan Agents mit Internet Explorer 9, 10 oder 11 müssen die Benutzer das Add-On `Trend Micro IE Protection` im Browser-Popup-Fenster aktivieren.

13. Konfigurieren Sie die Liste der zulässigen und gesperrten Absender.

Hinweis

Die Liste der zulässigen URLs hat Vorrang vor der Liste der gesperrten URLs. Wenn eine URL einem Eintrag in der Liste der zulässigen URLs entspricht, gewähren die Agents stets Zugriff, selbst wenn sie sich in der Liste der gesperrten URLs befindet.

a. Wählen Sie **Liste 'Zulässig/Gesperrt' aktivieren** aus.

b. Geben Sie einen URL ein.

Sie können an jeder Stelle im Link ein Platzhalterzeichen (*) verwenden.

Beispiel:

- Wenn Sie `www.trendmicro.com/*` eingeben, bedeutet das, dass Web Reputation alle Seiten der Website von Trend Micro zulässt.
- Wenn Sie `*.trendmicro.com/*` eingeben, bedeutet das, dass Web Reputation alle Seiten in jeder Unterdomäne von `trendmicro.com` zulässt.

Sie können URLs eingeben, die IP-Adressen enthalten. Wenn Sie einen URL eingeben, der eine IPv6-Adresse enthält, setzen Sie die Adresse in Klammern.

c. Klicken Sie auf **Zur Liste der zulässigen URLs hinzufügen** oder **Zur Liste der gesperrten URLs hinzufügen**.

d. Um die Liste in eine `.dat`-Datei zu exportieren, klicken Sie auf **Exportieren**, und klicken Sie anschließend auf **Speichern**.

e. Wenn Sie eine Liste von einem anderen Server exportiert haben und sie in dieses Fenster importieren möchten, klicken Sie auf **Importieren**, und navigieren Sie zur `.dat`-Datei. Die Liste wird in das Fenster geladen.

Wichtig

Web Reputation durchsucht keine Adressen in der Liste der zulässigen und gesperrten URLs.

14. Um einen Kommentar zu Web Reputation abzugeben, klicken Sie auf den entsprechenden Link unter **Neubewertung URL**. Das Trend Micro Web Reputation Hilfesystem wird in einem Browser-Fenster geöffnet.

15. Wählen Sie, ob der OfficeScan Agent Web-Reputation-Protokolle an den Server senden darf. Gestatten Sie Agents das Senden von Protokollen, wenn Sie die von Web Reputation gesperrten URLs analysieren und bei als sicher eingestuften URLs eine entsprechende Aktion durchführen möchten.

16. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

- **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen

Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Benachrichtigungen über Internet-Bedrohungen für Agent-Benutzer

OfficeScan kann unmittelbar nach der Sperrung einer URL, die gegen eine Web-Reputation-Richtlinie verstößt, eine Benachrichtigung auf dem OfficeScan Agent-Endpunkt anzeigen. Sie müssen die Benachrichtigung aktivieren und können optional den Inhalt der Benachrichtigung ändern.

Benachrichtigung über Internet-Bedrohungen aktivieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Klicken Sie auf die Registerkarte **Andere Einstellungen**.
5. Wählen Sie im Abschnitt **Web-Reputation-Einstellungen** die Option **Bei Zugriff auf gesperrte Websites wird eine Benachrichtigung angezeigt** aus.
6. Wählen Sie im Abschnitt **C&C-Callback-Einstellungen** die Option **Benachrichtigung anzeigen, wenn ein C&C-Callback erkannt wird** aus.

7. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Benachrichtigungen über Internet-Bedrohungen ändern

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Agent**.
2. Wählen Sie im Listenfeld **Typ** den Typ der Benachrichtigung über Internet-Bedrohungen aus, der geändert werden soll:
   - **Verstöße gegen die Web Reputation**
   - **C&C-Callbacks**
3. Sie können die Standardmeldung im dafür vorgesehenen Textfeld bearbeiten.
4. Klicken Sie auf **Speichern**.

C&C-Callback-Benachrichtigungen für Administratoren

OfficeScan verfügt über zahlreiche Standardbenachrichtigungen, die Sie und andere OfficeScan Administratoren über entdeckte C&C-Callbacks informieren. Sie können

diese Benachrichtigungen ändern und zusätzliche Benachrichtigungseinstellungen konfigurieren, die Ihren Anforderungen entsprechen.

C&C-Callback-Benachrichtigungen für Administratoren konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Administrator**.
2. Auf der Registerkarte **Kriterien**:
   a. Navigieren Sie zum Abschnitt **C&C-Callbacks**.
   b. Geben Sie an, ob Benachrichtigungen beim Entdecken eines C&C-Callbacks durch OfficeScan (die Aktion kann unterdrückt oder protokolliert werden) oder nur bei einer hohen Risikostufe der Callback-Adresse gesendet werden sollen.
3. Auf der Registerkarte **E-Mail**:
   a. Navigieren Sie zum Abschnitt **C&C-Callbacks**.
   b. Wählen Sie **Benachrichtigung über E-Mail aktivieren**.
   c. Wählen Sie **Benachrichtigungen an Benutzer mit Agent-Hierarchie-Domänenberechtigungen senden**.

      Mit der rollenbasierten Administration können Sie Benutzern agent-Hierarchie-Domänenberechtigungen gewähren. Wenn eine Übertragung auf einem agent stattfindet, der zu einer bestimmten Domäne gehört, werden die E-Mails an die E-Mail-Adressen der Benutzer mit Domänenberechtigungen gesendet. Beispiele dafür sehen Sie in der folgenden Tabelle:

TABELLE 12-4. Agent-Hierarchiedomänen und Berechtigungen

AGENT-HIERARCHIEDOMÄNE	ROLLEN MIT DOMÄNENBERECHTIGUNGEN	BENUTZERKONTO MIT DIESER ROLLE	E-MAIL-ADRESSE FÜR DAS BENUTZERKONTO
Domäne A	Administrator (integriert)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domäne B	Administrator (integriert)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

Entdeckt ein OfficeScan Agent, der zur Domäne A gehört, einen C&C-Callback, wird die E-Mail an mary@xyz.com, john@xyz.com und chris@xyz.com gesendet.

Entdeckt ein OfficeScan Agent, der zur Domäne B gehört, den C&C-Callback, wird die E-Mail an mary@xyz.com und jane@xyz.com versendet.

Hinweis

Wenn Sie die Option aktivieren, benötigen alle Benutzer mit Domänenberechtigung eine entsprechende E-Mail-Adresse. Die E-Mail-Benachrichtigung wird nicht an Benutzer ohne E-Mail-Adresse gesendet. Benutzer und E-Mail-Adressen werden unter **Administration** > **Kontenverwaltung** > **Benutzerkonten** konfiguriert.

d. Wählen Sie **Benachrichtigungen an folgende E-Mail-Adresse(n) senden**, und geben Sie dann die E-Mail-Adressen ein.

e. Übernehmen oder ändern Sie die Standardbetreffzeile und -nachricht. Verwenden Sie Token-Variablen als Platzhalter für Daten in den Feldern **Betreff** und **Nachricht**.

TABELLE 12-5. Token-Variablen für C&C-Callback-Benachrichtigungen

VARIABLE	BESCHREIBUNG
%CLIENTCOMPUTER%	Zielendpunkt, der den Callback gesendet hat
%IP%	IP-Adresse des Zielendpunkts
%DOMAIN%	Domäne des Endpunkts
%DATETIME%	Datum und Uhrzeit, als die Übertragung entdeckt wurde
%CALLBACKADDRESS%	Callback-Adresse des C&C-Servers
%CNCRISKLEVEL%	Risikostufe des C&C-Servers
%CNCLISTSOURCE%	Gibt die C&C-Quellenliste an
%ACTION%	Durchgeführte Aktion

4. Auf der Registerkarte **SNMP-Trap**:

   a. Navigieren Sie zum Abschnitt **C&C-Callbacks**.

   b. Wählen Sie **Benachrichtigung per SNMP-Trap aktivieren**.

   c. Übernehmen Sie die Standardmeldung oder ändern Sie sie. Sie können Token-Variablen als Platzhalter für Daten im Feld **Nachricht** verwenden. Weitere Informationen finden Sie unter *Tabelle 12-5: Token-Variablen für C&C-Callback-Benachrichtigungen auf Seite 12-18*.

5. Auf der Registerkarte **NT Ereignisprotokoll**:

   a. Navigieren Sie zum Abschnitt **C&C-Callbacks**.

   b. Wählen Sie **Benachrichtigung über NT-Ereignisprotokoll aktivieren**.

   c. Übernehmen Sie die Standardmeldung oder ändern Sie sie. Sie können Token-Variablen als Platzhalter für Daten im Feld **Nachricht** verwenden. Weitere Informationen finden Sie unter *Tabelle 12-5: Token-Variablen für C&C-Callback-Benachrichtigungen auf Seite 12-18*.

6. Klicken Sie auf **Speichern**.

C&C-Kontaktalarmbenachrichtigungen für Agent-Benutzer

OfficeScan kann auf einem OfficeScan Agent-Computer sofort eine Benachrichtigung anzeigen, nachdem eine C&C-Server-URL gesperrt wurde. Sie müssen die Benachrichtigung aktivieren und können optional den Inhalt der Benachrichtigung ändern.

C&C-Callback-Benachrichtigung aktivieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Klicken Sie auf die Registerkarte **Andere Einstellungen**.
5. Wählen Sie im Abschnitt **C&C-Callback-Einstellungen** die Option **Benachrichtigung anzeigen, wenn ein C&C-Callback erkannt wird** aus.
6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option

werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

C&C-Callback-Benachrichtigungen konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Agent**.
2. Wählen Sie aus dem Listenfeld **Typ** die Option **C&C-Callbacks** aus.
3. Sie können die Standardmeldung im dafür vorgesehenen Textfeld bearbeiten.
4. Klicken Sie auf **Speichern**.

C &C-Callback-Ausbrüche

Legen Sie einen C&C-Callback-Ausbruch anhand der Anzahl, Quelle und Risikostufe der Callbacks fest.

OfficeScan verfügt über zahlreiche Standardbenachrichtigungen, die Sie und andere OfficeScan Administratoren über einen Ausbruch informieren. Sie können die Benachrichtigung ändern, damit sie Ihren Anforderungen entspricht.

Hinweis

OfficeScan kann C&C-Callback-Ausbruchsbenachrichtigungen per E-Mail versenden. Konfigurieren Sie E-Mail-Einstellungen, damit OfficeScan die E-Mails erfolgreich versenden kann. Weitere Informationen finden Sie unter *Einstellungen für die Administratorbenachrichtigungen auf Seite 14-43*.

C&C-Callback-Ausbruchskriterien und -Benachrichtigungen konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Ausbruch**.

   Das Fenster **Ausbruchsbenachrichtigungen** wird angezeigt.

2. Konfigurieren Sie auf der Registerkarte **Kriterien** im Abschnitt **C&C-Callbacks** die folgenden Einstellungen:

OPTION	BEZEICHNUNG
Gleicher infizierter Host	Wählen Sie dies aus, um einen Ausbruch auf Grundlage der Callback-Erkennungen pro Endpunkt zu definieren.
C&C-Risikostufe	Geben Sie an, ob ein Ausbruch bei allen C&C-Callbacks oder nur bei Quellen mit hohem Risiko ausgelöst werden soll.
Aktion	Geben Sie an, welche Aktionen OfficeScan zählt, um ein Ausbruchsszenario zu bestimmen.
Funde	Geben Sie die Anzahl der Funde an, die OfficeScan überschreiten muss, damit ein Ausbruchszenario ausgelöst wird.
Zeitraum	Bestimmen Sie den Überwachungszeitraum.

3. Auf der Registerkarte **E-Mail**:

   a. Wählen Sie im Abschnitt **C&C-Callbacks** die Option **Benachrichtigung über E-Mail aktivieren** aus.

   b. Geben Sie im Feld **An** die E-Mail-Empfänger an.

   c. Geben Sie im Feld **Betreff** den Betreff der E-Mail-Benachrichtigung ein.

   d. Geben Sie im Feld **Nachricht** den Inhalt der Nachricht ein.

      OfficeScan unterstützt die Verwendung von Token in den Feldern **Betreff** und **Nachricht**.

TABELLE 12-6. Token-Variablen für C&C-Callback-Ausbruchsbenachrichtigungen

TOKEN-VARIABLE	BESCHREIBUNG
%C	Anzahl der C&C-Callback-Protokolle
%T	Zeitraum, in dem die C&C-Callback-Protokolle gesammelt wurden

e. Geben Sie zusätzliche Protokolldaten an, die in der Benachrichtigung (im Tabellenformat) enthalten sein sollen.

PROTOKOLLSPALTE	BESCHREIBUNG
Datum/Uhrzeit	Datum und Uhrzeit der Erkennung
Infizierter Host	Endpunkt mit Erkennung
IP-Adresse	IP-Adresse des infizierten Hosts
Domäne	Domäne des Endpunkts, auf dem die Erkennung erfolgte
Callback-Adresse	Name der URL, die die Erkennung ausgelöst hat
C&C-Risikostufe	Die Risikostufe der Callback-Adresse
C&C-Listenquelle	Die C&C-Listenquelle, die den C&C-Server identifiziert hat
Aktion	Für das Sicherheitsrisiko durchgeführte Aktionen

4. Auf der Registerkarte **SNMP-Trap**:

   a. Navigieren Sie zum Abschnitt **C&C-Callbacks**.

   b. Wählen Sie **Benachrichtigung per SNMP-Trap aktivieren**.

   c. übernehmen Sie die Standardmeldung oder ändern Sie sie. Sie können Token-Variablen als Platzhalter für Daten im Feld **Nachricht** verwenden. Weitere

Informationen finden Sie unter *Tabelle 12-6: Token-Variablen für C&C-Callback-Ausbruchsbenachrichtigungen auf Seite 12-22*.

5. Auf der Registerkarte **NT-Ereignisprotokoll**:

   a. Navigieren Sie zum Abschnitt **C&C-Callbacks**.

   b. Wählen Sie **Benachrichtigung über NT-Ereignisprotokoll aktivieren**.

   c. übernehmen Sie die Standardmeldung oder ändern Sie sie. Sie können Token-Variablen als Platzhalter für Daten im Feld **Nachricht** verwenden. Weitere Informationen finden Sie unter *Tabelle 12-6: Token-Variablen für C&C-Callback-Ausbruchsbenachrichtigungen auf Seite 12-22*.

6. Klicken Sie auf **Speichern**.

Protokolle für Internet-Bedrohungen

Konfigurieren Sie interne und externe agents so, dass sie Web-Reputation-Protokolle an den Server senden. Dadurch können Sie die von OfficeScan gesperrten URLs analysieren und bei als sicher eingestuften URLs eine entsprechende Aktion durchführen.

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell, oder konfigurieren Sie eine zeitgesteuerte Löschung der Protokolle. Weitere Informationen zur Protokollverwaltung finden Sie unter *Protokollmanagement auf Seite 14-47*.

Web-Reputation-Protokolle anzeigen

Prozedur

1. Navigieren Sie zu einer der folgenden Optionen:

   - **Protokolle** > **Agents** > **Sicherheitsrisiken**
   - **Agents** > **Agent-Verwaltung**

2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.

3. Navigieren Sie zum Fenster **Kriterien für das Web-Reputation-Protokoll**:

   - Klicken Sie im Fenster **Sicherheitsrisiko-Protokolle** auf **Protokolle anzeigen** > **Web-Reputation-Protokolle**.
   - Klicken Sie im Fenster **Agent-Verwaltung** auf **Protokolle** > **Web-Reputation-Protokolle**.

4. Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.

5. Sehen Sie die Protokolle ein. Die Protokolle enthalten die folgenden Informationen:

VORGANG	BESCHREIBUNG
Datum/Uhrzeit	Zeitpunkt der Erkennung
Endpunkt	Endpunkt, auf dem die Erkennung erfolgte
Domäne	Domäne des Endpunkts, auf dem die Erkennung erfolgte
URL	Durch Web-Reputation-Dienste gesperrte URL
Risikostufe	Risikostufe der URL
Beschreibung	Beschreibung der Sicherheitsbedrohung
Prozess	Prozess, über den die Kontaktaufnahme versucht wurde (Pfad\Anwendungsname)
Aktion	Hinsichtlich der Erkennung ergriffene Aktion

6. Klicken Sie auf **Zur Liste der zulässigen Programme hinzufügen**, um der Liste der genehmigten URLs die URLs hinzuzufügen, die nicht gesperrt werden sollen.

7. Wenn Sie Protokolle als kommagetrennte Datei (`CSV-Datei`) speichern möchten, klicken Sie auf **Alle in CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

C&C Callback-Protokolle anzeigen

Prozedur

1. Navigieren Sie zu einer der folgenden Optionen:
   - **Protokolle** > **Agents** > **Sicherheitsrisiken**
   - **Agents** > **Agent-Verwaltung**
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Navigieren Sie zum Fenster **C&C-Callback-Protokollkriterien**:
   - Klicken Sie im Fenster **Sicherheitsrisiko-Protokolle** auf **Protokolle anzeigen** > **C&C-Callback-Protokolle**.
   - Klicken Sie im Fenster **Agent-Verwaltung** auf **Protokolle** > **C&C-Callback-Protokolle**.
4. Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.
5. Sehen Sie die Protokolle ein. Die Protokolle enthalten die folgenden Informationen:

VORGANG	BESCHREIBUNG
Datum/Uhrzeit	Zeitpunkt der Erkennung
Benutzer	Benutzer, der zum Zeitpunkt der Erkennung angemeldet ist
Infizierter Host	Endpunkt, von dem der Callback stammt
IP-Adresse	IP-Adresse des infizierten Hosts
Domäne	Domäne des Endpunkts, auf dem die Erkennung erfolgte
Callback-Adresse	Adresse, an die der Endpunkt den Callback gesendet hat

VORGANG	BESCHREIBUNG
C&C-Listenquelle	Die C&C-Listenquelle, die den C&C-Server identifiziert hat
C&C-Risikostufe	Die Risikostufe des C&C-Servers
Protokoll	Für die übertragung verwendetes Internetprotokoll
Prozess	Prozess, der die übertragung gestartet hat (Pfad \Anwendungsname)
Aktion	Hinsichtlich der Erkennung ergriffene Aktion

6. Wenn Web Reputation eine URL gesperrt hat, die nicht gesperrt werden soll, klicken Sie auf die Schaltfläche **URL zur Liste der zulässigen Web-Reputation-URLs hinzufügen**, um die Adresse zur Liste der zulässigen Web-Reputation-URLs hinzuzufügen.

Hinweis

OfficeScan kann URLs nur zur Liste der zulässigen Web-Reputation-URLs hinzufügen. Für Erkennungen durch die globale C&C-IP-Liste oder die C&C-Liste für Virtual Analyzer (IP) fügen Sie diese IP-Adressen manuell zur Benutzerdefinierten C&C-Liste mit zulässigen IP-Adressen hinzu.

Weitere Informationen finden Sie unter *Globale Einstellungen für die benutzerdefinierte IP-Liste konfigurieren auf Seite 8-7*.

7. Wenn Sie Protokolle als kommagetrennte Datei (`CSV-Datei`) speichern möchten, klicken Sie auf **Alle in CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Kapitel 13

Die OfficeScan Firewall verwenden

In diesem Kapitel werden die Funktionen und die Konfiguration der OfficeScan Firewall beschrieben.

Es werden folgende Themen behandelt:

- *Die OfficeScan Firewall auf Seite 13-2*
- *Die OfficeScan Firewall aktivieren oder deaktivieren auf Seite 13-6*
- *Firewall-Richtlinien und -Profile auf Seite 13-8*
- *Firewall-Berechtigungen auf Seite 13-26*
- *Allgemeine Firewall-Einstellungen auf Seite 13-28*
- *Benachrichtigungen bei Firewall-Verstößen für OfficeScan Agent-Benutzer auf Seite 13-31*
- *Firewall-Protokolle auf Seite 13-32*
- *Ausbrüche bei Firewall-Verstoß auf Seite 13-34*
- *Die OfficeScan Firewall testen auf Seite 13-36*

Die OfficeScan Firewall

Die OfficeScan Firewall schützt OfficeScan Agents und Server im Netzwerk mit Hilfe von Stateful-Inspection-Technologie und leistungsstarken Funktionen zur Virensuche. über die zentrale Management-Konsole können Regeln zum Filtern von Verbindungen nach Anwendung, IP-Adresse, Portnummer oder Protokoll erstellt und dann auf verschiedene Benutzergruppen angewendet werden.

Hinweis

Die OfficeScan Firewall kann auf Endpunkten unter Windows XP, auf denen auch die Windows Firewall aktiviert ist, aktiviert, konfiguriert und verwendet werden. Es dürfen keine widersprüchlichen Firewall-Richtlinien erstellt werden, da dies zu unerwünschten Ergebnissen führen kann. Einzelheiten zur Windows Firewall finden Sie in der Dokumentation von Microsoft.

Die OfficeScan Firewall umfasst die folgenden Funktionen und bietet die folgenden Vorteile:

- *Den Datenverkehr filtern auf Seite 13-2*
- *Anwendungsfilter auf Seite 13-3*
- *Certified Safe Software Liste auf Seite 13-3*
- *Suche nach Netzwerkviren auf Seite 13-3*
- *Profile und Richtlinien benutzerdefiniert anpassen auf Seite 13-4*
- *Stateful Inspection auf Seite 13-4*
- *Intrusion Detection System auf Seite 13-4*
- *Firewall-Verstoß-Ausbruchsmonitor auf Seite 13-6*
- *OfficeScan Agent Firewall-Berechtigungen auf Seite 13-6*

Den Datenverkehr filtern

Die OfficeScan Firewall filtert den gesamten ein- und ausgehenden Datenverkehr und sperrt bestimmte Arten von Datenverkehr anhand folgender Kriterien:

- Richtung (eingehend/ausgehend)
- Protokoll (TCP/UDP/ICMP/ICMPv6)
- Zielports
- Quell- und Zielendpunkte

Anwendungsfilter

Die OfficeScan Firewall filtert den ein- und ausgehenden Datenverkehr für Anwendungen, die in der Ausnahmeliste der Firewall angegeben sind, so dass diese Anwendungen auf das Netzwerk zugreifen können. Die Verfügbarkeit der Netzwerkverbindungen hängt von den vom Administrator festgelegten Richtlinien ab.

Certified Safe Software Liste

Bei der lokalen Certified Safe Software Liste handelt es sich um eine Liste der Anwendungen, die die Sicherheitsebenen der Firewall-Richtlinie umgehen können. Die OfficeScan Firewall lässt automatisch die Ausführung von Anwendungen zu, die in der Certified Safe Software Liste enthalten sind, und gestattet ihnen den Zugriff auf das Netzwerk.

Sie können auch OfficeScan Agents gestatten, die auf Trend Micro Servern gehostete dynamisch aktualisierte globale Certified Safe Software Liste abzufragen.

Wichtig

Für die Abfrage der globalen Certified Safe Software List ist es erforderlich, dass Sie sowohl den Unauthorized Change Prevention Service als auch den Certified Safe Software Service aktivieren.

Suche nach Netzwerkviren

Die OfficeScan Firewall untersucht außerdem jedes Paket auf Netzwerkviren. Weitere Informationen finden Sie unter *Viren und Malware auf Seite 7-2*.

Profile und Richtlinien benutzerdefiniert anpassen

Mit der OfficeScan Firewall können Sie Richtlinien konfigurieren und bestimmte Typen von Netzwerkdatenverkehr sperren oder zulassen. Weisen Sie eine Richtlinie einem oder mehreren Profilen zu, die Sie dann auf ausgewählte OfficeScan Agents verteilen und installieren können. Die Firewall-Einstellungen für agents können dadurch völlig individuell organisiert und konfiguriert werden.

Stateful Inspection

Die OfficeScan Firewall verwendet Stateful Inspection, um alle Verbindungen und Verbindungsstatus für den OfficeScan Agent zu überwachen und zu speichern. Die OfficeScan Firewall kann bestimmte Bedingungen in den Verbindungen ermitteln, zu ergreifende Maßnahmen vorschlagen und Störungen bei normalen Verbindungen erkennen. 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.

Intrusion Detection System

Das Intrusion Detection System (IDS) kann bestimmte Muster in Netzwerkpaketen erkennen, die möglicherweise auf einen Angriff auf dem OfficeScan Agent 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.

Intrusion	Beschreibung
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.
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.

INTRUSION	BESCHREIBUNG
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.

Firewall-Verstoß-Ausbruchsmonitor

Überschreiten die Verstöße gegen die Firewall einen bestimmten Schwellenwert (dies könnte auf einen Angriff hindeuten), sendet die OfficeScan Firewall eine benutzerdefinierte Benachrichtigung an ausgewählte Empfänger.

OfficeScan Agent Firewall-Berechtigungen

OfficeScan Agent-Benutzer können dazu berechtigt werden, ihre Firewall-Einstellungen auf der OfficeScan Agent-Konsole anzuzeigen. die Firewall, das Intrusion Detection System und die Warnmeldung der Firewall zu aktivieren oder deaktivieren.

Die OfficeScan Firewall aktivieren oder deaktivieren

Bei der Installation von OfficeScan Server werden Sie aufgefordert, die OfficeScan Firewall zu aktivieren oder zu deaktivieren.

Wenn Sie die Firewall bei der Installation aktiviert und insbesondere auf Server-Plattformen (Windows Server 2003, Windows Server 2008 und Windows Server 2012) eine Leistungsbeeinträchtigung festgestellt haben, sollten Sie die Firewall eventuell deaktivieren.

Wenn Sie die Firewall bei der Installation deaktiviert haben, sie aber jetzt aktivieren möchten, um den agent vor Angriffen zu schützen, lesen Sie zuerst die Richtlinien und Anweisungen unter *OfficeScan Agent Dienste auf Seite 15-7*.

Sie können die Firewall auf allen oder auf ausgewählten OfficeScan Agent-Endpunkten aktivieren bzw. deaktivieren.

Aktivieren oder Deaktivieren der OfficeScan Firewall auf ausgewählten Endpunkten

Verwenden Sie eine der folgenden Methoden, um die Firewall in der Webkonsole zu aktivieren bzw. zu deaktivieren.

METHODE	VERFAHREN
Erstellen Sie eine neue Richtlinie und wenden Sie diese auf die OfficeScan Agents an.	1. Erstellen Sie eine neue Richtlinie, um die Firewall zu aktivieren/deaktivieren. Die Schritte für das Erstellen einer neuen Richtlinie finden Sie unter *Firewall-Richtlinie hinzufügen auf Seite 13-11*. 2. Wenden Sie die Richtlinie auf die OfficeScan Agents an.
Aktivieren/ Deaktivieren Sie den Firewall-Dienst über die Webkonsole	Weitere Informationen über die einzelnen Schritte finden Sie unter *OfficeScan Agent Dienste auf Seite 15-7*. **Hinweis** Beim automatischen Deaktivieren des Firewall-Diensts werden alle Firewall-Richtlinien auf den ausgewählten Agents deaktiviert.

Verwenden Sie eine der folgenden Methoden, um die Firewall auf ausgewählten Endpunkten zu aktivieren bzw. zu deaktivieren.

METHODE	VERFAHREN
Den Firewall-Treiber aktivieren/ deaktivieren	1. Öffnen Sie die **Windows Netzwerkverbindungseigenschaften**. 2. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Trend Micro Treiber für die allgemeine Firewall** über die Netzwerkkarte.

METHODE	VERFAHREN
Den Firewall-Dienst aktivieren/ deaktivieren	1. Öffnen Sie ein Befehlszeilenfenster, und geben Sie `services.msc` ein. 2. Starten oder stoppen Sie die **OfficeScan NT Firewall** über die Microsoft Management-Konsole (MMC).

Die OfficeScan Firewall auf allen Endpunkten aktivieren bzw. deaktivieren

Prozedur

1. Navigieren Sie zu **Administration** > **Einstellungen** > **Produktlizenz**.
2. Gehen Sie zum Abschnitt **Zusätzliche Dienste**.
3. Klicken Sie im Abschnitt **Zusätzliche Dienste** in der Zeile **Firewall für Endpunkte** auf **Aktiviert** oder **Deaktiviert**.

Firewall-Richtlinien und -Profile

Mit Richtlinien und Profilen erstellt die OfficeScan Firewall individuelle Schutzmaßnahmen für vernetzte Endpunkte.

Durch die Active Directory-Integration und die rollenbasierte Administration kann jede Benutzerrolle, abhängig von der Berechtigung, spezifische Richtlinien und Profile für ihre Domänen entweder erstellen, konfigurieren oder löschen.

Tipp

Mehrere Firewalls auf demselben Endpunkt können unerwünschte Folgen haben. Unter Umständen ist es ratsam, vor der Installation und Aktivierung der OfficeScan Agents Firewall andere auf OfficeScan installierte, softwarebasierte Firewall-Anwendungen zu deinstallieren.

Die folgenden Schritte sind zum erfolgreichen Einsatz der OfficeScan Firewall erforderlich:

1. Erstellen Sie eine Richtlinie. Über eine Richtlinie können Sie die Sicherheitsstufe festlegen, die den Datenverkehr auf Netzwerk-Endpunkten sperrt bzw. zulässt und die Firewall-Funktionen aktiviert.

2. Ausnahmen zur Richtlinie hinzufügen: OfficeScan Agents können in bestimmten Fällen von der Richtlinie abweichen. In den Ausnahmen können Sie agents angeben und bestimmte Arten von Datenverkehr sperren bzw. zulassen, wobei die Sicherheitsstufe der Richtlinie außer Acht gelassen wird. Sie können zum Beispiel den gesamten Datenverkehr für eine Reihe von agents sperren, aber gleichzeitig eine Ausnahme erstellen, die HTTP-Datenverkehr zulässt, damit die agents auf einen bestimmten Webserver zugreifen können.

3. Profile erstellen und den OfficeScan Agents zuweisen: Ein Firewall-Profil beinhaltet einen Satz agent-Attribute und ist mit einer Richtlinie verbunden. Wenn ein agent mit den im Profil festgelegten Attributen übereinstimmt, tritt die entsprechende Richtlinie in Kraft.

Firewall-Richtlinien

Mit Hilfe von OfficeScan Firewall-Richtlinien können Sie bestimmte Arten von Netzwerkdatenverkehr sperren oder zulassen, die nicht in einer Richtlinienausnahme angegeben sind. Eine Richtlinie definiert auch, welche Firewall-Funktionen aktiviert oder deaktiviert werden. Ordnen Sie eine Richtlinie einem oder mehreren Firewall-Profilen zu.

Durch die Active Directory-Integration und die rollenbasierte Administration kann jede Benutzerrolle, abhängig von der Berechtigung, spezifische Richtlinien für ihre Domänen entweder erstellen, konfigurieren oder löschen.

In der folgenden Tabelle werden die Einstellungen erläutert, die beim Konfigurieren einer Firewall-Richtlinie zur Verfügung stehen.

EINSTELLUNGEN	BESCHREIBUNG
Sicherheitsstufe	Eine allgemeine Einstellung, mit der der gesamte ein- und/oder ausgehende Datenverkehr auf dem OfficeScan Agent gesperrt oder zugelassen wird. Endpunkt
Firewall-Funktionen	Geben Sie an, ob Sie die OfficeScan Firewall, das Intrusion Detection System (IDS) und die Benachrichtigung bei Firewall-Verstoß aktivieren bzw. deaktivieren möchten. Weitere Informationen finden Sie unter *Intrusion Detection System auf Seite 13-4*.
Certified Safe Software Liste	Geben Sie an, ob die Anwendungen auf der Certified Safe Liste eine Verbindung zum Netzwerk aufbauen dürfen. Weitere Informationen finden Sie unter *Certified Safe Software Liste auf Seite 13-3*.
Liste der Richtlinienausnahmen	Eine Liste mit konfigurierbaren Ausnahmen zum Sperren oder Zulassen unterschiedlicher Arten von Netzwerkdatenverkehr

Hinweis

Sie können Endbenutzern die Berechtigung erteilen, die Sicherheitsstufe sowie die Liste der Richtlinienausnahmen beim Erstellen von Firewall-Profilen zu ändern.

Weitere Informationen finden Sie unter *Firewall-Profil hinzufügen auf Seite 13-23*.

Standard-Firewall-Richtlinien

OfficeScan wird mit mehreren Standardrichtlinien ausgeliefert, die Sie ändern oder löschen können.

Name der Richtlinie	Sicherheitsstufe	Agent Einstellungen	Ausnahmen	Empfohlene Verwendung
Uneingeschränkter Zugriff	Niedrig	Firewall aktivieren	Keine	agents uneingeschränkten Netzwerkzugriff gewähren
Kommunikationsports für Trend Micro Control Manager	Niedrig	Firewall aktivieren	Gesamten ein- und ausgehenden TCP/UDP-Datenverkehr durch die Ports 80 und 10319 zulassen	Für agents mit MCP Agent
ScanMail for Microsoft Exchange Konsole	Niedrig	Firewall aktivieren	Gesamten eingehenden und ausgehenden TCP-Datenverkehr über Port 16372 zulassen	Für agents, die Zugriff auf die ScanMail Konsole benötigen
InterScan Messaging Security Suite (IMSS) Konsole	Niedrig	Firewall aktivieren	Gesamten eingehenden und ausgehenden TCP-Datenverkehr über Port 80 zulassen	Für agents, die Zugriff auf die IMSS Konsole benötigen

Firewall-Richtlinie hinzufügen

Prozedur

1. Navigieren Sie zu **Agents** > **Firewall** > **-Richtlinien**.
2. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie hinzuzufügen.

   Wenn Sie eine Richtlinie erstellen möchten, die ähnliche Einstellungen wie eine vorhandene Richtlinie hat, wählen Sie die vorhandene Richtlinie, und klicken Sie auf **Kopieren**.
3. Geben Sie einen Namen für die Richtlinie ein.
4. Wählen Sie eine Sicherheitsstufe aus.

Die ausgewählte Sicherheitsstufe wird nicht auf Datenverkehr angewendet, der den Ausnahmekriterien der Firewall-Richtlinie entspricht.

5. Wählen Sie die für die Richtlinie zu verwendenden Firewall-Funktionen aus.

   - Die Benachrichtigung bei Firewall-Verstoß wird angezeigt, wenn die Firewall ein ausgehendes Paket sperrt. Informationen zur Anpassung der Meldung finden Sie unter *Den Inhalt der Firewall-Benachrichtigung ändern auf Seite 13-32*.
   - Wenn der Administrator alle Firewall-Funktionen aktiviert und OfficeScan Agent-Benutzern die Berechtigung erteilt, Firewall-Einstellungen zu konfigurieren, können Benutzer die Funktionen aktivieren/deaktivieren und Firewall-Einstellungen in der OfficeScan Agent-Konsole ändern.

     Warnung!

     Sie können die OfficeScan-Webkonsole nicht zum Überschreiben der vom Benutzer vorgenommenen Einstellungen für die OfficeScan Agent-Konsole verwenden.

   - Wenn Sie die Funktionen nicht aktivieren, werden die über die Webkonsole von OfficeScan vorgenommenen Firewall-Einstellungen unter **Liste der Netzwerkkarten** auf der OfficeScan Agent-Konsole angezeigt.
   - Die Informationen unter **Einstellungen** auf der Registerkarte **Firewall** der OfficeScan Agent-Konsole entsprechen immer den Einstellungen, die über die OfficeScan Agent-Konsole konfiguriert wurden, und nicht denen, die über die Webkonsole des Servers vorgenommen wurden.

6. Aktivieren Sie die lokale oder globale Certified Safe Software Liste.

   Hinweis

   Stellen Sie sicher, dass die Dienste "Trend Micro Unauthorized Change Prevention Service" und "Certified Safe Software Services" aktiviert wurden, bevor Sie diesen Service aktivieren.

7. Wählen Sie unter "Ausnahme" die Richtlinienausnahmen für die Firewall aus. Die hier aufgeführten Richtlinienausnahmen hängen von der Ausnahmevorlage der Firewall ab. Weitere Informationen finden Sie unter *Die Ausnahmevorlage der Firewall bearbeiten auf Seite 13-14*.

- Sie können eine bestehende Richtlinienausnahme ändern, indem Sie auf ihren Namen klicken und die Einstellungen im daraufhin angezeigten Fenster ändern.

Hinweis

Die geänderte Richtlinienausnahme wird nur auf die zu erstellende Richtlinie angewendet. Wenn die Änderung der Richtlinienausnahme dauerhaft sein soll, müssen Sie dieselbe Änderung an der Richtlinienausnahme in der Vorlage der Firewall-Ausnahme vornehmen.

- Klicken Sie auf **Hinzufügen**, um eine neue Richtlinienausnahme zu erstellen. Geben Sie im daraufhin angezeigten Fenster die entsprechenden Einstellungen ein.

Hinweis

Die Richtlinienausnahme wird auch nur auf die zu erstellende Richtlinie angewendet. Um diese Richtlinienausnahme auch auf andere Richtlinien anzuwenden, müssen Sie sie zunächst zur Liste der Richtlinienausnahmen in der Ausnahmevorlage der Firewall hinzufügen.

8. Klicken Sie auf **Speichern**.

Eine vorhandene Firewall-Richtlinie ändern

Prozedur

1. Navigieren Sie zu **Agents** > **Firewall** > **-Richtlinien**.
2. Klicken Sie auf eine Richtlinie.
3. Ändern Sie Folgendes:
   - Name der Richtlinie
   - Sicherheitsstufe
   - Die Funktionen dieser Firewall-Richtlinie

- Status der Certified Safe Software Service List
- Die Ausnahmen dieser Firewall-Richtlinie
    - Bearbeiten Sie eine bestehende Richtlinienausnahme (klicken Sie auf den Namen der Richtlinienausnahme und ändern Sie im daraufhin angezeigten Fenster die Einstellungen.)
    - Klicken Sie auf **Hinzufügen**, um eine neue Richtlinienausnahme zu erstellen. Geben Sie im daraufhin angezeigten Fenster die entsprechenden Einstellungen ein.

4. Klicken Sie auf **Speichern**, um die Änderungen für die bestehende Richtlinie zu übernehmen.

Die Ausnahmevorlage der Firewall bearbeiten

Über die Ausnahmevorlage der Firewall können Sie die Richtlinien so konfigurieren, dass anhand von Portnummer(n) und IP-Adresse(n) der OfficeScan Agent-Endpunkte verschiedene Arten von Netzwerkdatenverkehr gesperrt bzw. zugelassen werden. Erstellen Sie eine Richtlinienausnahme, und bearbeiten Sie dann die Richtlinien, für die diese Ausnahme gelten soll.

Wählen Sie zunächst die Art der Ausnahme. Es gibt zwei Möglichkeiten:

- **Einschränkend**

  Mit diesen Ausnahmen werden nur bestimmte Arten von Netzwerkdatenverkehr gesperrt. Sie werden auf Richtlinien angewendet, die den gesamten Netzwerkverkehr zulassen. Eine einschränkende Richtlinienausnahme wird beispielsweise verwendet, um anfällige OfficeScan Agent-Ports zu sperren, wie z. B. Ports, die häufig von Trojanern benutzt werden.

- **Zulassend**

  Mit diesen Ausnahmen werden nur bestimmte Arten von Netzwerkdatenverkehr zugelassen. Sie werden auf Richtlinien angewendet, die den gesamten Netzwerkverkehr sperren. Sie können den OfficeScan Agents zum Beispiel nur Zugriff auf den OfficeScan Server und einen Webserver gewähren. Lassen Sie hierfür den Datenverkehr vom vertrauenswürdigen Port (der für die

Kommunikation mit dem OfficeScan Server verwendet wird) und dem Port, den der OfficeScan Agent für die HTTP-Kommunikation verwendet, zu.

OfficeScan Agent-Listening-Port **Agents** > **Agent-Verwaltung > Status**. Die Portnummer finden Sie unter **Allgemeine Informationen**.

Server-Listening-Port: **Administration** > **Einstellungen** > **Agent-Verbindung**. Die Portnummer finden Sie unter **Agent-Verbindungseinstellungen**.

OfficeScan wird mit mehreren Standardausnahmen für Firewall-Richtlinien ausgeliefert, die Sie ändern oder löschen können.

TABELLE 13-1. Standardausnahmen für Firewall-Richtlinien

NAME DER AUSNAHME	AKTION	PROTOKOLL	PORT	RICHTUNG
DNS	Zulassen	TCP/UDP	53	Eingehend und ausgehend
NetBIOS	Zulassen	TCP/UDP	137, 138, 139, 445	Eingehend und ausgehend
HTTPS	Zulassen	TCP	443	Eingehend und ausgehend
HTTP	Zulassen	TCP	80	Eingehend und ausgehend
Telnet	Zulassen	TCP	23	Eingehend und ausgehend
SMTP	Zulassen	TCP	25	Eingehend und ausgehend
FTP	Zulassen	TCP	21	Eingehend und ausgehend
POP3	Zulassen	TCP	110	Eingehend und ausgehend
LDAP	Zulassen	TCP/UDP	389	Eingehend und ausgehend

Hinweis

Standardausnahmen gelten für alle agents. Wenn eine Standardausnahme nur für bestimmte agents gelten soll, bearbeiten Sie die Ausnahme, und geben Sie die IP-Adressen der agents an.

Die LDAP-Ausnahme steht nicht zur Verfügung, wenn Sie ein Upgrade von einer früheren OfficeScan Version durchgeführt haben. Fügen Sie diese Ausnahme manuell hinzu, wenn sie nicht in der Ausschlussliste angezeigt wird.

Ausnahme der Firewall-Richtlinie hinzufügen

Wenn Sie neue Ausnahmen hinzufügen, müssen Sie sicherstellen, dass die für die Kommunikation zwischen dem OfficeScan Server und den OfficeScan Agents verwendeten Ports nicht gesperrt sind.

Sie können die vom OfficeScan Server und den OfficeScan Agents verwendeten Listening-Ports wie folgt verwenden:

- Server-Listening-Port: Navigieren Sie zu **Administration** > **Einstellungen** > **Agent-Verbindung**. Die Portnummer finden Sie unter **Agent-Verbindungseinstellungen**.
- OfficeScan Agent-Listening-Port: Navigieren Sie zu **Agents** > **Agent-Verwaltung** > **Status**. Die Portnummer finden Sie unter **Allgemeine Informationen**.

Prozedur

1. Navigieren Sie zu **Agents** > **Firewall** > **-Richtlinien**.
2. Klicken Sie auf **Ausnahmevorlage bearbeiten**.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie einen Namen für die Richtlinienausnahme ein.
5. Wählen Sie den Typ der Anwendung. Sie können alle Anwendungen auswählen oder einen Anwendungspfad oder Registrierungsschlüssel angeben.

Hinweis

überprüfen Sie den eingegebenen Namen und den vollständigen Pfad. Die Anwendungsausnahme unterstützt keine Platzhalterzeichen.

6. Wählen Sie die Aktion, die OfficeScan für Netzwerkdatenverkehr ausführt (Datenverkehr, der die Ausnahmekriterien erfüllt, kann gesperrt oder zugelassen werden), und die Richtung des Datenverkehrs (eingehender oder ausgehender Netzwerkdatenverkehr auf dem OfficeScan Agent-Endpunkt).

7. Wählen Sie die Art des Netzwerkprotokolls aus: TCP, UDP, ICMP oder ICMPv6.

8. Geben Sie die Ports auf dem OfficeScan Agent-Endpunkt an, auf dem die Aktion durchgeführt werden soll.

9. Wählen Sie die IP-Adressen des OfficeScan Agent-Endpunkts aus, die in die Ausnahmen einbezogen werden sollen.

   Wenn Sie beispielsweise sämtlichen Netzwerkdatenverkehr (eingehend und ausgehend) ablehnen und die IP-Adresse für einen einzelnen Endpunkt im Netzwerk eingeben, kann kein OfficeScan Agent, dessen Richtlinie diese Ausnahme enthält, Daten an diese IP-Adresse senden oder von dieser Adresse empfangen.

   - **Alle IP-Adressen**: Schließt alle IP-Adressen ein.
   - **Einzelne IP-Adresse**: Geben Sie eine IPv4- oder eine IPv6-Adresse oder einen Host-Namen ein.
   - **Bereich (für IPv4 oder IPv6)**: Geben Sie einen IPv4- oder einen IPv6-Adressbereich ein.
   - **Bereich (für IPv6)**: Geben Sie ein IPv6-Adresspräfix und eine Länge ein.
   - **Subnetzmaske**: Geben Sie eine IPv4-Adresse und die jeweilige Subnetzmaske ein.

10. Klicken Sie auf **Speichern**.

    Das Fenster **Ausnahmevorlage bearbeiten** wird mit der neuen Ausnahme angezeigt.

11. Klicken Sie auf eine der folgenden Schaltflächen, um die neue Ausnahme auf die Liste anzuwenden:

    - **Vorlageänderungen speichern**: Speichert die aktuellen Einstellungen der Ausnahmevorlagenliste, wobei die Einstellungen jedoch nicht auf vorhandene Richtlinien angewendet werden.
    - **Speichern und für alle vorhandenen Richtlinien übernehmen**: Speichert die aktuellen Einstellungen der Ausnahmevorlagenliste und wendet die Einstellungen unmittelbar auf alle vorhandenen Richtlinien an.

Ausnahme der Firewall-Richtlinie ändern

Prozedur

1. Navigieren Sie zu **Agents** > **Firewall** > **-Richtlinien**.
2. Klicken Sie auf **Ausnahmevorlage bearbeiten**.
3. Klicken Sie auf eine Richtlinienausnahme.
4. Ändern Sie Folgendes:
    - Name der Richtlinienausnahme
    - Anwendungstyp, Name oder Pfad
    - Aktion, die OfficeScan bei Netzwerkdatenverkehr und Verkehrsrichtung durchführt
    - Art des Netzwerkprotokolls
    - Portnummern der Richtlinienausnahme
    - OfficeScan Agent Endpunkt-IP-Adressen
5. Klicken Sie auf **Speichern**.

Einstellungen zur Liste der Richtlinienausnahmen speichern

Prozedur

1. Navigieren Sie zu **Agents** > **Firewall** > **-Richtlinien**.
2. Klicken Sie auf **Ausnahmevorlage bearbeiten**.
3. Klicken Sie auf eine der folgenden Speicheroptionen:
   - **Vorlageänderungen speichern**: Speichert die Ausnahmevorlage mit den aktuellen Richtlinienausnahmen und Einstellungen. Mit dieser Option gilt die Vorlage nur für zukünftige, nicht aber für bereits vorhandene Richtlinien.
   - **Speichern und für alle vorhandenen Richtlinien übernehmen**: Speichert die Ausnahmevorlage mit den aktuellen Richtlinienausnahmen und Einstellungen. Mit dieser Option gilt die Vorlage für bereits vorhandene und zukünftige Richtlinien.

Firewall-Profile

Mit Firewall-Profilen können Sie außerdem überprüfen, ob einzelne Agents oder Agent-Gruppen bestimmte Attribute aufweisen, bevor eine Richtlinie angewendet wird. Sie können Benutzerrollen erstellen, die Profile für spezifische Domänen erstellen, konfigurieren oder löschen können.

Benutzer, die das integrierte Administratorkonto verwenden, oder Benutzer mit vollständigen Management-Berechtigungen können ebenfalls die Option **Agent-Sicherheitsstufe/-Ausnahmeliste überschreiben** aktivieren, um die OfficeScan Agent-Profileinstellungen durch die Server-Einstellungen zu ersetzen.

Die Profile umfassen:

- **Verknüpfte Richtlinie**:Jedes Profil verwendet genau eine Richtlinie.
- **Agent-Attribute**: OfficeScan Agents mit einem oder mehreren der folgenden Attribute wenden die verbundene Richtlinie an:

- **IP-Adresse**: Ein OfficeScan Agent mit einer bestimmten IP-Adresse, einer IP-Adresse in einem bestimmten Bereich oder einer IP-Adresse in einem bestimmten Subnetz
- **Domäne**: Ein OfficeScan Agent, der zu einer bestimmten OfficeScan Domäne gehört
- **Endpunkt**: Der OfficeScan Agent mit einem bestimmten Endpunktnamen
- **Plattform**: Ein OfficeScan Agent, der auf einem bestimmten Plattformtyp ausgeführt wird
- **Anmeldename**: OfficeScan Agent Endpunkte, an denen bestimmte Benutzer angemeldet sind
- **NIC-Beschreibung**: Ein OfficeScan Agent-Endpunkt mit einer übereinstimmenden NIC-Beschreibung
- **Agent-Standort**: Ob der OfficeScan Agent online oder offline ist

Hinweis

Der OfficeScan Agent gilt als online, wenn er eine Verbindung zum OfficeScan Server oder einem der Referenzserver aufbauen kann. Er gilt als offline, wenn keine Verbindung mit einem Server möglich ist.

OfficeScan wird mit einem Standardprofil mit der Bezeichnung "Alle Agents" ausgeliefert, das die Richtlinie "Uneingeschränkter Zugriff" verwendet. Sie können dieses Standardprofil ändern oder löschen. Sie können auch neue Profile erstellen. Alle Standard- und benutzerdefinierten Firewall-Profile, einschließlich der Richtlinie, die jedem Profil zugeordnet ist, und der aktuelle Profilstatus werden in der Liste der Firewall-Profile auf der Webkonsole angezeigt. Sie können die Profilliste verwalten und alle Profile an die OfficeScan Agents verteilen. OfficeScan Agents speichern alle Firewall-Profile auf dem Agent-Endpunkt.

Die Profilliste der Firewall konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Firewall** > **Profile**.
2. Aktivieren Sie wahlweise für Benutzer, die das integrierte Administratorkonto verwenden, oder für Benutzer mit vollständigen Management-Berechtigungen die Option **Agent-Sicherheitsstufe/-Ausnahmeliste überschreiben**, um die OfficeScan Agent-Profileinstellungen durch die Server-Einstellungen zu ersetzen.
3. Klicken Sie auf **Hinzufügen**, um ein neues Profil hinzuzufügen. Um ein bestehendes Profil zu bearbeiten, wählen Sie den Namen des Profils.

   Ein Fenster zur Konfiguration des Profils wird angezeigt. Weitere Informationen finden Sie unter *Ein Firewall-Profil hinzufügen oder bearbeiten auf Seite 13-23*.
4. Zum Löschen eines vorhandenen Profils aktivieren Sie das Kontrollkästchen neben der betreffenden Richtlinie und klicken auf **Löschen**.
5. Um die Reihenfolge der Profile in der Liste zu ändern, aktivieren Sie das Kontrollkästchen neben dem Profil, das verschoben werden soll, und klicken Sie anschließend auf **Nach oben** oder **Nach unten**.

   OfficeScan wendet die Firewall-Profile in der Reihenfolge auf die OfficeScan Agents an, in der sie in der Liste erscheinen. Wenn der Agent zum Beispiel dem ersten Profil entspricht, wendet OfficeScan die für dieses Profil konfigurierten Maßnahmen auf den Agent an. OfficeScan ignoriert die anderen für diesen Agent konfigurierten Profile.

   Tipp

   Je ausschließender eine Richtlinie ist, desto weiter oben sollte sie in der Liste stehen. Setzen Sie zum Beispiel die Richtlinien für einen einzigen Agent ganz nach oben, gefolgt von den Richtlinien für eine bestimmte Gruppe von Agents, eine Netzwerkdomäne und alle Agents.
6. Um die Referenzserver zu verwalten, klicken Sie auf **Liste der Referenzserver bearbeiten**. Bei den Referenzservern handelt es sich um Endpunkte, die als Ersatz für den OfficeScan Server bei der Anwendung von Firewall-Profilen fungieren.

Jeder beliebige Endpunkt im Netzwerk kann ein Referenzserver sein (weitere Informationen hierzu finden Sie unter *Referenzserver auf Seite 14-40*). Bei der Aktivierung von Referenzservern geht OfficeScan von folgenden Annahmen aus:

- Mit Referenzservern verbundene OfficeScan Agents sind online, auch wenn die Agents nicht mit dem OfficeScan Server kommunizieren können.
- Die Firewall-Profile für Online-OfficeScan Agents gelten auch für OfficeScan Agents, die mit Referenzservern verbunden sind.

Hinweis

Nur Benutzer, die das integrierte Administratorkonto verwenden, oder solche mit vollständigen Management-Berechtigungen können die Liste der Referenzserver anzeigen und konfigurieren.

7. Die aktuellen Einstellungen speichern und die Profile den OfficeScan Agents zuweisen:

   a. Entscheiden Sie, ob Sie die **Agent-Sicherheitsstufe/-Ausnahmeliste überschreiben** möchten. Diese Option überschreibt alle benutzerdefinierten Firewall-Einstellungen.

   b. Klicken Sie auf **Den Agents ein Profil zuweisen**. OfficeScan weist allen OfficeScan Agents alle Profile in der Liste zu.

8. So überprüfen Sie, ob die Profile den OfficeScan Agents zugewiesen wurden

   a. Navigieren Sie zu **Agents** > **Agent-Verwaltung**. Wählen Sie im Auswahlmenü der Agent-Hierarchie die **Firewall-Ansicht**.

   b. Stellen Sie sicher, dass unter die Spalte **Firewall** in der Agent-Hierarchie ein grünes Häkchen gesetzt ist. Wenn die dem Profil zugewiesene Richtlinie das Intrusion Detection System aktiviert, enthält auch die Spalte **IDS** ein grünes Häkchen.

   c. Überprüfen Sie, ob der Agent die richtige Firewall-Richtlinie anwendet. Die Richtlinie wird in der Spalte **Firewall-Richtlinie** in der Agent-Hierarchie angezeigt.

Ein Firewall-Profil hinzufügen oder bearbeiten

OfficeScan Agent Jeder Endpunkte benötigt individuelle Sicherheit. Über die Profile der Firewall können Sie die agent Endpunkte angeben, für die eine entsprechende Richtlinie übernommen wird. Im Allgemeinen ist ein Profil für jede verwendete Richtlinie erforderlich.

Firewall-Profil hinzufügen

Prozedur

1. Navigieren Sie zu **Agents** > **Firewall** > **Profile**.
2. Klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **Dieses Profil aktivieren**, damit OfficeScan das Profil auf OfficeScan Agents verteilen kann.
4. Geben Sie einen Namen und optional eine Beschreibung für das Profil ein.
5. Wählen Sie eine Richtlinie für dieses Profil aus.
6. Legen Sie die Agent-Endpunkte fest, auf die OfficeScan die Richtlinie anwendet. Wählen Sie die Endpunkte anhand der folgenden Kriterien aus:
   - IP-Adresse
   - Domäne: Klicken Sie auf die entsprechende Schaltfläche, um Domänen in der Agent-Hierarchie zu öffnen und auszuwählen.

     Hinweis

     Nur Benutzer mit vollständigen Domänenberechtigungen können Domänen auswählen.

   - Endpunktname: Klicken Sie auf die entsprechende Schaltfläche, um OfficeScan Agent-Endpunkte in der Agent-Hierarchie auszuwählen.
   - Betriebssystem
   - Anmeldename

- NIC-Beschreibung: Geben Sie eine vollständige oder kurze Beschreibung ohne Platzhalter ein.

Tipp

Trend Micro empfiehlt, den Hersteller der Netzwerkkarte einzugeben, da NIC-Beschreibungen gewöhnlich mit dem Herstellernamen beginnen. Wenn Sie beispielsweise "Intel" eingeben, erfüllen alle von Intel hergestellten Netzwerkkarten diese Kriterien. Wenn Sie die Modellbezeichnung einer bestimmten Netzwerkkarte eingegeben haben, beispielsweise "Intel(R) Pro/100", werden nur NIC-Beschreibungen, die mit "Intel(R) Pro/100" beginnen, diese Kriterien erfüllen.

- Agent-Standort: Wählen Sie eine der folgenden Optionen aus:
  - **Intern – OfficeScan Agents können eine Verbindung mit einem konfigurierten Referenzserver herstellen**

Hinweis

Klicken Sie auf **Liste der Referenzserver bearbeiten**, um die Standorteinstellungen zu konfigurieren.

Weitere Informationen finden Sie unter *Referenzserver auf Seite 14-40*.

  - **Extern – OfficeScan Agents können keine Verbindung zu einem konfigurierten Referenzserver herstellen**

7. Geben Sie an, ob Benutzer berechtigt sein sollen, die Sicherheitsstufe der Firewall zu ändern oder eine konfigurierbare Liste mit Ausnahmen zu bearbeiten, um bestimmte Arten von Verkehr zuzulassen.

   Weitere Informationen finden Sie unter *Firewall-Richtlinien auf Seite 13-9*.

8. Klicken Sie auf **Speichern**.

Firewall-Profil ändern

Prozedur

1. Navigieren Sie zu **Agents** > **Firewall** > **Profile**.
2. Klicken Sie auf ein Profil.
3. Klicken Sie auf **Dieses Profil aktivieren**, damit OfficeScan das Profil auf OfficeScan Agents verteilen kann. Ändern Sie Folgendes:
    - Namen und Beschreibung des Profils
    - Dem Profil zugeordnete Richtlinie
    - OfficeScan Agent Endpunkte basierend auf den folgenden Kriterien:
        - IP-Adresse
        - Domäne: Klicken Sie auf die entsprechende Schaltfläche, um die agent-Hierarchie zu öffnen und dort die Domänen auszuwählen.
        - Endpunkt-Name: Klicken Sie auf die entsprechende Schaltfläche, um die agent-Hierarchie zu öffnen und dort die agent-Endpunkte auszuwählen.
        - Betriebssystem
        - Anmeldename
        - NIC-Beschreibung: Geben Sie eine vollständige oder kurze Beschreibung ohne Platzhalter ein.

Tipp

Trend Micro empfiehlt, den Hersteller der Netzwerkkarte einzugeben, da NIC-Beschreibungen gewöhnlich mit dem Herstellernamen beginnen. Wenn Sie beispielsweise "Intel" eingeben, erfüllen alle von Intel hergestellten Netzwerkkarten diese Kriterien. Wenn Sie die Modellbezeichnung einer bestimmten Netzwerkkarte eingegeben haben, beispielsweise "Intel(R) Pro/100", werden nur NIC-Beschreibungen, die mit "Intel(R) Pro/100" beginnen, diese Kriterien erfüllen.

- Verbindungsstatus des Agents

4. Klicken Sie auf **Speichern**.

Firewall-Berechtigungen

Erlauben Sie Benutzern die Konfiguration ihrer eigenen Firewall-Einstellungen. Alle benutzerkonfigurierten Einstellungen können nicht durch Einstellungen überschrieben werden, die vom OfficeScan Server verteilt werden. Wenn der Benutzer beispielsweise das Intrusion Detection System (IDS) deaktiviert hat und Sie IDS auf dem OfficeScan Server aktivieren, bleibt IDS auf dem OfficeScan Agent-Endpunkt deaktiviert.

Aktivieren Sie die folgenden Einstellungen, damit Benutzer die Firewall konfigurieren können.

TABELLE 13-2. Firewall-Berechtigungen

BERECHTIGUNG	BESCHREIBUNG
Firewall-Einstelllungen auf der OfficeScan Agent-Konsole anzeigen	Die Option **Firewall** zeigt alle Firewall-Einstellungen auf dem OfficeScan Agent an.
Clients dürfen Firewall, Intrusion Detection System (IDS) und Warnmeldung der Firewall aktivieren/deaktivieren	Die OfficeScan Firewall schützt Agents und Server im Netzwerk mit Stateful-Inspection-Technologie und leistungsstarkes Suchen und Entfernen von Netzwerkviren. Wenn Sie Benutzern die Berechtigung erteilen, die Firewall und ihre Funktionen zu aktivieren bzw. zu deaktivieren, warnen Sie sie vor der Deaktivierung der Firewall über einen längeren Zeitraum, um zu verhindern, dass die Gefahr von Intrusion- und Hackerangriffen für den Endpunkt entsteht. Wenn Sie den Benutzern die Berechtigungen nicht gewähren, werden die über die Webkonsole des OfficeScan Servers vorgenommenen Firewall-Einstellungen unter "Liste der Netzwerkkarten" auf der OfficeScan Agent-Konsole angezeigt.

BERECHTIGUNG	BESCHREIBUNG
OfficeScan Agents dürfen Firewall-Protokolle an den OfficeScan Server senden	Wählen Sie diese Option, um den Datenverkehr zu analysieren, den die OfficeScan Firewall sperrt und zulässt. Weitere Informationen über Firewall-Protokolle finden Sie unter *Firewall-Protokolle auf Seite 13-32*. Wenn Sie diese Option auswählen, konfigurieren Sie den Zeitplan für das Senden des Protokolls unter **Agents** > **Globale Agent-Einstellungen** auf der Registerkarte **Sicherheitseinstellungen**. Gehen Sie zum Abschnitt **Firewall-Einstellungen**. Der Zeitplan gilt nur für agents mit Berechtigung zum Versenden von Firewall-Protokollen. Anweisungen finden Sie unter *Allgemeine Firewall-Einstellungen auf Seite 13-28*.

Firewall-Berechtigungen gewähren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der agent-Hierarchie auf das Stammsymbol ( ), um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Gehen Sie auf der Registerkarte **Berechtigungen** zum Abschnitt **Firewall-Berechtigungen**.
5. Wählen Sie die folgenden Optionen:
   - *Die Registerkarte 'Firewall' auf der OfficeScan Agent-Konsole anzeigen auf Seite 13-26*
   - *Clients dürfen Firewall, Intrusion Detection System (IDS) und Warnmeldung der Firewall aktivieren/deaktivieren auf Seite 13-26*
   - *OfficeScan Agents dürfen Firewall-Protokolle an den OfficeScan Server senden auf Seite 13-27*

6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Allgemeine Firewall-Einstellungen

Es gibt mehrere Möglichkeiten, die allgemeinen Firewall-Einstellungen auf die OfficeScan Agents anzuwenden.

- Eine bestimmte Firewall-Einstellung kann sich auf alle Agents beziehen, die der Server verwaltet.
- Es gibt aber auch Einstellungen, die sich nur auf OfficeScan Agents mit bestimmten Firewall-Berechtigungen beziehen. Der Zeitplan für das Versenden von Firewall-Protokollen bezieht sich zum Beispiel nur auf OfficeScan Agents mit der Berechtigung zum Versenden von Protokollen an den Server.

Aktivieren Sie bei Bedarf die folgenden allgemeine Einstellungen:

- **Firewall-Protokolle an den Server senden**

  Sie können bestimmten OfficeScan Agents die Berechtigung erteilen, Firewall-Protokolle an den OfficeScan Server zu senden. In diesem Bereich können Sie den Zeitplan für das Senden des Protokolls festlegen. Diesen Zeitplan verwenden nur Agents, die zum Senden von Firewall-Protokollen berechtigt sind.

  Informationen zu den Firewall-Berechtigungen, die für ausgewählte Agents verfügbar sind, finden Sie unter *Firewall-Berechtigungen auf Seite 13-26*.

- **OfficeScan Firewall-Treiber nur nach einem Neustart des Systems aktualisieren**

  Ermöglichen Sie dem OfficeScan Agent, erst ein Update des allgemeinen Firewall-Treibers durchzuführen, nachdem der OfficeScan Agent-Endpunkt neu gestartet wurde. Aktivieren Sie diese Option, um potenzielle Störungen des agent-Endpunkts zu vermeiden (wie eine temporäre Trennung vom Netzwerk), wenn der allgemeine Firewall-Treiber während eines Agent-Upgrades aktualisiert wird.

- **Firewall-Protokollinformationen stündlich an den OfficeScan Server senden, um die Möglichkeit eines Firewall-Ausbruchs festzustellen**

  Wenn Sie diese Option aktivieren, senden die OfficeScan Agents die Firewall-Protokollzähler nur ein Mal pro Stunde an den OfficeScan Server.

  Weitere Informationen über Firewall-Protokolle finden Sie unter *Firewall-Protokolle auf Seite 13-32*.

  OfficeScan verwendet Protokollzähler und Kriterien für den Ausbruch von Verstößen gegen die Firewall, um die Wahrscheinlichkeit eines Ausbruchs von Firewall-Verstößen zu ermitteln. OfficeScan versendet im Fall eines Ausbruchs E-Mail-Benachrichtigungen an die OfficeScan Administratoren.

- Navigieren Sie zum Abschnitt **Einstellungen für Certified Safe Software Service**, und ändern Sie ggf. den Certified Safe Software Service.

  Der Certified Safe Software Service fragt Trend Micro Rechenzentren ab, um die Sicherheit eines von der Sperrung bei Malware-Verhalten, der Ereignisüberwachung, der Firewall oder der Virensuche erkannten Programms zu überprüfen. Aktivieren Sie den Certified Safe Software Service, um die Häufigkeit von Fehlalarmen zu verringern.

Hinweis

Achten Sie auf korrekte Proxy-Einstellungen für OfficeScan Agents (weitere Informationen finden Sie unter *OfficeScan Agent Proxy-Einstellungen auf Seite 15-53*), bevor Certified Safe Software Service aktiviert wird. Bei fehlerhaften Proxy-Einstellungen sowie einer Internet-Verbindung, die nicht ständig besteht, kann es zu Verzögerungen kommen, oder Antworten von Trend Micro Rechenzentren können nicht abgerufen werden, was zur Folge hat, dass überwachte Programme nicht zu antworten scheinen.

Des Weiteren können IPv6-OfficeScan Agents keine direkten Abfragen an Trend Micro Rechenzentren richten. Ein Dual-Stack-Proxy-Server wie beispielsweise DeleGate, der IP-Adressen konvertieren kann, muss ermöglichen, dass die OfficeScan Agents eine Verbindung zu Trend Micro Rechenzentren herstellen können.

Einstellungen der allgemeinen Firewall konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Wechseln Sie auf der Registerkarte **Sicherheitseinstellungen** zum Abschnitt **Firewall-Einstellungen** und konfigurieren Sie Folgendes:
   - *Firewall-Protokolle an den Server senden auf Seite 13-28*
   - *OfficeScan Firewall-Treiber nur nach einem Neustart des Systems aktualisieren auf Seite 13-29*
   - *Firewall-Protokollinformationen stündlich an den OfficeScan Server senden, um die Möglichkeit eines Firewall-Ausbruchs festzustellen auf Seite 13-29*
3. Wechseln Sie auf der Registerkarte **System** zum Abschnitt **Einstellungen für Certified Safe Software Service** und konfigurieren Sie Folgendes:
   - *Certified Safe Software Service für Verhaltensüberwachung, Firewall und Virensuchen aktivieren auf Seite 13-29*
4. Klicken Sie auf **Speichern**.

Benachrichtigungen bei Firewall-Verstößen für OfficeScan Agent-Benutzer

OfficeScan kann sofort, nachdem die OfficeScan Firewall den ausgehenden Datenverkehr gesperrt hat, der gegen Firewall-Richtlinien verstößt, eine Benachrichtigung auf Endpunkten anzeigen. Gewähren Sie den Benutzern die Berechtigung, die Benachrichtigung zu aktivieren/deaktivieren.

Hinweis

Sie können die Benachrichtigung auch bei der Konfiguration einer bestimmten Firewall-Richtlinie aktivieren. Informationen zum Konfigurieren einer Firewall-Richtlinie finden Sie unter *Firewall-Richtlinie hinzufügen auf Seite 13-11*.

Den Benutzern die Berechtigung gewähren, die Benachrichtigung zu aktivieren/deaktivieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Gehen Sie auf der Registerkarte **Berechtigungen** zum Abschnitt **Firewall-Berechtigungen**.
5. Wählen Sie **Benutzer dürfen Firewall, Intrusion Detection System (IDS) und Warnmeldung der Firewall aktivieren/deaktivieren**.
6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen

Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Den Inhalt der Firewall-Benachrichtigung ändern

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Agent**.
2. Wählen Sie im Listenfeld **Typ** die Option **Firewall-Verstöße** aus.
3. Sie können die Standardmeldungen im dafür vorgesehenen Textfeld bearbeiten.
4. Klicken Sie auf **Speichern**.

Firewall-Protokolle

Firewall-Protokolle, die auf dem Server verfügbar sind, werden von OfficeScan Agents gesendet, die die Berechtigung haben, Firewall-Protokolle zu senden. Gewähren Sie bestimmten agents diese Berechtigung, um den Datenverkehr auf dem Endpunkte zu überwachen und zu analysieren, der von der OfficeScan Firewall gesperrt wird.

Weitere Informationen über Firewall-Berechtigungen finden Sie unter *Firewall-Berechtigungen auf Seite 13-26*.

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell, oder konfigurieren Sie eine zeitgesteuerte Löschung der Protokolle. Weitere Informationen zur Protokollverwaltung finden Sie unter *Protokollmanagement auf Seite 14-47*.

Firewall-Protokolle anzeigen

Der OfficeScan Agent generiert Protokolle, nachdem Firewall-Verstöße erkannt wurden, und sendet die Protokolle an den Server.

Prozedur

1. Navigieren Sie zu einer der folgenden Optionen:
   - **Protokolle** > **Agents** > **Sicherheitsrisiken**
   - **Agents** > **Agent-Verwaltung**
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Navigieren Sie zum Fenster **Kriterien für das Firewall-Protokoll**:
   - Klicken Sie im Fenster **Sicherheitsrisiko-Protokolle** auf **Protokolle anzeigen** > **Firewall-Protokolle**.
   - Klicken Sie im Fenster **Agent-Verwaltung** auf **Protokolle** > **Firewall-Protokolle**.
4. Um sicherzustellen, dass die aktuellen Protokolle verfügbar sind, klicken Sie auf **Agents benachrichtigen**. Warten Sie einen Moment, bis die Agents die Firewall-Protokolle gesendet haben, bevor Sie mit dem nächsten Schritt fortfahren.
5. Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.
6. Sehen Sie die Protokolle ein. Die Protokolle enthalten die folgenden Informationen:

VORGANG	BESCHREIBUNG
Datum/Uhrzeit	Zeitpunkt der Erkennung
Endpunkt	Endpunkt, auf dem die Erkennung erfolgte
Domäne	Die Domäne, in der der Fund aufgetreten ist.

Vorgang	Beschreibung
Remote-Host	Die IP-Adresse des Remote-Hosts
Lokaler Host	Die IP-Adresse des lokalen Hosts
Protokoll	Das verwendete Protokoll
Port	Die Portnummer
Richtung	• **Empfangen**: Gibt an, dass es sich um eingehenden Datenverkehr gehandelt hat. • **Senden**: Gibt an, dass es sich um ausgehenden Datenverkehr gehandelt hat.
Prozess	Das ausführbare Programm oder der Dienst, der auf dem Endpunkt ausgeführt wird, der den Firewall-Verstoß ausgelöst hat
Beschreibung	Beschreibt das tatsächliche Sicherheitsrisiko (z. B. Netzwerkvirus oder IDS-Angriff) oder den Verstoß gegen eine Firewall-Richtlinie

7. Wenn Sie Protokolle als kommagetrennte Datei (CSV-Datei) speichern möchten, klicken Sie auf **Alle in CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Ausbrüche bei Firewall-Verstoß

Definieren Sie einen Ausbruch von Verstößen gegen die Firewall durch die Anazhl der Verstöße gegen die Firewall und den Entdeckungszeitraum.

OfficeScan verfügt über zahlreiche Standardbenachrichtigungen, die Sie und andere OfficeScan Administratoren über einen Ausbruch informieren. Sie können die Benachrichtigung ändern, damit sie Ihren Anforderungen entspricht.

Hinweis

OfficeScan kann Firewall-Ausbruchsbenachrichtigungen per E-Mail versenden. Konfigurieren Sie E-Mail-Einstellungen, damit OfficeScan die E-Mails erfolgreich versenden kann. Weitere Informationen finden Sie unter *Einstellungen für die Administratorbenachrichtigungen auf Seite 14-43*.

Kriterien für den Ausbruch von Verstößen gegen die Firewall und Benachrichtigungen konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Ausbruch**.
2. Auf der Registerkarte **Kriterien**:
   a. Gehen Sie zum Abschnitt **Firewall-Verstöße**.
   b. Wählen Sie **Firewall-Verstöße auf OfficeScan Agents überwachen** aus.
   c. Bestimmen Sie die Anzahl von IDS-Protokollen, Firewall-Protokollen und Netzwerkvirenprotokollen.
   d. SBestimmen Sie den Entdeckungszeitraum.

   Tipp

   Trend Micro empfiehlt, die Standardeinstellungen in diesem Fenster zu übernehmen.

   OfficeScan sendet eine Benachrichtigung, wenn die vorgegebene Anzahl von Protokollen überschritten wird.. Wenn Sie zum Beispiel 100 IDS-Protokolle, 100 Firewall-Protokolle, 100 Netzwerkvirenprotokolle und einen Zeitraum von 3 Stunden angeben, versendet OfficeScan die Benachrichtigung, wenn der Server 301 Protokolle innerhalb von 3 Stunden empfängt.
3. Auf der Registerkarte **E-Mail**:
   a. Gehen Sie zum Abschnitt **Ausbrüche von Firewall-Verstößen**.

b. Wählen Sie **Benachrichtigung über E-Mail aktivieren**.

c. Bestimmen Sie die Empfänger der E-Mail.

d. Übernehmen oder ändern Sie die Standardbetreffzeile und -nachricht. Sie können Token-Variablen als Platzhalter für Daten in den Feldern **Betreff** und **Nachricht** verwenden.

TABELLE 13-3. Token-Variablen für Benachrichtigungen über Ausbrüche von Verstößen gegen die Firewall

VARIABLE	BESCHREIBUNG
%A	Anzahl der Einträge für einen bestimmten Protokolltyp wurde überschritten
%C	Anzahl der Protokolle bei Firewall-Verstoß.
%T	Zeitraum, in dem die Protokolle bei Firewall-Verstoß gesammelt wurden

4. Klicken Sie auf **Speichern**.

Die OfficeScan Firewall testen

Führen Sie Tests auf einem einzelnen OfficeScan Agent oder einer Gruppe von OfficeScan Agents durch, um die ordnungsgemäße Funktionsweise der OfficeScan Firewall zu gewährleisten.

Warnung!

Sie sollten die Einstellungen des OfficeScan Agent-Programms nur in einer kontrollierten Umgebung testen. Die getesteten Endpunkte sollten nicht mit dem Netzwerk oder dem Internet verbunden sein. Ansonsten wären OfficeScan Agent Endpunkte dem Risiko eines Angriffs durch Viren, Hacker usw. ausgesetzt.

Prozedur

1. Testrichtlinie erstellen und speichern. Konfigurieren Sie die Einstellungen, um den zu testenden Datenverkehr zu sperren. Um beispielsweise zu verhindern, dass der

OfficeScan Agent eine Internet-Verbindung herstellt, verwenden Sie folgende Einstellungen:

a. Legen Sie als Sicherheitsebene **Niedrig** fest (der gesamte eingehende/ausgehende Datenverkehr wird zugelassen).

b. Wählen Sie **Firewall aktivieren und Benutzer bei Verstoß gegen die Firewall benachrichtigen**.

c. Erstellen Sie eine Ausnahme zum Sperren von HTTP- (bzw. HTTPS-) Datenverkehr.

2. Erstellen und speichern Sie ein Testprofil durch Auswahl der agents, auf denen Sie die Firewall-Funktionen testen möchten. Ordnen Sie dem Testprofil eine Testrichtlinie zu.

3. Klicken Sie auf **Den Agents ein Profil zuweisen**.

4. Überprüfen Sie die Verteilung.

   a. Klicken Sie auf **Agents** > **Agent-Verwaltung**.

   b. Wählen Sie die Domäne des agents aus.

   c. Wählen Sie aus der agent-Hierarchie die Option **Firewall-Ansicht**.

   d. Stellen Sie sicher, dass unter die Spalte **Firewall** in der agent-Hierarchie ein grünes Häkchen gesetzt ist. Wenn das Intrusion Detection System für diesen agent aktiviert ist, überprüfen Sie, ob sich in der Spalte **IDS** auch ein grünes Häkchen befindet.

   e. Überprüfen Sie, ob der agent die richtige Firewall-Richtlinie anwendet. Die Richtlinie wird in der Spalte **Firewall-Richtlinie** in der agent-Hierarchie angezeigt.

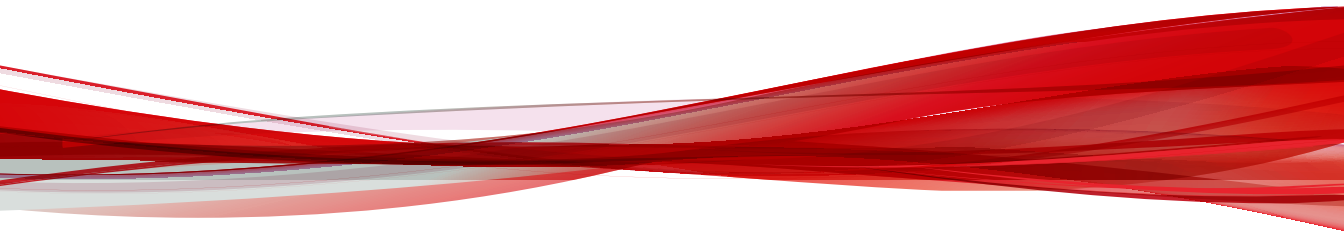
5. Testen Sie die Firewall auf dem agent Endpunkt, indem Sie versuchen, den in der Richtlinie festgelegten Datenverkehr zu versenden oder zu empfangen.

6. Um eine Richtlinie zu testen, die den agent am Zugriff auf das Internet hindern soll, öffnen Sie ein Browser-Fenster auf dem agent Endpunkt. Wenn Sie OfficeScan so konfiguriert haben, dass eine Benachrichtigung bei Firewall-

Verstößen angezeigt wird, wird die Meldung auf dem agent-Endpunkt angezeigt, wenn der ausgehende Datenverkehr gegen die Firewall-Richtlinien verstößt.

Teil III

OfficeScan Server und Agents verwalten



Kapitel 14

Den OfficeScan Server verwalten

In diesem Kapitel werden Verwaltung und Konfiguration von OfficeScan Servern beschrieben.

Es werden folgende Themen behandelt:

- *Rollenbasierte Administration auf Seite 14-3*
- *Trend Micro Control Manager auf Seite 14-25*
- *Einstellungen für Liste der verdächtigen Objekte auf Seite 14-38*
- *Referenzserver auf Seite 14-40*
- *Einstellungen für die Administratorbenachrichtigungen auf Seite 14-43*
- *Systemereignisprotokolle auf Seite 14-45*
- *Protokollmanagement auf Seite 14-47*
- *Lizenzen auf Seite 14-51*
- *OfficeScan Datenbanksicherung auf Seite 14-54*
- *SQL Server Migration Tool auf Seite 14-56*
- *Einstellungen des OfficeScan Webservers/Agents auf Seite 14-61*
- *Kommunikation zwischen Server und Agents auf Seite 14-62*

- *Kennwort der Webkonsole auf Seite 14-68*
- *Einstellungen der Webkonsole konfigurieren auf Seite 14-69*
- *Quarantäne-Manager auf Seite 14-70*
- *Server Tuner auf Seite 14-71*
- *Smart Feedback auf Seite 14-73*

Rollenbasierte Administration

Benutzen Sie eine rollenbasierte Administration, um den Zugriff auf die OfficeScan Webkonsole sicherzustellen und zu steuern. Gibt es in Ihrem Unternehmen mehrere OfficeScan Administratoren, können Sie diese Funktion nutzen, um den Administratoren bestimmte Berechtigungen für die Webkonsole zuzuweisen und sie nur mit den Tools und Berechtigungen auszustatten, die erforderlich sind, um bestimmte Aufgaben auszuführen. Sie können auch den Zugriff auf die agent-Hierarchie steuern, indem Sie ihnen eine oder mehrere Domänen zur Verwaltung zuordnen. Außerdem können Sie Nicht-Administratoren einen Zugriff auf die Webkonsole über "Nur anzeigen" gewähren.

Jeder Benutzer (Administrator oder Nicht-Administrator) bekommt eine bestimmte Rolle zugewiesen. Eine Rolle definiert die Zugriffsrechte auf die Webkonsole. Benutzer melden sich bei der Webkonsole mit benutzerdefinierten Konten oder Active Directory-Konten an.

Die rollenbasierte Administration umfasst die folgenden Aufgaben:

1. Benutzerrollen definieren. Weitere Informationen finden Sie unter *Benutzerrollen auf Seite 14-14*.

2. Benutzerkonten konfigurieren und jedem Benutzerkonto eine bestimmte Rolle zuweisen. Weitere Informationen finden Sie unter *Benutzerkonten auf Seite 14-3*.

Aktivitäten der Webkonsole für alle Benutzer aus den Systemereignisprotokollen anzeigen. Die folgenden Aktivitäten werden protokolliert:

- Anmeldung an der Konsole
- Kennwortänderung
- Abmeldung von der Konsole
- Zeitüberschreitung der Sitzung (der Benutzer wird automatisch abgemeldet)

Benutzerkonten

Richten Sie manuelle Benutzerkonten ein oder verwenden Sie Active Directory-Konten, um Berechtigungen zum Anzeigen oder Konfigurieren der detaillierten Agent-

Einstellungen, der Aufgaben und der in der Agent-Hierarchie verfügbaren Daten zuzuweisen. Sie müssen jedem Benutzer eine bestimmte Rolle zuweisen, anhand derer die Menüelemente der Webkonsole bestimmt werden, die der Benutzer anzeigen oder konfigurieren kann. Sie können OfficeScan-Benutzerkonten verwenden, um die Single-Sign-On-Funktion für OfficeScan über die Trend Micro Control Manager Konsole zu verwenden.

Während Installation von OfficeScan Server erstellt Setup automatisch ein integriertes Konto mit der Bezeichnung "root". Benutzer, die sich am Root-Konto anmelden, können auf alle Menübefehle zugreifen. Sie können das Root-Konto nicht löschen, aber Sie können die Kontodaten ändern, beispielsweise das Kennwort und den vollständigen Namen oder die Kontobeschreibung. Wenn Sie das Kennwort für das Root-Konto vergessen, wenden Sie sich zur Unterstützung beim Zurücksetzen des Kennworts an Ihren Support-Anbieter.

Hinweis

Nach dem Aktualisieren des OfficeScan Servers müssen Sie alle benutzerdefinierten Konten bearbeiten und alle neuen Funktionen im Bildschirm **Schritt 3 Agent-Hierarchiemenü definieren** für zuvor hinzugefügte benutzerdefinierte Konten manuell aktivieren.

Weitere Informationen zu Berechtigungen finden Sie unter *Definieren von Berechtigungen für Domänen auf Seite 14-11*.

In der folgenden Tabelle sind die Aufgaben aufgeführt, die im Fenster **Benutzerkonten** verfügbar sind.

TASK	BESCHREIBUNG
Konto hinzufügen	Klicken Sie auf **Hinzufügen**, um eine neues Benutzerkonto zu erstellen. Weitere Informationen finden Sie unter *Ein Benutzerkonto hinzufügen auf Seite 14-7*.
Vorhandene Konten löschen	Wählen Sie bereits vorhandene Benutzerkonten aus und klicken Sie auf **Löschen**.

TASK	BESCHREIBUNG
Vorhandene Konten bearbeiten	Klicken Sie auf den Namen eines bereits vorhandenen Benutzerkontos, um die aktuellen Kontoeinstellungen anzuzeigen oder zu ändern.

Menüelemente der Agent-Verwaltung

Die folgende Tabelle enthält die verfügbaren Menüelemente der Agent-Verwaltung.

Hinweis

Menüelemente werden erst nach der Aktivierung des entsprechenden Plug-in-Programms angezeigt. Wenn beispielsweise das Modul für 'Prävention vor Datenverlust' nicht aktiviert ist, werden in der Liste keine Menüelemente für die Prävention vor Datenverlust angezeigt.

TABELLE 14-1. Menüelemente der Agent-Verwaltung

HAUPTMENÜPUNKT	UNTERMENÜS
Status	n. v.
Aufgaben	• Jetzt durchsuchen • Agent deinstallieren • Zentrale Quarantänewiederherstellung • Spyware/Grayware wiederherstellen

HAUPTMENÜPUNKT	UNTERMENÜS

Einstellungen	• Sucheinstellungen
	  • Suchmethoden
	  • Einstellungen für manuelle Suche
	  • Einstellungen für Echtzeitsuche
	  • Einstellungen für die zeitgesteuerte Suche
	  • Einstellungen für Jetzt durchsuchen
	• Web-Reputation-Einstellungen
	• Verdächtige Verbindungseinstellungen
	• Einstellungen der Verhaltensüberwachung
	• Einstellungen der Gerätesteuerung
	• DLP-Einstellungen
	• Exemplar Zusendung
	• Update-Agent-Einstellungen
	• Berechtigungen und andere Einstellungen
	• Zusätzliche Diensteinstellungen
	• Liste der zugelassenen Spyware/Grayware
	• Liste der vertrauenswürdigen Programme
	• Einstellungen für "Vorausschauendes Maschinenlernen"
	• Einstellungen exportieren
	• Einstellungen importieren

HAUPTMENÜPUNKT	UNTERMENÜS
Protokolle	• Viren-/Malware-Protokolle • Spyware-/Grayware-Protokolle • Firewall-Protokolle • Web-Reputation-Protokolle • Protokolle zu verdächtigen Verbindungen • Protokolle zu verdächtigen Dateien • C&C-Callback-Protokolle • Verhaltensüberwachungsprotokolle • Protokolldaten für "Vorausschauendes Maschinenlernen" • Protokolle der Gerätesteuerung • Protokolle für 'Prävention vor Datenverlust' • Protokolle zu Suchvorgängen • Protokolle löschen
Agent-Hierarchie verwalten	• Domäne hinzufügen • Domäne umbenennen • Agent verschieben • Domäne/Agent entfernen
Exportieren	n. v.

Ein Benutzerkonto hinzufügen

Richten Sie manuelle Benutzerkonten ein oder verwenden Sie Active Directory-Konten, um Berechtigungen zum Anzeigen oder Konfigurieren der detaillierten Agent-Einstellungen, der Aufgaben und der in der Agent-Hierarchie verfügbaren Daten zuzuweisen.

Prozedur

1. Navigieren Sie zu **Administration** > **Kontenverwaltung** > **Benutzerkonten**.
2. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Schritt 1 Benutzerinformationen** wird angezeigt.
3. Wählen Sie **Dieses Konto aktivieren** aus.
4. Wählen Sie im Listenfeld **Rolle auswählen** eine zuvor konfigurierte Rolle aus.

   Weitere Informationen finden Sie unter *Eine benutzerdefinierte Rolle hinzufügen auf Seite 14-17*.
5. Konfigurieren Sie im Abschnitt **Benutzerinformationen** folgende Einstellungen:
   - **Benutzerdefiniertes Konto**: Wählen Sie diese Option aus, um ein manuelles Benutzerkonto zu erstellen und die erforderlichen Informationen anzugeben.
     - **Benutzername**: Geben Sie einen eindeutigen Benutzernamen für das Konto ein.
     - **Beschreibung**: Geben Sie eine Beschreibung für das Konto ein.
     - **Kennwort**: Geben Sie das Kennwort ein, das das Konto für die Anmeldung bei der OfficeScan Webkonsole verwendet, und bestätigen Sie es.

       Wichtig

       Sie können den Benutzernamen nicht als Kennwort für das Konto verwenden. Geben Sie ein Kennwort ein, das sich vom Benutzernamen unterscheidet.
     - **E-Mail-Adresse**: Geben Sie die E-Mail-Adresse ein, die dem Benutzerkonto zugeordnet ist.

Hinweis

OfficeScan sendet Benachrichtigungen an diese E-Mail Adresse. Die Benachrichtigungen informieren den Empfänger über Sicherheitsrisiko-Funde und Übertragungen digitaler Assets.

Weitere Informationen zu Benachrichtigungen finden Sie unter *Benachrichtigungen bei Sicherheitsrisiken für Administratoren auf Seite 7-90*.

- **Active Directory-Benutzer oder -Gruppe**: Wählen Sie diese Option aus, wenn Sie vorhandene Active Directory-Konten oder -Gruppen für die Anmeldung bei der OfficeScan Webkonsole verwenden möchten.

Hinweis

Die Option **Active Directory-Benutzer oder -Gruppe** wird nur dann angezeigt, wenn die Active Directory-Integration bereits konfiguriert wurde.

a. Geben Sie im Feld **Benutzername oder Gruppe** das Active Directory-Konto ein, das Sie verwenden möchten.

b. Geben Sie im Feld **Domäne** die Active Directory-Domäne ein, zu der die Angabe im Feld **Benutzername oder Gruppe** gehört.

c. Klicken Sie auf **Suchen**.

d. Wählen Sie in der Liste **Benutzer und Gruppen** das gewünschte Konto aus und klicken Sie auf **>**, um das Konto in der Liste **Ausgewählte Benutzer und Gruppen** hinzuzufügen.

6. Klicken Sie auf **Weiter**.

   Das Fenster **Schritt 2 Agent-Domänensteuerung** wird angezeigt.

7. Wählen Sie das Root-Konto aus, um es dem Konto zu gestatten, alle OfficeScan Domänen anzuzeigen, oder wählen Sie bestimmte OfficeScan Domänen aus, auf die das Benutzerkonto in der Agent-Hierarchie zugreifen kann.

Wichtig

OfficeScan zeigt die ausgewählten Domänen nur dann an, wenn das Benutzerkonto auf die Agent-Hierarchie zugreift. Wenn Sie keine Domäne auswählen, blendet OfficeScan die Domäne in der Agent-Hierarchie aus.

8. Klicken Sie auf **Weiter**.

   Das Fenster **Schritt 3 Agent-Hierarchiemenü definieren** wird angezeigt.

9. Klicken Sie auf **Verfügbare Menüelemente**, und geben Sie die Berechtigung für jedes verfügbare Menüelement an. Eine Liste aller verfügbaren Menüelemente finden Sie unter *Menüelemente der Agent-Verwaltung auf Seite 14-5*.

   Der Bereich der agent-Hierarchie, den Sie in Schritt 8 konfiguriert haben, bestimmt die Berechtigungsstufe für die Menüelemente und definiert die Berechtigungsziele. Der Bereich der agent-Hierarchie kann entweder die Root-Domäne (alle agents) oder spezielle Domänen der agent-Hierarchie umfassen.

TABELLE 14-2. Agent-Verwaltung – Menüelemente und Bereich der Agent-Hierarchie

KRITERIEN	BEREICH DER AGENT-HIERARCHIE	
	ROOT-DOMÄNE	BESTIMMTE DOMÄNEN
Menüelement-Berechtigung	Konfigurieren, Anzeigen oder Kein Zugriff	Konfigurieren, Anzeigen oder Kein Zugriff

Kriterien	Bereich der Agent-Hierarchie	
	Root-Domäne	Bestimmte Domänen
Ziel	Root-Domäne (alle agents) oder bestimmte Domänen Sie weisen beispielsweise einer Rolle die Berechtigung "Konfigurieren" für das Menüelement "Aufgaben" in der agent-Hierarchie zu. Wenn das Ziel die Root-Domäne ist, kann der Benutzer die Aufgaben auf allen agents starten. Wenn die Ziele die Domänen A und B sind, können die Aufgaben nur auf den agents in den Domänen A und B gestartet werden.	Nur ausgewählte Domänen Sie weisen beispielsweise einer Rolle die Berechtigung "Konfigurieren" für das Menüelement "Einstellungen" in der agent-Hierarchie zu. Hier kann der Benutzer die Einstellungen nur auf agents in den ausgewählten Domänen verteilen.
	Die agent-Hierarchie wird nur angezeigt, wenn die Berechtigung für das Agent-Verwaltung-Menüelement in "Menüelemente für Server/Agents" auf "Anzeigen" festgelegt ist.	

- Wenn Sie das Kontrollkästchen unter **Konfigurieren** aktivieren, wird das Kontrollkästchen unter **Anzeigen** automatisch ausgewählt.
- Bei deaktiviertem Kontrollkästchen lautet die Berechtigung "Kein Zugriff".
- Wenn Sie Berechtigungen für eine bestimmte Domäne konfigurieren, können Sie die Berechtigungen in andere Domänen kopieren, indem Sie auf **Einstellungen der ausgewählten Domäne in andere Domänen kopieren** klicken.

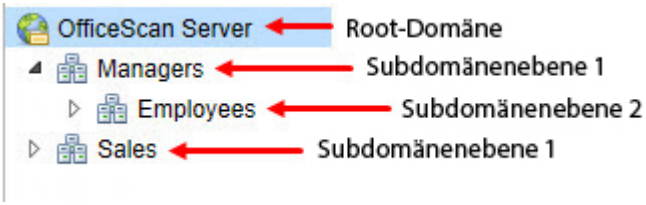
10. Klicken Sie auf **Fertig stellen**.
11. Senden Sie die Kontodaten an den Benutzer.

Definieren von Berechtigungen für Domänen

Beim Definieren von Berechtigungen für Domänen wendet OfficeScan automatisch die Berechtigungen für eine übergeordnete Domäne auf alle Subdomänen an, die verwaltet

werden. Eine Subdomäne kann nicht über weniger Berechtigungen als ihre übergeordnete Domäne verfügen. Beispiel: Wenn der Systemadministrator über die Berechtigung verfügt, alle agents anzuzeigen und zu konfigurieren, die OfficeScan verwaltet (die „OfficeScan Server“-Domäne), müssen die Berechtigungen für Subdomänen dem Systemadministrator den Zugriff auf diese Konfigurationsfunktionen ermöglichen. Das Entfernen einer Berechtigung auf einer Subdomäne würde bedeuten, dass der Systemadministrator nicht über vollständige Konfigurationsberechtigungen für alle agents verfügt.

Die Domänenstruktur ist für das folgende Verfahren wie folgt:



Beispiel: Um dem Benutzerkonto „Chris“ Berechtigungen zum Anzeigen und Konfigurieren spezifischer Menüelemente für die Subdomäne „Mitarbeiter“ zu erteilen, aber der übergeordneten Domäne „Managers“ nur die Berechtigung zum Anzeigen von Protokollen zu erteilen, führen Sie den folgenden Vorgang durch.

TABELLE 14-3. Berechtigungen für das Benutzerkonto „Chris“

DOMÄNE	GEWÜNSCHTE BERECHTIGUNGEN
OfficeScan Server	Keine bestimmten Berechtigungen.
Managers	**Protokolle** anzeigen
Mitarbeiter	**Aufgaben** anzeigen und konfigurieren **Protokolle** anzeigen und konfigurieren **Einstellungen** anzeigen
Vertrieb	Keine bestimmten Berechtigungen.

Prozedur

1. Navigieren Sie zum Fenster **Benutzerkonten: Schritt 3: Agent-Hierarchiemenü definieren**.
2. Klicken Sie auf die „OfficeScan Server“-Domäne.
3. Deaktivieren Sie die Kontrollkästchen **Anzeigen** und **Konfigurieren**.

   Hinweis

   Die „OfficeScan Server“-Domäne kann nur konfiguriert werden bei folgender Auswahl aller Subdomänen im Fenster **Benutzerkonto: Schritt 2: Agent-Domänensteuerung**.

4. Klicken Sie auf die Domäne „Vertrieb“.
5. Deaktivieren Sie die Kontrollkästchen **Anzeigen** und **Konfigurieren**.

   Hinweis

   Die Domäne „Vertrieb“ wird nur angezeigt bei folgender Auswahl im Fenster **Benutzerkonten: Schritt 2: Agent-Domänensteuerung**.

6. Klicken Sie auf die Domäne „Managers“.
7. Wählen Sie „Protokolle anzeigen“ aus und deaktivieren Sie die Kontrollkästchen **Anzeigen** und **Konfigurieren**.
8. Klicken Sie auf die Domäne „Mitarbeiter“.
9. Wählen Sie die folgenden Menüelemente für Chris aus:
   - **Aufgaben**: Anzeigen und konfigurieren
   - **Protokolle**: Anzeigen und konfigurieren
   - **Einstellungen**: Ansicht

   Chris kann jetzt die ausgewählten Menüelemente für die Domäne „Mitarbeiter“ anzeigen sowie konfigurieren und **Protokolle** nur für die Domäne „Managers“ anzeigen.

Wenn Chris über die Berechtigung zum Anzeigen und Konfigurieren der Domäne „Managers“ verfügt, erteilt OfficeScan die Berechtigungen automatisch zur Subdomäne „Mitarbeiter“. Dies tritt auf, da die Domäne „Managers“ alle Subdomänen verwaltet.

Benutzerrollen

Definieren Sie Benutzerrollen, um den Zugriff zu beschränken, den bestimmte Benutzerkonten auf bestimmte Fenster der Webkonsole haben, und weisen Sie diese zu. Sie können Benutzerrollen definieren, um die Fenster der Webkonsole vollständig auszublenden, den Zugriff auf „Schreibgeschützt“ beschränken oder Rechte für die vollständige Konfiguration erteilen.

In der folgenden Tabelle sind die Aufgaben aufgeführt, die im Fenster **Benutzerrollen** verfügbar sind.

TASK	BESCHREIBUNG
Benutzerdefinierte Rolle hinzufügen	Klicken Sie auf **Hinzufügen**, um eine neue benutzerdefinierte Rolle zu erstellen. Weitere Informationen finden Sie unter *Eine benutzerdefinierte Rolle hinzufügen auf Seite 14-17*. **Wichtig** Nur das „Root“-Konto oder Benutzer mit der integrierten Administratorrolle können benutzerdefinierte Benutzerrollen erstellen und Benutzerkonten zuweisen.
Einstellungen aus einer vorhandenen benutzerdefinierten Rolle kopieren	Wählen Sie eine bereits vorhandene benutzerdefinierte Rolle aus und klicken Sie auf **Kopieren**. Das Fenster **Rolle kopieren** wird angezeigt und Sie haben die Möglichkeit, eine neue benutzerdefinierte Rolle basierend auf den ursprünglichen Einstellungen zu erstellen.

TASK	BESCHREIBUNG
Vorhandene benutzerdefinierte Rollen löschen	Wählen Sie die gewünschten bereits vorhandenen benutzerdefinierten Rollen aus und klicken Sie auf **Löschen**. **Wichtig** Rollen, die zurzeit Benutzerkonten zugewiesen sind, können nicht gelöscht werden.
Benutzerdefinierte Rollen exportieren	Wählen Sie bereits vorhandene benutzerdefinierte Rollen aus, klicken Sie auf die Schaltfläche **Exportieren** und wählen Sie dann eine der folgenden Optionen aus: • **In DAT-Datei exportieren**: Exportiert die ausgewählten Rollen in eine DAT-Datei, die Sie in einen anderen OfficeScan Server importieren können. • **In CSV-Datei exportieren**: Exportiert die ausgewählten Rollen in eine CSV-Datei, über die Sie Rolleneinstellungen anzeigen können. **Wichtig** Sie können die generierte CSV-Datei nicht in den OfficeScan Server importieren.
Benutzerdefinierte Rollen importieren	Klicken Sie auf **Importieren**, um die Einstellungen der benutzerdefinierten Rollen aus einer zuvor exportierten DAT-Datei mit Benutzerrollen zu importieren. Weitere Informationen finden Sie unter *Benutzerdefinierte Rollen importieren oder exportieren auf Seite 14-24*.

TASK	BESCHREIBUNG
Vorhandene benutzerdefinierte Rollen bearbeiten	Klicken Sie auf den Namen einer bereits vorhandenen Benutzerrolle, um die aktuellen Rolleneinstellungen anzuzeigen oder zu ändern. **Hinweis** Die Inhalte vordefinierter Benutzerrollen können nicht geändert werden. Weitere Informationen finden Sie unter *Integrierte Benutzerrollen auf Seite 14-16*.

Integrierte Benutzerrollen

Zum Lieferumfang von OfficeScan gehören mehrere integrierte Benutzerrollen, die Sie weder ändern noch löschen können. Bei den integrierten Rollen handelt es sich um Folgende:

TABELLE 14-4. Integrierte Benutzerrollen

ROLLENNAME	BESCHREIBUNG
Administrator	Delegieren Sie diese Rolle an andere OfficeScan Administratoren oder Benutzer mit ausreichenden Kenntnissen über OfficeScan. Benutzer mit dieser Rolle können alle Menüelemente konfigurieren. **Hinweis** Nur Benutzer, denen die Rolle „Administrator (integriert)“ zugewiesen ist, haben Zugriff auf das Plug-ins-Menüelement.

ROLLENNAME	BESCHREIBUNG

Gastbenutzer	Delegieren Sie diese Rolle an Benutzer, die die Webkonsole zu Referenzzwecken anzeigen möchten.
	• Benutzer mit dieser Rolle haben keinen Zugriff auf die folgenden Menüpunkte:
	  • Plug-ins
	  • **Administration** > **Kontenverwaltung** > **Benutzerrollen**
	  • **Administration** > **Kontenverwaltung** > **Benutzerkonten**
	• Benutzer können alle anderen Menübefehle sehen.

Trend Hauptbenutzer (nur Upgrade-Rolle)	Diese Rolle ist nur verfügbar, wenn OfficeScan 10 auf diese Version aktualisiert wird. Diese Rolle erbt die Berechtigungen der Hauptbenutzerrolle in OfficeScan 10. Benutzer mit dieser Rolle sind berechtigt, alle Domänen in der agent-Hierarchie zu konfigurieren, haben jedoch keinen Zugriff auf die neuen Funktionen aus dieser Version.

Eine benutzerdefinierte Rolle hinzufügen

Fügen Sie neue benutzerdefinierte Rollen hinzu, wenn die verfügbaren integrierten Rollen Ihre Anforderungen nicht erfüllen.

Weitere Informationen finden Sie unter *Integrierte Benutzerrollen auf Seite 14-16*.

Prozedur

1. Navigieren Sie zu **Administration** > **Kontenverwaltung** > **Benutzerrollen**.
2. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Rolle hinzufügen** wird angezeigt.
3. Geben Sie im Abschnitt **Informationen über die Rolle** Folgendes an:
   - **Name**: Geben Sie einen eindeutigen Namen für die Rolle ein.

- **Beschreibung**: (Optional)

4. Im Abschnitt **Rollenberechtigungen**:

   a. Wählen Sie die Menüelemente aus, auf die der Rolle zugewiesene Benutzerkonten zugreifen können.

      - **Menüelemente für Server/Agents**: Enthält globale OfficeScan Agent- und OfficeScan Servereinstellungen, -aufgaben und -daten.

        Weitere Informationen finden Sie unter *Menüelemente für Server und Agents auf Seite 14-19*.

      - **Menüelemente für verwaltete Domänen**: Enthält granulare OfficeScan Agent-Einstellungen, -Aufgaben und -Daten, die außerhalb der Agent-Hierarchie verfügbar sind.

        Weitere Informationen finden Sie unter *Menüelemente für verwaltete Domänen auf Seite 14-22*.

   b. Wählen Sie die Zugriffsberechtigungen für die ausgewählten Menüelemente aus, über die der Rolle zugewiesene Benutzerkonten verfügen können.

      - **Konfigurieren**: Gewährt den Vollzugriff auf ein Menüelement.

        Der Benutzer ist berechtigt alle Einstellungen zu konfigurieren, alle Aufgaben auszuführen und Daten in einem Menüpunkt anzuzeigen.

      - **Anzeigen**: Benutzer sind nur berechtigt, Einstellungen, Aufgaben und Daten eines Menüelements anzuzeigen.

Hinweis

Deaktivieren Sie die Kontrollkästchen **Konfigurieren** und **Anzeigen**, um ein Menüelement vollständig aus der Ansicht auszublenden. Menüelemente werden nicht für der Rolle zugewiesene Benutzerkonten angezeigt.

5. Klicken Sie auf **Speichern**.

   Die neue Rolle wird im Fenster **Benutzerrollen** angezeigt.

Menüelemente für Server und Agents

Die folgenden Tabellen enthalten die für Server/Agents verfügbaren Menüelemente.

Hinweis

Menüelemente werden erst nach der Aktivierung des entsprechenden Plug-in-Programms angezeigt. Wenn beispielsweise das Modul für 'Prävention vor Datenverlust' nicht aktiviert ist, werden in der Liste keine Menüelemente für die Prävention vor Datenverlust angezeigt. Zusätzliche Plug-in-Programme werden unter dem Plug-ins-Menüelement angezeigt.

Nur Benutzer, denen die Rolle „Administrator (integriert)“ zugewiesen ist, haben Zugriff auf das Plug-ins-Menüelement.

TABELLE 14-5. Menüelemente für "Agents"

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT
Agents	• Agent-Verwaltung • Agent-Gruppierung • Globale Agent-Einstellungen • Endpunktspeicherort • Prävention vor Datenverlust • Verbindungsüberprüfung • Ausbruchsprävention

TABELLE 14-6. Menüelemente für "Protokolle"

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT

Protokolle	• Agents
	  • Sicherheitsrisiken
	  • Agent-Komponenten-Update
	• Server-Update
	• Systemereignisse
	• Protokollwartung

TABELLE 14-7. Menüelemente für "Updates"

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Updates	Server	• Zeitgesteuertes Update • Manuelles Update • Update-Adresse
	Agents	• Automatisches Update • Update-Adresse
	Rollback	n. v.

TABELLE 14-8. Menüelemente für "Administration"

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Administration	Kontenverwaltung	• Benutzerkonten • Benutzerrollen

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
		Hinweis Nur Benutzer, die das integrierte Administratorkonto verwenden, können auf Benutzerkonten und Benutzerrollen zugreifen.
	Smart Protection	• Smart Protection Quellen • Integrierter Server • Smart Feedback
	Active Directory	• Active Directory-Integration • Zeitgesteuerte Synchronisierung
	Benachrichtigungen	• Allgemeine Einstellungen • Ausbruch • Agent
	Einstellungen	• Proxy • Agent-Verbindung • Inaktive Agents • Quarantäne-Manager • Produktlizenz • Control Manager • Webkonsole • Datenbanksicherung • Liste der verdächtigen Objekte

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
		• Edge-Relais • Server Migration

Menüelemente für verwaltete Domänen

Die folgende Tabelle enthält die verfügbaren Menüelemente für verwaltete Domänen.

TABELLE 14-9. Menüelemente für "Dashboard"

HAUPTMENÜPUNKT	MENÜELEMENT
Dashboard **Hinweis** Alle Benutzer können unabhängig von der Berechtigung auf diese Seite zugreifen.	n. v.

TABELLE 14-10. Menüelemente für "Bewertung"

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Bewertung	Einhaltung von Sicherheitsrichtlinien	• Manueller Bericht • Zeitgesteuerter Bericht
	Nicht verwaltete Endpunkte	n. v.

TABELLE 14-11. Menüelemente für "Agents"

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Agents	Firewall	• Richtlinien • Profile
	Agent-Installation	• Browserbasiert • Remote

TABELLE 14-12. Menüelemente für "Protokolle"

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Protokolle	Agents	• Verbindungsüberprüfung • Zentrale Quarantänewiederherstellung • Spyware/Grayware-Wiederherstellung

TABELLE 14-13. Menüelemente für "Updates"

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Updates	Zusammenfassung	n. v.
	Agents	Manuelles Update

TABELLE 14-14. Menüelemente für "Administration"

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Administration	Benachrichtigungen	Administrator

Benutzerdefinierte Rollen importieren oder exportieren

Prozedur

1. Navigieren Sie zu **Administration** > **Kontenverwaltung** > **Benutzerrollen**.
2. So exportieren Sie benutzerdefinierte Rollen in eine `.dat`-Datei, die Sie auf einem anderen OfficeScan Server wieder importieren können:
   a. Wählen Sie die Rollen aus und klicken Sie auf **Exportieren** > **In DAT-Datei exportieren**.
   b. Speichern Sie die `.DAT`-Datei. Wenn Sie einen anderen OfficeScan Server verwalten, können Sie mit Hilfe dieser `.DAT`-Datei benutzerdefinierte Rollen auf diesen Server importieren.

   Hinweis
   Rollen können nur zwischen Servern derselben Version exportiert werden.
3. Benutzerdefinierte Rollen in eine `.CSV`-Datei exportieren:
   a. Wählen Sie die Rollen aus und klicken Sie auf **Exportieren** > **In CSV-Datei exportieren**.
   b. Speichern Sie die `.CSV`-Datei. Verwenden Sie diese Datei, um die Informationen und Berechtigungen für die ausgewählten Rollen zu ermitteln.
4. Wenn Sie benutzerdefinierte Rollen von einem anderen OfficeScan Server gespeichert haben und diese Rollen in den aktuellen OfficeScan Server importieren möchten, klicken Sie auf **Importieren**, und navigieren Sie zur `.DAT`-Datei mit den benutzerdefinierten Rollen.

- Eine Rolle im Fenster "Benutzerrollen" wird überschrieben, wenn eine Rolle mit dem gleichen Namen importiert wird.
- Rollen können nur zwischen Servern derselben Version importiert werden.
- Eine Rolle, die von einem anderen OfficeScan Server importiert wurde:
  - Speichert die Berechtigungen für Menüelemente für Server/Agents und für Menüelemente für verwaltete Domänen.
  - Wendet die Standardberechtigungen auf die Menüelemente der Agent-Verwaltung an. Erfasst die Berechtigungen der Rolle für die Menüelemente der Agent-Verwaltung auf dem anderen Server und wendet sie dann wieder auf die Rolle an, die dort importiert wurde.

Trend Micro Control Manager

Trend Micro™ Control Manager™ ist eine zentrale Management-Konsole zur Verwaltung von Produkten und Diensten von Trend Micro auf Gateways, Mail-Servern, File-Servern und Unternehmensdesktops. Die webbasierte Management-Konsole des Control Managers bietet einen zentralen Überwachungspunkt für verwaltete Produkte und Services im gesamten Netzwerk.

Mit dem Control Manager kann der Systemadministrator Aktivitäten, wie auftretende Virenausbrüche, Sicherheitsverstöße oder mögliche Vireneintrittsstellen, überwachen und aufzeichnen. Der Systemadministrator kann Update-Komponenten herunterladen und im Netzwerk verteilen und somit einen einheitlichen und aktuellen Schutz gewährleisten. Mit Control Manager können manuelle und zeitgesteuerte Updates durchgeführt und Produkte in Gruppen oder einzeln konfiguriert und verwaltet werden.

Integration von Control Manager in dieser Version von OfficeScan

Diese Version von OfficeScan beinhaltet die folgenden Funktionen und Fähigkeiten bei der Verwaltung der OfficeScan Server vom Control Manager aus:

- Erstellen, verwalten und verteilen Sie Richtlinien für OfficeScan Antivirus, die Funktion "Prävention vor Datenverlust" und die Gerätesteuerung, und weisen Sie OfficeScan Agents von der Control Manager-Konsole aus direkt Berechtigungen zu.

  Die folgende Tabelle enthält die in Control Manager 6.0 SP3 Patch 2 verfügbaren Richtlinienkonfigurationen.

TABELLE 14-15. OfficeScan Richtlinienverwaltungtypen inControl Manager

RICHTLINIENTYP	FUNKTIONEN
OfficeScan Antivirus- und Agent-Einstellungen	• Zusätzliche Diensteinstellungen • Einstellungen der Verhaltensüberwachung • Einstellungen der Gerätesteuerung • Einstellungen für manuelle Suche • Einstellungen für "Vorausschauendes Maschinenlernen" • Berechtigungen und andere Einstellungen • Einstellungen für Echtzeitsuche • Exemplar Zusendung • Suchmethoden • Einstellungen für Jetzt durchsuchen • Einstellungen für die zeitgesteuerte Suche • Liste der zugelassenen Spyware/ Grayware • Verdächtige Verbindungseinstellungen • Liste der vertrauenswürdigen Programme • Update-Agent-Einstellungen • Web-Reputation-Einstellungen

RICHTLINIENTYP	FUNKTIONEN
Datenschutz	Einstellungen der Richtlinien für 'Prävention vor Datenverlust' **Hinweis** Verwalten Sie die Gerätesteuerungsberechtigungen für den Datenschutz in den OfficeScan Agent-Richtlinien.

Weitere Informationen über die Migration von OfficeScan Agent Richtlinieneinstellungen auf den Control Manager Server finden Sie unter *Das Einstellungsexporttool von OfficeScan auf Seite 14-33*.

- Die folgenden Einstellungen von einem OfficeScan Server auf einen anderen von der Control Manager Konsole aus replizieren:
  - *Datenbezeichnertypen auf Seite 11-6*
  - *Vorlagen für 'Prävention vor Datenverlust' auf Seite 11-22*

Hinweis

Werden diese Einstellungen auf OfficeScan Server repliziert, auf dem die Lizenz für den Datenschutz nicht aktiviert wurde, werden die Einstellungen nur wirksam, wenn die Lizenz aktiviert wird.

Unterstützte Versionen von Control Manager

Diese Version von OfficeScan unterstützt die folgenden Versionen von Control Manager:

- Control Manager 6.0 SP3 Patch 2 oder höher

Weitere Informationen zu den IP-Adressen, die OfficeScan Server und OfficeScan Agents Agents an Control Manager melden, finden Sie unter *Fenster, auf denen IP-Adressen angezeigt werden auf Seite A-7*.

Übernehmen Sie die aktuellen Patches und kritischen Hotfixes für diese Control Manager Versionen, damit der Control Manager OfficeScan verwalten kann. Die neuesten Patches und Hotfixes erhalten Sie von Ihrem Support-Anbieter oder vom Trend Micro Update Center unter:

http://www.trendmicro.com/download/emea/?lng=de

Führen Sie nach der Installation von OfficeScan eine Registrierung bei Control Manager durch, und konfigurieren Sie anschließend die Einstellungen für OfficeScan auf der Management-Konsole von Control Manager. Informationen zur Verwaltung von OfficeScan Servern finden Sie unter *Control Manager Dokumentation*.

OfficeScan beim Control Manager registrieren

Wichtig

Nach der Aktualisierung auf OfficeScan XG oder höher von OfficeScan 10.6 SP3 oder früher müssen Sie die Registrierung der Verbindung mit dem Control Manager Server aufheben und die Verbindung erneut registrieren, wenn Sie Zertifikatsautorisierung verwenden möchten.

Prozedur

1. Navigieren Sie zu **Administration** > **Einstellungen** > **Control Manager**.
2. Geben Sie den Anzeigename des Elements an, bei dem es sich um den Namen des OfficeScan Servers handelt, der im Control Manager angezeigt wird.

   Standardmäßig besteht der Anzeigename des Elements aus dem Host-Namen des Servers und dem Namen dieses Produkts (z. B. Server01_OSCE).

   Hinweis

   In Control Manager werden OfficeScan Server und andere von Control Manager verwaltete Produkte als "Elemente" bezeichnet.

3. Geben Sie den FQDN oder die IP-Adresse und die Portnummer des Control Manager Servers für die Verbindung mit diesem Server an. Optional kann die Verbindung auch über HTTPS (mit strengeren Sicherheitsauflagen) erfolgen.

- Bei einem Dual-Stack OfficeScan Server geben Sie den Control Manager FQDN oder die IP-Adresse (IPv4 oder IPv6, wenn verfügbar) ein.
- Bei einem reinen IPv4 OfficeScan Server geben die den Typ des Control Managers FQDN oder die IPv4-Adresse ein.
- Bei einem reinen IPv6 OfficeScan Server geben die den Typ des Control Manager FQDN oder die IPv6-Adresse ein.

4. Klicken Sie neben **Control Manager-Zertifikat** auf **Durchsuchen...** und wählen Sie die Zertifikatsdatei aus, die vom Control Manager Zielserver heruntergeladen wurde.

   Um die Control Manager Zertifikatsdatei zu erhalten, wechseln Sie zum Control Manager Server und kopieren Sie die Zertifikatsdatei auf den OfficeScan Server an folgendem Speicherort:

   ```
   <Control Manager installation folder>\Certificate\CA
   \TMCM_CA_Cert.pem
   ```

   Wichtig

   Wenn Ihr Unternehmen ein benutzerdefiniertes Zertifikat auf dem Control Manager Server verwendet, müssen Sie das Stammzertifikat des Zertifikatsausstellers während der Control Manager Registrierung hochladen.

   Weitere Informationen finden Sie unter *Autorisierung von Control Manager-Zertifikaten auf Seite 14-31*.

5. Erfordert der IIS Webserver des Control Manager eine Authentifizierung, geben Sie den Benutzernamen und das Kennwort ein.

6. Wird die Verbindung zum Control Manager Server über einen Proxy-Server hergestellt, geben Sie die folgenden Proxy-Einstellungen an:

   - Proxy-Protokoll
   - Server FQDN oder IPv4-/IPv6-Adresse und Port
   - Benutzerkennung und Kennwort für die Authentifizierung am Proxy-Server

7. Entscheiden Sie, ob Sie die Ein-Wege- oder Zwei-WegePort-Weiterleitung verwenden möchten, und geben Sie anschließend die IPv4/IPv6-Adresse und den Port an.

8. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob OfficeScan mit den angegebenen Einstellungen eine Verbindung zum Control Manager Server herstellen kann.

   Klicken Sie auf **Registrieren**, wenn die Verbindung erfolgreich aufgebaut wurde.

9. Wenn der Control Manager Server Version 6.0 SP1 oder höher aufweist, wird eine Meldung angezeigt, ob der Control Manager Server als Update-Adresse für den in OfficeScan integrierten Smart Protection Server verwendet werden soll. Klicken Sie auf **OK**, um den Control Manager Server als Update-Adresse für den integrierten Smart Protection Server zu verwenden, oder klicken Sie auf **Abbrechen**, um weiterhin die aktuelle Update-Adresse zu verwenden (standardmäßig der ActiveUpdate Server).

10. Werden die Einstellungen in diesem Fenster nach der Registrierung geändert, klicken Sie auf **Update-Einstellungen**, um den Control Manager Server über die Änderungen zu informieren.

Hinweis

Wenn der Control Manager-Server mit Deep Discovery verbunden ist, startet der automatische Abonnementvorgang nach abgeschlossener Registrierung. Weitere Informationen finden Sie unter *Einstellungen für Liste der verdächtigen Objekte auf Seite 14-38*.

11. Klicken Sie auf **Registrierung aufheben**, wenn OfficeScan nicht mehr vom Control Manager Server verwaltet werden soll.

Autorisierung von Control Manager-Zertifikaten

Vor der Registrierung von OfficeScan am Control Manager Server müssen Sie zuerst die Control Manager Zertifikatsdatei vom Control Manager Server aus folgendem Speicherort herunterladen:

```
<Installationsordner des Control Managers>\Certificate\CA
\TMCM_CA_Cert.pem
```

OfficeScan und Control Manager verwenden das Zertifikat und die Verschlüsselung mit öffentlichen Schlüsseln, um sicherzustellen, dass zwischen den Servern ausschließlich autorisierter Informationsaustausch zur Registrierung und Richtlinienverwaltung entsteht. Erkennt einer der Server nicht autorisierten Informationsaustausch, weist der jeweilige Server alle eingehenden Registrierungs- oder Richtlinieneinstellungen zurück.

Wichtig

Wenn Ihr Unternehmen ein benutzerdefiniertes Zertifikat auf dem Control Manager Server verwendet, müssen Sie das Stammzertifikat des Zertifikatsausstellers während der Control Manager Registrierung hochladen.

Den OfficeScan Status auf der Control Manager Management-Konsole überprüfen

Prozedur

1. Öffnen Sie die Control Manager Management-Konsole.

   Um die Control Manager Konsole auf einem Endpunkt im Netzwerk zu öffnen, öffnen Sie einen Webbrowser und geben Sie Folgendes ein:

   ```
   https://<Name des Control Manager Servers>/Webapp/
   login.aspx
   ```

   `<Name des Control Manager Servers>` steht für die IP-Adresse oder den Host-Namen des Control Manager Servers.

2. Klicken Sie im Hauptmenü auf **Verzeichnisse** > **Produkte**.

3. Navigieren Sie in der angezeigten Hierarchie zum Ordner **[Control Manager Server]** > **Lokaler Ordner** > **Neue Entität**.

4. Überprüfen Sie, ob das Symbol des OfficeScan Servers angezeigt wird.

Das Einstellungsexporttool von OfficeScan

OfficeScan beinhaltet das Einstellungsexporttool von OfficeScan, mit dem Administratoren OfficeScan Einstellungen aus früheren OfficeScan Versionen in die aktuelle Version übertragen können. Mit dem Einstellungsexporttool von OfficeScan werden folgende Einstellungen übertragen:

FUNKTION	MIGRIERTE EINSTELLUNGEN
Agent-Verwaltung **Hinweis** Das Einstellungsexporttool von OfficeScan migriert die entsprechenden Agent-Verwaltungs-Einstellungen zu den Paketen `OfficeScan_Agent_DLP_Policies.zip` und `OfficeScan_Agent_Policies.zip`, die während des Imports auf einen Control Manager Server verwendet werden.	• Manuelle Suche • Zeitgesteuerte Suche • Echtzeitsuche • Jetzt durchsuchen • Suchmethode • Web Reputation • Verhaltensüberwachung • Gerätesteuerung • Prävention vor Datenverlust • Berechtigungen und andere Einstellungen • Zusätzliche Diensteinstellungen • Liste der zugelassenen Spyware/Grayware • Vorausschauendes Maschinenlernen • Verdächtige Verbindung • Liste der vertrauenswürdigen Programme **Hinweis** • Das Server-Migrationstool migriert die Datensicherungsverzeichnisse für Manuelle Suche, Zeitgesteuerte Suche, Echtzeitsuche und „Jetzt durchsuchen“ nicht. • Einstellungen werden sowohl auf Stamm- als auch auf Domänenebene beibehalten.

FUNKTION	MIGRIERTE EINSTELLUNGEN
Agent-Gruppierung	Alle Einstellungen **Hinweis** Die Active-Directory-Domänenstrukturen werden nach dem ersten Synchronisieren mit Active Directory angezeigt.
Globale Agent-Einstellungen	Alle Einstellungen
Endpunktspeicherort	• Einstellungen für Location Awareness • Gateway-IP- und MAC-Adressenlisten:
Prävention vor Datenverlust	• Datenbezeichner • Vorlagen
Firewall	• Richtlinien • Profile
Protokollwartung	Alle Einstellungen
Agent-Update-Adresse	• Agent-Update-Adresse • Liste der benutzerdefinierten Update-Adressen
Smart Protection Quellen	Liste der Smart Protection Quellen
Benachrichtigungen	• Allgemeine Benachrichtigungseinstellungen • Einstellungen für die Administratorbenachrichtigungen • Einstellungen für die Ausbruchsbenachrichtigungen • Einstellungen für Agent-Benachrichtigungen
Proxy	Alle Einstellungen
Inaktive Agents	Alle Einstellungen
Quarantäne-Manager	Alle Einstellungen

FUNKTION	MIGRIERTE EINSTELLUNGEN
Webkonsole	Alle Einstellungen
`ofcscan.ini`-Einstellungen	• [INI_CLIENT_INSTALLPATH_SECTION] WinNT_InstallPath • [INI_REESTABLISH_COMMUNICATION_SECTION]: Alle Einstellungen
`ofcserver.ini`-Einstellungen	[INI_SERVER_DISK_THRESHOLD]: Alle Einstellungen

Hinweis

- Das Tool erstellt keine Sicherungskopien der OfficeScan Agent-Liste für die OfficeScan Server, sondern nur der Domänenstrukturen.
- OfficeScan Agentmigriert nur die Funktionen der älteren Version des OfficeScan Agent-Servers. Für Funktionen, die auf dem älteren Server nicht verfügbar sind, verwendet OfficeScan Agent die Standardeinstellungen.

Verwenden des Einstellungsexporttools von OfficeScan

Hinweis

Diese Version von OfficeScan unterstützt die folgenden Migrationen:

- Lokale OfficeScan-Server: Ab OfficeScan Version 10.6 Service Pack 3 und höher
- OfficeScan SaaS-Server: Ab OfficeScan Version XG Service Pack 1

Eine vollständige Liste der vom Einstellungsexporttool von OfficeScan migrierten Einstellungen finden Sie unter *Das Einstellungsexporttool von OfficeScan auf Seite 14-33*.

Ältere Versionen von OfficeScan enthalten möglicherweise nicht alle Einstellungen, die in der aktuellen Version verfügbar sind. OfficeScan wendet für alle Funktionen, die nicht aus der früheren OfficeScan Server-Version migriert werden, automatisch die Standardeinstellungen an.

Prozedur

1. Suchen Sie nach dem Server-Migrationstool-Paket.

   - Navigieren Sie in der OfficeScan Webkonsole zu **Administration** > **Einstellungen** > **Server-Migration** und klicken Sie auf den Link **Einstellungsexporttool von OfficeScan herunterladen**.
   - Navigieren Sie auf dem OfficeScanXG Service Pack 1 Servercomputer zu <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\PolicyExportTool`.

2. Kopieren Sie das Einstellungsexporttool von OfficeScan auf den OfficeScan Server-Computer, der als Quelle fungiert.

   Wichtig

   Sie müssen das XG Service Pack 1 OfficeScan Einstellungsexporttool von OfficeScan auf der Version des OfficeScan Quellservers verwenden, um sicherzustellen, dass das Format aller Daten für den neuen Zielserver korrekt ist. OfficeScanXG Service Pack 1 ist nicht mit älteren Versionen des Server Migration Tools kompatibel.

3. Doppelklicken Sie auf `OfficeScanSettingsExportTool.exe`, um das Einstellungsexporttool von OfficeScan zu starten.

   Das Einstellungsexporttool von OfficeScan wird ausgeführt.

   Hinweis

   Die Standardnamen des Exportpakets lauten:

   - `OfficeScan_Agent_DLP_Policies.zip` (zum Importieren der DLP-Richtlinieneinstellungen in Control Manager verwendet)
   - `OfficeScan_Agent_Policies.zip` (zum Importieren aller anderen OfficeScan Agent Richtlinieneinstellungen in Control Manager verwendet)
   - `OfficeScan_Server_Migration.zip` (zum Importieren aller OfficeScan Agent Richtlinieneinstellungen und OfficeScan Servereinstellungen in andere lokale oder OfficeScan Cloud-Konsolenserver verwendet)

4. Kopieren Sie das Exportpaket in einen Speicherort, auf den der OfficeScan oder Control Manager-Server zugreifen kann.

5. So importieren Sie die Einstellungen in den neuen OfficeScan Zielserver:

   a. Navigieren Sie in der OfficeScan Webkonsole zu **Administration** > **Einstellungen** > **Server-Migration** und klicken Sie auf die Schaltfläche **Einstellungen importieren...**.

   b. Suchen Sie das `OfficeScan_Server_Migration.zip`-Paket und klicken Sie auf **Öffnen**.

   c. Vergewissern Sie sich, dass der Server alle Einstellungen aus der früheren OfficeScan Version enthält.

6. So importieren Sie die OfficeScan Agent Richtlinieneinstellungen in die Control Manager Zielkonsole:

   a. Navigieren Sie auf der Control Manager Webkonsole zu **Richtlinien** > **Richtlinienverwaltung**.

   b. Wählen Sie im Listenfeld **Produkt** die Option **OfficeScan Agent** aus.

   c. Klicken Sie auf **Einstellungen importieren**.

   d. Suchen Sie das `OfficeScan_Agent_Policies.zip`-Paket und klicken Sie auf **Öffnen**.

7. So importieren Sie die OfficeScan Agent DLP-Richtlinieneinstellungen in die Control Manager Zielkonsole:

   a. Navigieren Sie auf der Control Manager Webkonsole zu **Richtlinien** > **Richtlinienverwaltung**.

   b. Wählen Sie im Listenfeld **Produkt** die Option **OfficeScan Prävention vor Datenverlust** aus.

   c. Klicken Sie auf **Einstellungen importieren**.

   d. Suchen Sie das `OfficeScan_Agent_DLP_Policies.zip`-Paket und klicken Sie auf **Öffnen**.

8. Verschieben Sie die alten OfficeScan Agents auf den neuen OfficeScan Server.

Weitere Informationen zum Verschieben von OfficeScan Agents finden Sie unter *OfficeScan Agenten in eine andere Domäne oder auf einen anderen OfficeScan Server verschieben auf Seite 2-63* oder *Agent Mover auf Seite 15-24*.

Einstellungen für Liste der verdächtigen Objekte

Verdächtige Objekte sind digitale Elemente als Ergebnis einer Analyse, die von Trend Micro Deep Discovery-Produkten oder anderen Quellen abgeschlossen wurde. OfficeScan kann verdächtige Objekte synchronisieren und Aktionen für diese Objekte über einen lokalen Server mit TMCM 6.0 SP3 Patch 2 oder höher abrufen, der mit Deep Discovery verbunden ist.

Wählen Sie nach dem Abonnieren von Control Manager die Typen der verdächtigen Objekte aus, um C&C-Callbacks oder möglicherweise gezielte Angriffe zu überwachen, die von Agents im Netzwerk identifiziert wurden. Verdächtige Objekte beinhalten:

- Liste der verdächtigen URLs
- Liste der verdächtigen IPs
- Liste der verdächtigen Dateien
- Liste der verdächtigen Domänen

Hinweis

In OfficeScan 10.6 bis 11.0 stellt Deep Discovery Analyzer die primäre Quelle der verdächtigen Objekte dar. Ab OfficeScan 11.0 SP1 stellt Control Manager 6.0 SP3 die primäre Quelle dar, der ein zuverlässigeres Verfahren zur Verwaltung und Behandlung verdächtiger Objekte bietet.

Wenn OfficeScan für Deep Discovery Analyzer abonniert ist, ist nur die Liste der verdächtigen URLs verfügbar. Nachdem Sie das Abonnement von OfficeScan in Deep Discovery Analyzer gekündigt haben, ist ein erneutes Abonnieren nicht möglich. OfficeScan muss Control Manager abonnieren, der mit Deep Discovery verbunden ist, um verdächtige Objekte zu synchronisieren.

Weitere Informationen darüber, wie Control Manager verdächtige Objekte verwaltet, finden Sie im *Administratorhandbuch für Control Manager*.

Einstellungen für Liste der verdächtigen Objekte konfigurieren

Bei der OfficeScan-Registrierung bei einem lokalen Control Manager stellt Control Manager einen API-Schlüssel für OfficeScan bereit, um den Abonnementvorgang zu starten. Um diesen automatischen Abonnementvorgang zu aktivieren, setzen Sie sich mit dem Control Manager-Administrator in Verbindung, um sicherzustellen, dass Control Manager mit Deep Discovery verbunden ist und dass die erforderlichen Einstellungen konfiguriert sind.

Nähere Informationen zum Registrieren eines Control Manager Servers finden Sie unter *OfficeScan beim Control Manager registrieren auf Seite 14-29*.

Prozedur

1. Navigieren Sie zu **Administration** > **Einstellungen** > **Liste der verdächtigen Objekte**.
2. Wählen Sie aus, welche Liste Sie auf den Agents aktivieren möchten.
   - Liste der verdächtigen URLs
   - Liste der verdächtigen IP-Adressen (nur beim Abonnieren des registrierten Control Manager Servers verfügbar)

- Liste der verdächtigen Dateien (nur beim Abonnieren des registrierten Control Manager Servers verfügbar)
- Liste der verdächtigen Domänen (nur beim Abonnieren des registrierten Control Manager Servers verfügbar)

Administratoren können jederzeit eine manuelle Synchronisierung der Listen der verdächtigen Objekte vornehmen, indem sie auf die Schaltfläche **Jetzt synchronisieren** klicken.

3. Geben Sie unter **Liste der verdächtigen Objekte auf OfficeScan Agents aktualisieren** an, wenn Agents die Liste der verdächtigen Objekte aktualisieren.
   - **Basierend auf dem Aktualisierungszeitplan der OfficeScan Agent-Komponente**: OfficeScan Agents aktualisieren die Listen der verdächtigen Objekte basierend auf dem aktuellen Update-Zeitplan.
   - **Automatisch nach der Aktualisierung der Liste der verdächtigen Objekte auf dem Server**: OfficeScan Agents aktualisiert die Listen der verdächtigen Objekte automatisch, wenn der OfficeScan-Server die aktualisierten Listen erhält.

Hinweis

OfficeScan Agents, die nicht für den Empfang von Updates von Update-Agents konfiguriert sind, führen inkrementelle Updates der abonnierten Listen der verdächtigen Objekte während der Synchronisierung durch.

4. Klicken Sie auf **Speichern**.

Referenzserver

Eine der Möglichkeiten, wie der OfficeScan Agent ermittelt, welche Richtlinie bzw. welches Profil verwendet werden soll, besteht darin, den Verbindungsstatus mit dem OfficeScan Server zu prüfen. Wenn ein interner OfficeScan Agent (oder ein agent innerhalb des Unternehmensnetzwerks) keine Verbindung zum Server aufbauen kann, erhält der agent den Status "Offline". Der agent übernimmt anschließend die

gewünschte Richtlinie bzw. das gewünschte Profil für externe agents. Referenzserver lösen dieses Problem.

Ein OfficeScan Agent, dessen Verbindung zum OfficeScan Server getrennt wird, versucht sich mit einem Referenzserver zu verbinden. Wenn der agent die Verbindung mit einem Referenzserver hergestellt hat, wird die Richtlinie bzw. das Profil für interne agents übernommen.

Zu den von Referenzservern verwalteten Richtlinien und Profilen gehören:

- Firewall-Profile
- Web-Reputation-Richtlinien
- Datenschutzrichtlinien
- Gerätesteuerungsrichtlinien

Beachten Sie dabei Folgendes:

- Weisen Sie Computer mit Serverfunktionen, wie z. B. Webserver, SQL-Server oder FTP-Server, als Referenzserver zu. Es können maximal 320 Referenzserver angegeben werden.
- verbinden sich mit dem ersten Referenzserver in der Liste. Wenn die Verbindung nicht aufgebaut werden kann, versucht der agent, sich mit dem nächsten Server in der Liste zu verbinden.
- verwenden Referenzserver zum Ermitteln der zu verwendenden Antivirus-Einstellungen (Verhaltensüberwachung, Gerätesteuerung, Firewall-Profile, Web-Reputation-Richtlinie) bzw. Datenschutzeinstellungen. Referenzserver verwalten keine agents und verteilen keine Updates oder agent-Einstellungen. Diese Tasks führt der OfficeScan Server durch.
- Der OfficeScan Agent kann weder Protokolle an Referenzserver senden noch diese als Update-Adresse verwenden.

Liste der Referenzserver verwalten

Prozedur

1. Navigieren Sie zu **Agents** > **Firewall** > **Profile** oder **Agents** > **Endpunktspeicherort**.
2. Führen Sie je nach angezeigtem Fenster Folgendes aus:
   - Wenn Sie sich im Bildschirm **Firewall-Profile für Agents** befinden, klicken Sie auf **Liste der Referenzserver bearbeiten**.
   - Wenn Sie sich im Bildschirm **Endpunktspeicherort** befinden, klicken Sie auf **Liste der Referenzserver**.
3. Wählen Sie **Liste der Referenzserver aktivieren**.
4. Klicken Sie auf **Hinzufügen**, um einen Endpunkt zur Liste hinzuzufügen.
   a. Geben Sie die IPv4-/IPv6-Adresse des Endpunkts, den Namen oder den vollqualifizierten Domänennamen (FQDN) ein, wie beispielsweise:
      - `computer.networkname`
      - `12.10.10.10`
      - `mycomputer.domain.com`
   b. Geben Sie die Portnummer ein, über die die agents mit diesem Endpunkt kommunizieren. Sie können einen beliebigen offenen Port (z. B. die Ports 20, 23 oder 80) auf dem Referenzserver angeben.

      Hinweis

      Um für denselben Referenzserver eine weitere Portnummer festzulegen, wiederholen Sie die Schritte 2a und 2b. Der OfficeScan Agent verwendet die erste Portnummer in der Liste. Schlägt die Verbindung fehl, verwendet er die nächste Portnummer.

   c. Klicken Sie auf **Speichern**.

5. Klicken Sie auf den Endpunkt-Namen, um die Einstellungen eines Endpunkts in der Liste zu bearbeiten. Ändern Sie den Endpunkt-Namen oder Port und klicken Sie dann auf **Speichern**.

6. Um einen Endpunkt aus der Liste zu entfernen, wählen Sie den Endpunkt-Namen aus und klicken Sie auf **Löschen**.

7. Um die Funktion eines Endpunktes als Referenzserver zu aktivieren, klicken Sie auf **Den Agents zuweisen**.

Einstellungen für die Administratorbenachrichtigungen

Sie können die Einstellungen für die Benachrichtigung des Administrators konfigurieren, damit OfficeScan erfolgreich Benachrichtigungen per E-Mail und SNMP Trap senden kann. OfficeScan kann auch Benachrichtigungen über das Windows NT Ereignisprotokoll senden, es sind jedoch keine Einstellungen für diesen Benachrichtigungskanal konfiguriert.

OfficeScan kann Benachrichtigungen and Sie oder andere OfficeScan Administratoren senden, wenn folgendes entdeckt wurde:

TABELLE 14-16. Funde, die Administratorbenachrichtigungen auslösen

FUNDE	BENACHRICHTIGUNGSKANÄLE		
	E-MAIL	SNMP-TRAP	WINDOWS NT EREIGNISPROTOKOLLE
Viren und Malware	Ja	Ja	Ja
Spyware und Grayware	Ja	Ja	Ja
Übertragungen digitaler Assets	Ja	Ja	Ja
C&C-Callbacks	Ja	Ja	Ja

Funde	Benachrichtigungskanäle		
	E-Mail	SNMP-Trap	Windows NT Ereignisprotokolle
Viren- und Malware-Ausbrüche	Ja	Ja	Ja
Spyware- und Grayware-Ausbrüche	Ja	Ja	Ja
Ausbrüche bei Firewall-Verstoß	Ja	Nein	Nein
Ausbrüche bei Freigabesitzungen	Ja	Nein	Nein
C &C-Callback-Ausbrüche	Ja	Ja	Ja

Einstellungen für Allgemeine Benachrichtigungen konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Allgemeine Einstellungen**.
2. Konfigurieren Sie die Einstellungen für E-Mail-Benachrichtigungen.
   a. Geben Sie im Feld **SMTP-Server** den Namen des Endpunkts oder die IPv4- oder IPv6-Adresse des SMTP-Servers ein.
   b. Geben Sie den vom SMTP-Server verwendeten Port an.

      Gültige Portnummern liegen zwischen 1 und 65535.
   c. Geben Sie im Feld **Von** die E-Mail-Adresse an, die als Absender der Benachrichtigung angezeigt wird.

      Wenn Sie im nächsten Schritt ESMTP aktivieren möchten, geben Sie eine gültige E-Mail-Adresse an.

d. Wahlweise können Sie **ESMTP** aktivieren.

e. Geben Sie den Benutzernamen und das Kennwort für die E-Mail-Adresse an, die Sie im Feld **Von** angegeben haben.

f. Wählen Sie eine Methode für die Agent-Authentifizierung beim Server:

- **Anmeldung**: "Anmeldung" ist eine ältere Variante des Mail User Agent. Server und Agent verwenden beide BASE64 für die Authentifizierung des Benutzernamens und des Kennworts.
- **Einfacher Text**: "Einfacher Text" ist am benutzerfreundlichsten zu verwenden, jedoch nicht besonders sicher, da Benutzername und Kennwort als Zeichenfolge gesendet werden. Bevor sie über das Internet gesendet werden, werden sie BASE64-kodiert.
- **CRAM-MD5**: CRAM-MD5 kombiniert ein Challenge-Response-Verfahren mit einem kryptographischem MD5-Algorithmus für den Austausch und die Authentifizierung von Informationen.

3. Konfigurieren Sie die Einstellungen für SNMP-Trap-Benachrichtigungen.

a. Geben Sie im Feld **IP-Adresse des Servers** entweder eine IPv4-/IPv6-Adresse oder einen Endpunktnamen an.

b. Geben Sie einen schwer zu erratenden Community-Namen ein.

Hinweis

Aus Sicherheitsgründen wird der Community-Name unter Verwendung eines Sternchens (*) als maskierter Wert angezeigt. Der zugewiesene Standardwert lautet: „öffentlich“.

4. Klicken Sie auf **Speichern**.

Systemereignisprotokolle

OfficeScan protokolliert Ereignisse im Zusammenhang mit dem Serverprogramm, wie beispielsweise Hoch- und Herunterfahren. Anhand dieser Protokolle können Sie überprüfen, ob der OfficeScan Server und die Dienste einwandfrei funktionieren.

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell, oder konfigurieren Sie eine zeitgesteuerte Löschung der Protokolle. Weitere Informationen zur Protokollverwaltung finden Sie unter *Protokollmanagement auf Seite 14-47*.

Systemereignisprotokolle anzeigen

Prozedur

1. Navigieren Sie zu **Protokolle** > **Systemereignisse**.
2. Suchen Sie unter **Ereignis** nach Protokollen, die weitere Aktionen erfordern. OfficeScan protokolliert die folgenden Ereignisse:

TABELLE 14-17. Systemereignisprotokolle

PROTOKOLLTYP	EREIGNISSE
OfficeScan Master Service und Datenbankserver	• Master Service gestartet • Der Master Service wurde beendet. • Der Master Service konnte nicht beendet werden.
Ausbruchsprävention	• Ausbruchsprävention aktiviert • Ausbruchsprävention deaktiviert • Anzahl der Netzwerkzugriffe auf Freigabeordner in den letzten <Minutenanzahl>
Datenbanksicherung	• Datenbanksicherung erfolgreich • Datenbank-Backup fehlgeschlagen
Rollenbasierter Zugriff auf die Webkonsole	• Anmeldung an der Konsole • Kennwortänderung • Abmeldung von der Konsole • Zeitüberschreitung der Sitzung (der Benutzer wird automatisch abgemeldet)

PROTOKOLLTYP	EREIGNISSE
Serverauthentifizierung	• Der OfficeScan Agent hat vom Server ungültige Befehle erhalten. • Ungültiges oder abgelaufenes Authentifizierungszertifikat
Virtual Analyzer	• Exemplar zur Analyse gesendet • Exemplaranalyse abgeschlossen • Virtual Analyzer hat eine vorherige doppelte Zusendung eines Exemplars von einem anderen verbundenen OfficeScan Server erkannt.

3. Wenn Sie das Protokoll als komma-separierte Datei (`CSV-Datei`) speichern möchten, klicken Sie auf **In CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Protokollmanagement

OfficeScan führt umfangreiche Protokolle über entdeckte Sicherheitsrisiken, Updates und andere wichtige Ereignisse und Vorgänge. Mit Hilfe dieser Protokolle können Sie die Virenschutzrichtlinien Ihres Unternehmens bewerten und OfficeScan Agents ermitteln, die einem höheren Infektions- oder Angriffsrisiko ausgesetzt sind. Sie können anhand dieser Protokolle auch die Verbindung der agents zum Server überprüfen und feststellen, ob Komponenten-Updates erfolgreich durchgeführt wurden.

OfficeScan setzt außerdem eine Methode zur zentralen Zeitüberprüfung ein, um eine einheitliche Zeit zwischen OfficeScan Server und den agents zu gewährleisten. Das verhindert inkonsistente Protokolldaten, die durch Zeitzonen, Sommerzeit und Zeitunterschiede verursacht wurdenund beim Lesen der Protokolle für Verwirrung sorgen könnten.

Hinweis

OfficeScan führt die Zeitüberprüfung für alle Protokolle durch, mit Ausnahme der Server-Update- und Systemereignisprotokolle.

Der OfficeScan Server erhält die folgenden Protokolle von den OfficeScan Agents:

- *Viren-/Malware-Protokolle anzeigen auf Seite 7-101*
- *Spyware/Grayware-Protokolle anzeigen auf Seite 7-110*
- *Spyware-/Grayware-Wiederherstellungsprotokolle anzeigen auf Seite 7-114*
- *Firewall-Protokolle anzeigen auf Seite 13-33*
- *Web-Reputation-Protokolle anzeigen auf Seite 12-23*
- *Protokolle zu verdächtigen Verbindungen anzeigen auf Seite 8-17*
- *Protokolle zu verdächtigen Dateien anzeigen auf Seite 7-115*
- *C&C Callback-Protokolle anzeigen auf Seite 12-25*
- *Verhaltensüberwachungsprotokolle anzeigen auf Seite 9-25*
- *Anzeigen von Protokolldaten für "Vorausschauendes Maschinenlernen" auf Seite 8-13*
- *Protokolle der Gerätesteuerung anzeigen auf Seite 10-20*
- *Protokolle zu Suchvorgängen anzeigen auf Seite 7-116*
- *Protokolle der Funktion "Prävention vor Datenverlust" anzeigen auf Seite 11-63*
- *OfficeScan Agent Update-Protokolle anzeigen auf Seite 6-55*
- *Verbindungsüberprüfungsprotokolle anzeigen auf Seite 15-48*

Der OfficeScan Server erstellt die folgenden Protokolle:

- *OfficeScan Server-Update-Protokolle auf Seite 6-28*
- *Systemereignisprotokolle auf Seite 14-45*

Die folgenden Protokolle sind auch auf dem OfficeScan Server und den OfficeScan Agents verfügbar:

- *Windows Ereignisprotokolle auf Seite 18-26*
- *OfficeScan Serverprotokolle auf Seite 18-3*

- *OfficeScan Agent Protokolle auf Seite 18-15*

Protokollwartung

Damit die Protokolle nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell, oder konfigurieren Sie von der Webkonsole aus ein zeitgesteuertes Löschen der Protokolle.

Protokolle nach einem Zeitplan löschen

Prozedur

1. Navigieren Sie zu **Protokolle** > **Protokollwartung**.
2. Wählen Sie **Zeitgesteuertes Löschen von Protokollen aktivieren**.
3. Wählen Sie die Protokollarten aus, die gelöscht werden sollen. Alle von OfficeScan erstellten Protokolle, mit Ausnahme von Debug-Protokollen, können zeitgesteuert gelöscht werden. Im Fall von Debug-Protokollen deaktivieren Sie die Debug-Protokollierung, um die Erfassung von Protokollen anzuhalten.

   Hinweis

   Bei Viren-/Malware-Protokollen können Sie Protokolle, die von bestimmten Suchtypen und Damage Cleanup Services erstellt wurden, löschen. Bei Spyware-/Grayware-Protokollen können Sie Protokolle von bestimmten Suchtypen löschen. Weitere Informationen über Suchtypen finden Sie unter *Suchtypen auf Seite 7-16*.

4. Wählen Sie aus, ob alle Protokolle der angegebenen Protokollarten oder nur diejenigen gelöscht werden sollen, die älter als eine bestimmte Anzahl von Tagen sind.
5. Geben Sie Startzeitpunkt und Zeitintervall für die Protokolllöschung an.
6. Klicken Sie auf **Speichern**.

Protokolle manuell löschen

Prozedur

1. Navigieren Sie zu **Protokolle** > **Agents** > **Sicherheitsrisiken** oder **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Führen Sie einen der folgenden Schritte durch:
   - Wenn Sie auf das Fenster **Sicherheitsrisiko-Protokolle** zugreifen, klicken Sie auf **Protokolle löschen**.
   - Wenn Sie auf das Fenster **Agent-Verwaltung** zugreifen, klicken Sie auf **Protokolle** > **Protokolle löschen**.
4. Wählen Sie unter **Zu löschende Protokolltypen** den Typ der Protokolldaten aus, die entfernt werden sollen:
   - Verhaltensüberwachungsprotokolle
   - C&C-Callback-Protokolle
   - Protokolle für 'Prävention vor Datenverlust'
   - Protokolle der Gerätesteuerung
   - Firewall-Protokolle
   - Protokolldaten für "Vorausschauendes Maschinenlernen"
   - Spyware-/Grayware-Protokolle
   - Protokolle zu Suchvorgängen
   - Protokolle zu verdächtigen Verbindungen
   - Protokolle zu verdächtigen Dateien
   - Viren-/Malware-Protokolle

- Web-Reputation-Protokolle

Hinweis

Bei Viren-/Malware-Protokollen können Sie Protokolle, die von bestimmten Suchtypen und Damage Cleanup Services erstellt wurden, löschen. Bei Spyware-/Grayware-Protokollen können Sie Protokolle von bestimmten Suchtypen löschen.

Weitere Informationen über Suchtypen finden Sie unter *Suchtypen auf Seite 7-16*.

5. Wählen Sie unter **Zu löschende Protokolle** eine der folgenden Optionen aus:
   - **Alle Protokolle des ausgewählten Protokolltyps**: Löscht alle Protokolldaten für die ausgewählten Protokolltypen.
   - **Protokolle, die älter sind als XX Tage**: Löscht alle Protokolldaten, die älter sind als die Anzahl Tage, die für die ausgewählten Protokolltypen angegeben wurden.
6. Klicken Sie auf **Löschen**.

Lizenzen

Sie können die OfficeScan Lizenz auf der Webkonsole anzeigen, aktivieren und verlängern sowie die OfficeScan Firewall aktivieren bzw. deaktivieren. Die OfficeScan Firewall ist Teil des Virenschutzes, der auch die Unterstützung für die Ausbruchsprävention umfasst.

Hinweis

Einige native OfficeScan Funktionen, wie Data Protection und Virtual Desktop Support, sind gesondert lizenziert. Die Lizenzen für diese Funktionen werden über den Plug-in-Manager aktiviert und verwaltet. Weitere Informationen über die Lizenzierung dieser Funktionen finden Sie unter *Datenschutzlizenz auf Seite 3-4* und *Virtual Desktop Support Lizenz auf Seite 15-87*.

Ein reiner IPv6 OfficeScan Server kann keine Verbindung mit dem Trend Micro Online-Registrierungsserver herstellen, um die Lizenz zu aktivieren oder zu verlängern. Ein Dual-Stack-Proxy-Server, der IP-Adressen konvertieren kann wie DeleGate, muss ermöglichen, dass der OfficeScan Server eine Verbindung zum Registrierungsserver herstellen kann.

Produktlizenzinformationen anzeigen

Prozedur

1. Navigieren Sie zu **Administration** > **Einstellungen** > **Produktlizenz**.
2. Oben im Fenster wird eine Zusammenfassung zum Lizenzstatus angezeigt. In folgenden Fällen werden Hinweise zu Lizenzen angezeigt:

TABELLE 14-18. Lizenzerinnerung

LIZENZTYP	ERINNERUNG
Vollversion	• Während der Übergangsfrist des Produkts. Die Dauer der Übergangsfrist ist regional verschieden. Erkunden Sie sich bei Ihrem Trend Micro Vertriebspartner über die Länge der Übergangsfrist. • Bei Ablauf der Lizenz und der Übergangsfrist. Innerhalb dieses Zeitraums erhalten Sie keinen technischen Support und können keine Komponenten-Updates durchführen. Die Scan Engines durchsuchen die Endpunkte, jedoch unter Verwendung nicht aktueller Komponenten. Diese veralteten Komponenten schützen Sie möglicherweise nicht vollständig vor den aktuellen Sicherheitsrisiken.

LIZENZTYP	ERINNERUNG
Testversion	Bei Ablauf der Lizenz Währenddessen deaktiviert OfficeScan Komponenten-Updates. Die Scan Engines durchsuchen die Endpunkte, jedoch unter Verwendung nicht aktueller Komponenten. Diese veralteten Komponenten schützen Sie möglicherweise nicht vollständig vor den aktuellen Sicherheitsrisiken.

3. Sie können sich die Lizenzinformationen ansehen. Der Abschnitt **Lizenzinformationen** enthält folgende Informationen:

   - **Dienste**: Umfasst alle OfficeScan Lizenzdienste
   - **Status**: Wird entweder als "Aktiviert", "Nicht aktiviert" oder "in Übergangsfrist" angezeigt. Verfügt ein Dienst über mehrere Lizenzen, und ist mindestens eine Lizenz noch immer aktiviert, wird der Status "Aktiviert" angezeigt.
   - **Version**: Wird entweder als "Vollversion" oder "Testversion" angezeigt. Wenn Sie die Voll- und die Testversion besitzen, wird "Vollversion" angezeigt.
   - **Ablaufdatum**: Verfügt ein Service über mehrere Lizenzen, wird das am weitesten in der Zukunft liegende Ablaufdatum angezeigt. Laufen die Lizenzen am 31.12.2007 und am 30.06.2008 ab, wird das Datum 30.06.2008 angezeigt.

   Hinweis

   Bei nicht aktivierten Lizenz-Diensten wird als Version und Ablaufdatum der Wert "N/V" angezeigt.

4. OfficeScan ermöglicht Ihnen die Aktivierung mehrerer Lizenzen für einen Service. Um alle Lizenzen (aktive und abgelaufene) für diesen Dienst anzuzeigen, klicken Sie auf den Namen des Service.

Eine Lizenz aktivieren oder erneuern

Prozedur

1. Navigieren Sie zu **Administration** > **Einstellungen** > **Produktlizenz**.
2. Klicken Sie auf den Namen des Service.
3. Klicken Sie im geöffneten Fenster **Einzelheiten zur Produktlizenz** auf **Neuer Aktivierungscode**.
4. Geben Sie den Aktivierungscode in das daraufhin angezeigte Fenster ein, und klicken Sie auf **Speichern**.

   Hinweis

   Registrieren Sie einen Dienst, bevor Sie ihn aktivieren. Weitere Informationen über Registrierungsschlüssel und Aktivierungscode erhalten Sie bei Ihrem Trend Micro Vertriebspartner.

5. Klicken Sie im Fenster **Einzelheiten zur Produktlizenz** auf **Informationen aktualisieren**, um das Fenster mit den neuen Informationen über die Produktlizenz und den Status des Diensts zu aktualisieren. In diesem Fenster wird auch ein Link zur Trend Micro Website angezeigt, auf der Sie detaillierte Informationen über die Lizenz finden.

OfficeScan Datenbanksicherung

In der OfficeScan Serverdatenbank sind alle OfficeScan Einstellungen, einschließlich Sucheinstellungen und Berechtigungen, gespeichert. Bei Beschädigung der Serverdatenbank kann diese über die Sicherungskopie wiederhergestellt werden. Sie können die Datenbank jederzeit manuell sichern oder einen Zeitplan für die Datensicherung festlegen.

Beim Sichern der Datenbank wird diese von OfficeScan automatisch defragmentiert und eventuelle Schäden an der Index-Datei werden repariert.

Überprüfen Sie die Systemereignisprotokolle, um den Status der Datensicherung zu ermitteln. Weitere Informationen finden Sie unter *Systemereignisprotokolle auf Seite 14-45*.

Tipp

Trend Micro empfiehlt, einen Zeitplan für die automatische Sicherung festzulegen. Sichern Sie die Datenbank, wenn der Netzwerkverkehr gering ist.

Warnung!

Verwenden Sie für die Datensicherung kein anderes Tool und keine andere Software. Die Datenbanksicherung kann nur über die OfficeScan Webkonsole konfiguriert werden.

Die OfficeScan Datenbank sichern

Prozedur

1. Navigieren Sie zu **Administration** > **Einstellungen** > **Datenbanksicherung**.
2. Geben Sie an, wo die Datenbank gespeichert werden soll. Ist der gewünschte Ordner noch nicht vorhanden, wählen Sie **Ordner erstellen, falls nicht bereits vorhanden**. Geben Sie das Laufwerk und den vollständigen Verzeichnispfad an, wie z. B. `C:\OfficeScan\DatabaseBackup`.

   Der OfficeScan Standardspeicherort für die Datenbanksicherung lautet: <*Installationsordner des Servers*>`\DBBackup`

   Hinweis

   OfficeScan erstellt im Backup-Pfad einen Unterordner. Der Ordnername gibt den Zeitpunkt der Datensicherung an und hat folgendes Format: JJJJMMTT_HHMMSS. OfficeScan behält die sieben zuletzt erstellten Backup-Ordner bei und löscht automatisch ältere Ordner.
3. Befindet sich der Backup-Pfad (als UNC-Pfad) auf einem externen Computer, geben Sie den entsprechenden Kontonamen und das zugehörige Kennwort ein. Stellen Sie sicher, dass das Konto über Schreibrechte auf dem Computer verfügt.

4. Einen Zeitplan für die Datensicherung festlegen:

   a. Wählen Sie **Zeitgesteuerte Datenbanksicherung aktivieren**.

   b. Geben Sie den Startzeitpunkt und das Zeitintervall für die Datensicherung an.

   c. Klicken Sie zum Sichern der Datenbank und Speichern der vorgenommenen Änderungen auf **Jetzt sichern**. Wenn nur die vorgenommenen Änderungen gespeichert, aber nicht die Datenbank gesichert werden soll, klicken Sie auf **Speichern**.

Datenbanksicherungsdateien wiederherstellen

Prozedur

1. Beenden Sie den OfficeScan Master Service.
2. Überschreiben Sie die Datenbankdateien in <*Installationsordner des Servers*>`\PCCSRV\HTTPDB` mit den Sicherungsdateien.
3. Starten Sie den OfficeScan Master Service neu.

SQL Server Migration Tool

Administratoren können mit dem SQL Server Migration Tool die vorhandene OfficeScan Datenbank vom nativen CodeBase-Format zu einer SQL Server-Datenbank migrieren. Das SQL Server Migration Tool unterstützt die folgenden Datenbankmigrationen:

- OfficeScan CodeBase-Datenbank zu neuer SQL Server Express-Datenbank
- OfficeScan CodeBase-Datenbank zu vorhandener SQL Server-Datenbank
- OfficeScan SQL-Datenbank (zuvor migriert), die an einen anderen Speicherort verschoben wurde

SQL Server Migration Tool verwenden

Das SQL Server Migration Tool migriert die vorhandene CodeBase-Datenbank zu einer SQL-Datenbank unter Verwendung von SQL Server 2016 SP1 Express.

Tipp

Nach der Migration der OfficeScan Datenbank können Sie die zuletzt migrierte SQL-Datenbank in einen anderen SQL Server verschieben. Führen Sie das SQL Server Migration Tool erneut aus und wählen Sie **Zu einer vorhandenen OfficeScan SQL-Datenbank wechseln** aus, um den anderen SQL Server zu verwenden.

Prozedur

1. Navigieren Sie auf dem OfficeScan Server zu <*Server installation folder*>`\PCCSRV\Admin\Utility\SQL`.
2. Doppelklicken Sie auf die Datei `SQLTxfr.exe`, um das Tool auszuführen.

   Die **SQL Server Migration Tool**-Konsole wird geöffnet.
3. Wählen Sie den Migrationstyp aus:

OPTION	BEZEICHNUNG
Neue SQL Server 2016 SP1 Express-Instanz installieren/erstellen und OfficeScan Datenbank migrieren	Installiert SQL Server 2016 SP1 Express automatisch und migriert die vorhandene OfficeScan Datenbank zu einer neuen SQL-Datenbank. **Hinweis** OfficeScan weist den Port 1433 automatisch zum SQL Server zu.
OfficeScan-Datenbank zu einem vorhandenen SQL Server migrieren	Migriert die vorhandene OfficeScan-Datenbank zu einer neuen SQL-Datenbank auf einem vorhandenen SQL Server
Zu einer vorhandenen OfficeScan SQL-Datenbank wechseln	Ändert die OfficeScan Konfigurationseinstellungen, so dass auf eine vorhandene OfficeScan SQL-Datenbank auf einem vorhandenen SQL Server verwiesen wird

4. Geben Sie den **Servernamen** wie folgt an:

   - Für neue SQL-Installationen: <Hostname oder IP-Adresse des SQL Servers>\<Name der Instanz>
   - Für Migrationen des SQL Servers: <Hostname oder IP-Adresse des SQL Servers>,<Portnummer>\<Name der Instanz>
   - Beim Wechsel zu einer vorhandenen OfficeScan SQL-Datenbank: <Hostname oder IP-Adresse des SQL Servers>,<Portnummer>\<Name der Instanz>

Wichtig

OfficeScan erstellt automatisch eine Instanz für die OfficeScan Datenbank, wenn SQL Server installiert wird. Geben Sie beim Migrieren zu einem vorhandenen SQL Server oder einer vorhandenen Datenbank den bisher vorhandenen Instanznamen für die OfficeScan-Instanz auf dem SQL Server ein.

5. Geben Sie die Authentifizierungsdaten für die SQL Server-Datenbank ein.

   - Bei Verwendung des **Windows-Kontos** für die Anmeldung beim Server muss für den **Benutzernamen** das folgende Format verwendet werden:

     domain_name\user_name oder user_name

Wichtig

Das Benutzerkonto muss der lokalen Administratorgruppe oder dem integrierten Active Directory (AD)-Administrator angehören, und Sie müssen die folgenden Richtlinien für die Zuweisung von Benutzerrechten mit der Konsole **Lokale Sicherheitsrichtlinie** oder **Gruppenrichtlinienverwaltung** unter Windows konfigurieren:

- Als Dienst anmelden
- Als Batchauftrag anmelden
- Lokal anmelden

Das Benutzerkonto muss außerdem über die folgenden Datenbankrollen verfügen:

- dbcreator
- bulkadmin
- db_owner

6. Geben Sie für neue SQL Server-Installationen ein neues Kennwort ein, und bestätigen Sie dieses Kennwort.

Hinweis

Kennwörter müssen die folgenden Mindestanforderungen an die Sicherheit erfüllen:

a. Mindestlänge: 8 Zeichen

b. Sie müssen mindestens 3 der folgenden Elemente enthalten:

- Großbuchstaben: A – Z
- Kleinbuchstaben: a – z
- Zahlen: 0 - 9
- Sonderzeichen: !@#$^*?_~-();.+:

7. Geben Sie den **Datenbanknamen** von OfficeScan auf dem SQL Server an.

Beim Migrieren der OfficeScan CodeBase-Datenbank zu einer neuen SQL-Datenbank erstellt OfficeScan die neue Datenbank automatisch mit dem eingegebenen Namen.

8. Führen Sie optional folgende Aufgaben aus:

   - Klicken Sie auf **Verbindung testen**, um die Authentifizierungsdaten für den vorhandenen SQL Server oder die Datenbank zu überprüfen.
   - Klicken Sie auf **Nichtverfügbarkeitswarnung für SQL-Datenbank…**, um die Benachrichtigungseinstellungen für die SQL-Datenbank zu konfigurieren.

     Weitere Informationen finden Sie unter *Nichtverfügbarkeitswarnung für SQL-Datenbank konfigurieren auf Seite 14-60*.

9. Klicken Sie auf **Start**, um die Konfigurationsänderungen zu übernehmen.

Nichtverfügbarkeitswarnung für SQL-Datenbank konfigurieren

OfficeScan sendet diese Warnung automatisch, wenn die SQL-Datenbank nicht verfügbar ist.

Warnung!

OfficeScan beendet automatisch alle Dienste, wenn die Datenbank nicht verfügbar ist. OfficeScan kann keine Agent- oder Ereignisinformationen protokollieren, Updates durchführen oder Agents konfigurieren, wenn die Datenbank nicht verfügbar ist.

Prozedur

1. Navigieren Sie auf dem OfficeScan Server-Computer zu <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\SQL`.
2. Doppelklicken Sie auf die Datei `SQLTxfr.exe`, um das Tool auszuführen.

   Die **SQL Server Migration Tool**-Konsole wird geöffnet.
3. Klicken Sie auf **Nichtverfügbarkeitswarnung für SQL-Datenbank…**.

   Das Fenster **Nichtverfügbarkeitswarnung für SQL Server** wird geöffnet.
4. Geben Sie die E-Mail-Adressen für die Empfänger der Warnung ein.

Trennen Sie mehrere Einträge durch Strichpunkte (;) voneinander.

5. Ändern Sie ggf. den Text in den Feldern **Betreff** und **Nachricht**.

   OfficeScan stellt die folgenden Token-Variablen zur Verfügung:

TABELLE 14-19. Token für die Nichtverfügbarkeitswarnung für SQL-Datenbank

VARIABLE	BESCHREIBUNG
%x	Der Name der OfficeScan SQL Server-Instanz
%s	Der Name des betroffenen OfficeScan Servers

6. Klicken Sie auf **OK**.

Einstellungen des OfficeScan Webservers/ Agents

Bei der Installation des OfficeScan Servers richtet das Setup-Programm automatisch einen Webserver ein, damit sich die Netzwerkcomputer mit dem OfficeScan Server verbinden können. Konfigurieren Sie den Webserver, mit dem sich die Agent-Endpunkte im Netzwerk verbinden sollen.

Ändern Sie die Einstellungen für den Webserver extern (beispielsweise über die IIS Management-Konsole), müssen Sie die Änderungen auch in OfficeScan vornehmen. Falls Sie beispielsweise die IP-Adresse des Servers für die Netzwerkcomputer manuell ändern oder dem Server eine dynamische IP-Adresse zuweisen, müssen Sie die OfficeScan Servereinstellungen neu konfigurieren.

Warnung!

Bei einer Änderung der Verbindungseinstellungen ist es möglich, dass die Verbindung zwischen dem Server und den Agents dauerhaft getrennt wird und eine erneute Bereitstellung der OfficeScan Agents erforderlich ist.

Verbindungseinstellungen konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Einstellungen** > **Agent-Verbindung**.
2. Geben Sie den Domänennamen oder die IPv4-/IPv6-Adresse und die Portnummer des Webservers ein.

   Hinweis

   Bei der Portnummer handelt es sich um den vertrauenswürdigen Port, den der OfficeScan Server für die Kommunikation mit den OfficeScan Agents verwendet.

3. Klicken Sie auf **Speichern**.

Kommunikation zwischen Server und Agents

Sie können OfficeScan so konfigurieren, dass die Gültigkeit der gesamten Kommunikation zwischen dem Server und den Agents sichergestellt wird. OfficeScan ermöglicht die Verschlüsselung mit öffentlichem Schlüssel und enthält erweiterte Verschlüsselungsfunktionen zum Schutz der gesamten Kommunikation zwischen dem Server und den Agents.

Nähere Informationen zu den Schutzfunktionen für die Kommunikation finden Sie unter:

- *Authentifizierung der vom Server gestarteten Kommunikation auf Seite 14-62*
- *Erweiterte Verschlüsselung der Kommunikation zwischen Server und Agent auf Seite 14-67*

Authentifizierung der vom Server gestarteten Kommunikation

OfficeScan verwendet die Verschlüsselung mit öffentlichem Schlüssel zum Authentifizieren der Kommunikation, die der OfficeScan Server auf agents startet. Mit

der Verschlüsselung mit öffentlichem Schlüssel bewahrt der Server einen privaten Schlüssel auf und verteilt einen öffentlichen Schlüssel an alle agents. Die agents überprüfen mit dem öffentlichen Schlüssel, ob die eingehende Kommunikation vom Server gestartet wurde und gültig ist. Die agents antworten, falls die Überprüfung erfolgreich ist.

Hinweis

OfficeScan authentifiziert keine Kommunikationen, die agents auf dem Server starten.

Die öffentlichen und privaten Schlüssel werden einem Trend Micro-Zertifikat zugeordnet. Während der Installation des OfficeScan Servers speichert Setup das Zertifikat im Zertifikatspeicher des Hosts. Verwenden Sie den Zertifikat-Manager für Serverauthentifizierung zum Verwalten der Zertifikate und Schlüssel von Trend Micro.

Wenn Sie die Verwendung eines einzelnen Authentifizierungsschlüssels auf allen OfficeScan Servern auswählen, beachten Sie das Folgende:

- Das Implementieren eines einzelnen Zertifizierungsschlüssels ist übliche Praxis für standardmäßige Sicherheitsstufen. Diese Methode gleicht die Sicherheitsebene Ihres Unternehmens aus und reduziert den Aufwand, der mit der Verwaltung mehrere Schlüssel verbunden ist.
- Das Implementieren mehrerer Zertifikatsschlüssel auf OfficeScan Servern liefert die höchstmögliche Sicherheitsstufe. Durch die Methode wird die Wartung erhöht, die erforderlich ist, wenn Zertifikatsschlüssel ablaufen und auf den Servern verteilt werden müssen.

Wichtig

Vor der Neuinstallation des OfficeScan Servers sollten Sie unbedingt das vorhandene Zertifikat sichern. Nach Abschluss der Neuinstallation importieren Sie das gesicherte Zertifikat, damit die Kommunikationsauthentifizierung zwischen dem OfficeScan Server und den OfficeScan Agents nicht unterbrochen wird. Falls Sie während der Serverinstallation ein neues Zertifikat erstellen, können OfficeScan Agents die Serverkommunikation nicht authentifizieren, da sie noch das alte Zertifikat verwenden (das nicht mehr vorhanden ist).

Weitere Informationen zum Sichern, Wiederherstellen, Exportieren und Importieren von Zertifikaten finden Sie unter *Zertifikat-Manager für Serverauthentifizierung verwenden auf Seite 14-64*.

Zertifikat-Manager für Serverauthentifizierung verwenden

Der OfficeScan Server verwaltet abgelaufene Zertifikate für agents mit abgelaufenen öffentlichen Schlüsseln. Beispielsweise können agents, die längere Zeit keine Verbindung zum Server hergestellt haben, abgelaufene öffentliche Schlüssel aufweisen. Wenn die agents erneut eine Verbindung herstellen, ordnen sie den abgelaufenen öffentlichen Schlüssel dem abgelaufenen Zertifikat zu, um die vom Server gestartete Kommunikation zu erkennen. Der Server verteilt dann den neuesten öffentlichen Schlüssel an die agents.

Beachten Sie beim Konfigurieren von Zertifikaten Folgendes:

- Für den Zertifikatpfad sind zugeordnete Laufwerke und UNC-Pfade zulässig.
- Wählen Sie ein sicheres Kennwort, und bewahren Sie es zur späteren Verwendung gut auf.

Wichtig

Beachten Sie Folgendes bei der Verwendung des Managers für das Authentifizierungszertifikat:

- Der Benutzer muss über Administratorrechte verfügen
- Mit dem Tool können Sie nur Zertifikate verwalten, die sich auf dem lokalen Endpunkt befinden Endpunkt

Prozedur

1. Öffnen Sie auf dem OfficeScan Server die Eingabeaufforderung, und navigieren Sie zum Verzeichnis <*Installationsordner des Servers*>\PCCSRV\Admin\Utility\CertificateManager.

2. Verwenden Sie die folgenden Befehle:

BEFEHL	BEISPIEL	BESCHREIBUNG
CertificateManager.exe -c [Backup_Password]	CertificateManager.exe -c strongpassword	Generiert ein neues Trend Micro-Zertifikat und ersetzt das vorhandene Zertifikat Verwenden Sie diesen Befehl, wenn das vorhandene Zertifikat abgelaufen ist oder wenn es an unbefugte Personen weitergegeben wurde.
CertificateManager.exe -b [Kennwort] [Zertifikatpfad] **Hinweis** Das Zertifikat liegt im ZIP-Format vor.	CertificateManager.exe -b strongpassword D:\Test\TrendMicro.zip	Sichert alle Zertifikate von Trend Micro, die vom aktuellen OfficeScan Server ausgegeben werden Verwenden Sie diesen Befehl zum Sichern des Zertifikats auf dem OfficeScan Server. **Hinweis** Durch das Sichern der Zertifikate von OfficeScan Server können Sie diese Zertifikate verwenden, wenn Sie den OfficeScan Server neu installieren müssen.

BEFEHL	BEISPIEL	BESCHREIBUNG
CertificateManager.exe -r [Kennwort] [Zertifikatpfad] **Hinweis** Das Zertifikat liegt im ZIP-Format vor.	`CertificateManager.exe -r strongpassword D:\Test\TrendMicro.zip`	Führt die Wiederherstellung aller Trend Micro-Zertifikate auf dem Server aus Verwenden Sie diesen Befehl zum Wiederherstellen des Zertifikats auf einem neu installierten OfficeScan Server.
CertificateManager.exe -e [Zertifikatpfad]	`CertificateManager.exe -e <Agent_installation_folder>\OfcNTCer.dat`	Exportiert den öffentlichen Schlüssel des OfficeScan Agents, der dem aktuell verwendeten Zertifikat zugeordnet ist Verwenden Sie diesen Befehl, wenn der von agents verwendete öffentliche Schlüssel beschädigt wird. Kopieren Sie die `.dat`-Datei in den Stammordner des agents, und überschreiben Sie dabei die vorhandene Datei. **Wichtig** Der Dateipfad des Zertifikats auf dem OfficeScan Agent muss wie folgt sein: `<Agent_installation_folder>\OfcNTCer.dat`

BEFEHL	BEISPIEL	BESCHREIBUNG
CertificateManager.exe -i [Kennwort] [Zertifikatpfad] **Hinweis** Der Standarddateiname des Zertifikats ist: `OfcNTCer.pfx`	`CertificateManager.exe -i strongpassword D:\Test\OfcNTCer.pfx`	Importiert ein Trend Micro-Zertifikat in den Zertifikatspeicher
CertificateManager.exe -l [CSV-Pfad]	`CertificateManager.exe -l D:\Test\MismatchedAgentList.csv`	Listet agents (im CSV-Format) auf, die derzeit ein nicht übereinstimmendes Zertifikat verwenden

Erweiterte Verschlüsselung der Kommunikation zwischen Server und Agent

OfficeScan bietet die erweiterte Verschlüsselung der Kommunikation zwischen dem Server und den Agents unter Verwendung des Advanced Encryption Standard (AES) 256, um Branchenstandards und gesetzliche Vorschriften einzuhalten.

Wichtig

OfficeScan unterstützt die AES-256-Verschlüsselung nur auf Servern und Agents unter OfficeScan 11.0 SP1 oder höheren Versionen und Plug-in Manager 2.2 oder höheren Versionen.

Warnung!

Stellen Sie sicher, dass Sie alle vom Server verwalteten OfficeScan Agents auf Version 11.0 SP1 aktualisieren, bevor Sie die AES-256-Verschlüsselung aktivieren. Ältere OfficeScan Agent können die mit AES-256 verschlüsselte Kommunikation möglicherweise nicht entschlüsseln. Die Aktivierung der AES-256-Verschlüsselung für ältere OfficeScan Agent Versionen kann bei Verwendung eines Proxy-Servers zu einem vollständigen Verlust der Kommunikation zum OfficeScan Server führen.

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Klicken Sie auf die Registerkarte **Netzwerk**.
3. Navigieren Sie zum Abschnitt **Kommunikation zwischen Server und Agent**.
4. Klicken Sie auf die Schaltfläche **Ändern** neben **AES-256-Verschlüsselung für Kommunikation zwischen dem OfficeScan Server und OfficeScan Agents**.

   Eine Meldung wird angezeigt.
5. Klicken Sie auf **Versionen überprüfen**, um zu bestätigen, dass Sie alle Agents auf OfficeScan 11.0 SP1 oder höher aktualisiert haben.
6. Klicken Sie auf **OK**.

Kennwort der Webkonsole

Das Fenster, in dem das Kennwort der Webkonsole (oder das Kennwort für das Root-Konto, das während der Installation von OfficeScan Server erstellt wurde) verwaltet wird, wird nur angezeigt, wenn der Server-Computer nicht über die erforderlichen Ressourcen für die rollenbasierte Administration verfügt. Wenn auf dem Server-Computer z. B. Windows Server 2000 läuft und Authorization Manager Runtime nicht installiert ist, kann auf dieses Fenster zugegriffen werden. Bei angemessenen Ressourcen wird dieses Fenster nicht angezeigt, und Sie können das Kennwort über Änderungen am Root-Konto im Fenster **Benutzerkonten** verwalten.

Wenn OfficeScan nicht bei Control Manager registriert wurde, wenden Sie sich an Ihren Support-Anbieter, und fragen Sie nach Anweisungen, wie Sie Zugang zur Webkonsole erhalten.

Einstellungen der Webkonsole konfigurieren

Konfigurieren Sie die Einstellungen der OfficeScan Webkonsole, um festzulegen, wie Benutzer auf die Webkonsole zugreifen und wie häufig eine Bildschirmaktualisierung durchgeführt wird.

Prozedur

1. Navigieren Sie zu **Administration** > **Einstellungen** > **Webkonsole**.
2. Konfigurieren Sie die erforderlichen Einstellungen.

ABSCHNITT	SETTINGS
Einstellungen für automatische Aktualisierung	Wählen Sie **Webkonsole automatisch aktualisieren** aus, um es dem OfficeScan Server zu ermöglichen, die Bildschirmdaten im angegebenen Intervall zu aktualisieren. • **Aktualisierungsintervall**: Wählen Sie die Häufigkeit (in Sekunden) aus, mit der die Bildschirmdaten der Webkonsole aktualisiert werden.
Einstellungen für die Zeitüberschreitung	Wählen Sie **Inaktive Benutzer automatisch abmelden** aus, um es dem OfficeScan Server zu ermöglichen, Benutzer im angegebenen Intervall abzumelden. • **Inaktivitätsintervall**: Wählen Sie den Zeitraum der Inaktivität (in Minuten) aus, nach dem die Webkonsole die Benutzer automatisch abmeldet.

3. Klicken Sie auf **Speichern**.

Quarantäne-Manager

Wenn der OfficeScan Agent Sicherheitsrisiken entdeckt und als Suchaktion "Quarantäne" festgelegt ist, wird die infizierte Datei verschlüsselt und in den lokalen Quarantäne-Ordner verschoben, der sich im Verzeichnis <*Installationsordner des Agents*>`\SUSPECT\Backup` befindet.

Nachdem Sie die Datei in den lokalen Quarantäne-Ordner verschoben haben, sendet der OfficeScan Agent sie an den vorgesehenen Quarantäne-Ordner. Geben Sie das Verzeichnis auf der Registerkarte **Agents** > **Agent-Verwaltung** > **Einstellungen** > **{Suchtyp} Einstellungen** > **Aktion** an. Die Dateien in diesem Quarantäne-Ordner sind ebenfalls verschlüsselt, damit sie keine anderen Dateien infizieren können. Weitere Informationen finden Sie unter *Quarantäne-Ordner auf Seite 7-45*.

Wenn sich das vorgesehene Quarantäne-Verzeichnis auf dem OfficeScan Server befindet, ändern Sie die Einstellungen für das Quarantäne-Verzeichnis des Servers über die Webkonsole. Der Server speichert die unter Quarantäne gestellten Dateien im Verzeichnis <*Installationsordner des Servers*>`\PCCSRV\Virus`.

Hinweis

Wenn der OfficeScan Agent die verschlüsselte Datei aus irgendeinem Grund, z. B. wegen Netzwerkproblemen, nicht an den OfficeScan Server senden kann, verbleibt die verschlüsselte Datei im Quarantäne-Ordner des OfficeScan Agents. Der OfficeScan Agent Agent wird bei Verbindung mit dem OfficeScan Server versuchen, die Datei erneut zu senden.

Einstellungen des Quarantäne-Ordners konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Einstellungen** > **Quarantäne-Manager**.
2. Übernehmen oder ändern Sie die Standardkapazität des Quarantäne-Ordners und die maximale Größe einer infizierten Datei, die OfficeScan im Quarantäne-Ordner speichern kann.

   Die Standardwerte werden im Fenster angezeigt.

3. Klicken Sie auf **Quarantäne-Einstellungen speichern**.

4. Um alle im Quarantäne-Ordner enthaltenen Dateien zu entfernen, klicken Sie auf **Alle Dateien in Quarantäne löschen**.

Server Tuner

Mit Server Tuner können Sie die Leistung des OfficeScan Servers optimieren. Parameter können für die folgenden leistungsbezogenen Daten festgelegt werden:

- **Download**

  Übersteigt die Anzahl der OfficeScan Agents (inkl. Update-Agents), die Updates vom OfficeScan Server anfordern, die Serverkapazität, so leitet der Server die agent-Update-Anfragen in eine Warteschlange um und bearbeitet sie erst dann, wenn wieder Ressourcen frei sind. Nachdem die Komponenten auf dem agent aktualisiert wurden, sendet dieser Agent eine entsprechende Benachrichtigung an den OfficeScan Server. Legen Sie dazu fest, wie viele Minuten der OfficeScan Server maximal auf eine agent-Update-Benachrichtigung warten soll. Legen Sie außerdem fest, wie oft der Server versuchen soll, dem agent Benachrichtigungen zu Updates und neuen Konfigurationseinstellungen zu senden. Der Server versucht dies so lange, bis er die entsprechende Bestätigung vom agent erhält.

- **Puffer**

  Erhält der OfficeScan von mehreren OfficeScan Agents gleichzeitig Anfragen (z. B. zum Durchführen von Updates), bearbeitet er die maximal mögliche Anzahl und speichert die übrigen Anfragen in einem Puffer. Sobald wieder ausreichend Ressourcen vorhanden sind, werden die Anfragen im Puffer der Reihe nach abgearbeitet. Legen Sie die Größe des Ereignispuffers (z. B. für agent Update-Anfragen) und des Puffers für agent-Protokolle fest.

- **Netzwerkdatenverkehr**

  Das Volumen des Netzwerkdatenverkehrs variiert während des Tages. Sie können den Netzwerkdatenverkehr zum OfficeScan Server und zu anderen Update-Adressen steuern, indem Sie für jede Tageszeit festlegen, wie viele OfficeScan Agents gleichzeitig aktualisiert werden können.

Server Tuner benötigt die folgende Datei: `SvrTune.exe`

Server Tuner ausführen

Prozedur

1. Navigieren Sie auf dem OfficeScan Server-Computer zu <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\SvrTune`.
2. Doppelklicken Sie auf die Datei `SvrTune.exe`, um Server Tuner zu starten.

   Die Server Tuner Konsole wird geöffnet.
3. Ändern Sie unter **Download** die folgenden Einstellungen:
   - **Timeout for client**: Legen Sie fest, wie viele Minuten der OfficeScan Server auf eine Update-Antwort der agents warten soll. Antwortet der agent innerhalb dieses Zeitraums nicht, gilt der agent für den OfficeScan Server als nicht aktualisiert. Wird die Zeitbegrenzung des agents überschritten, rückt ein anderer agent nach, der auf Benachrichtigung wartet.
   - **Timeout for Update-Agent**: Legen Sie fest, wie viele Minuten der OfficeScan Server auf eine Update-Antwort eines Update-Agents warten soll. Wird die Zeitbegrenzung des agents überschritten, rückt ein anderer agent nach, der auf Benachrichtigung wartet.
   - **Anzahl an Versuchen**: Legen Sie fest, wie oft der OfficeScan Server versuchen soll, dem agent Benachrichtigungen zu Updates und neuen Konfigurationseinstellungen zu senden.
   - **Versuchsintervall**: Legen Sie fest, wie viele Minuten der OfficeScan Server zwischen den einzelnen Benachrichtigungsversuchen warten soll.
4. Ändern Sie unter **Network Traffic** die folgenden Einstellungen:
   - **Normal hours**: Stellen Sie über die Optionsfelder die Zeiten ein, deren Netzwerk-Datenverkehrsvolumen Sie als normal einschätzen.
   - **Off-peak hours**: Stellen Sie über die Optionsfelder die Zeiten ein, deren Netzwerk-Datenverkehrsvolumen Sie als besonders gering einschätzen.

- **Peak hours**: Stellen Sie über die Optionsfelder die Zeiten ein, deren Netzwerk-Datenverkehrsvolumen Sie als besonders hoch einschätzen.

- **Maximum client connections**: Legen Sie fest, wie viele Clients gleichzeitig Komponenten-Updates über die unter "Andere Update-Adresse" angegebene Quelle und über den OfficeScan Server beziehen können. Für jeden genannten Zeitraum muss die maximale Anzahl von Clients angegeben werden. Wenn die maximale Anzahl von Verbindungen erreicht wurde, können OfficeScan Agents erst dann wieder Komponenten aktualisieren, wenn eine aktuelle agent-Verbindung unterbrochen wurde (da Updates abgeschlossen wurden oder der in **Timeout for client** oder **Timeout for Update-Agent** angegebene Zeitraum für die Antwort des agent überschritten wurde).

5. Klicken Sie auf **OK**. Sie werden nun aufgefordert, den OfficeScan Master Service neu zu starten.

Hinweis

Nur der Dienst wird neu gestartet, nicht der Computer.

6. Wählen Sie eine der folgenden Optionen zum Neustart aus:

   - Klicken Sie auf **Ja**, um die Einstellungen für Server Tuner zu speichern und den Dienst neu zu starten. Die Einstellungen sind nach dem Neustart sofort wirksam.

   - Klicken Sie auf **Nein**, um die Einstellungen für Server Tuner zu speichern, jedoch den Dienst nicht neu zu starten. Starten Sie den OfficeScan Master Service oder den OfficeScan Server-Computer neu, damit die Einstellungen wirksam werden.

Smart Feedback

Trend Micro Smart Feedback leitet anonyme Informationen über Bedrohungen an das Smart Protection Network weiter, damit Trend Micro neue Bedrohungen schnell

identifizieren und davor schützen kann. Sie können Smart Feedback jederzeit über diese Konsole deaktivieren.

Am Smart Feedback Programm teilnehmen

Prozedur

1. Navigieren Sie zu **Administration** > **Smart Protection** > **Smart Feedback**.
2. Klicken Sie auf **Trend Micro Smart Feedback aktivieren**.
3. Um Trend Micro beim Verständnis Ihre Unternehmens zu unterstützen, wählen Sie die **Branche**.
4. Um die Informationen über potenzielle Sicherheitsbedrohungen in den Dateien auf den OfficeScan Agents zu senden, aktivieren Sie das Kontrollkästchen **Feedback zu verdächtigen Programmdateien aktivieren**.

   Hinweis

   Die Dateien, die an Smart Feedback gesendet werden, enthalten keine Benutzerdaten und werden nur zur Bedrohungsanalyse übertragen.

5. Um die Kriterien für das Versenden von Feedback zu konfigurieren, wählen Sie die Anzahl der Erkennungen für die angegebene Zeitdauer, die das Feedback auslöst.
6. Geben Sie die maximale Bandbreite ein, die OfficeScan beim Senden des Feedbacks verwenden kann, um Netzwerkbeeinträchtigungen zu minimieren.
7. Klicken Sie auf **Speichern**.

Kapitel 15

OfficeScan Agent verwalten

In diesem Kapitel werden die Verwaltung und Konfiguration von OfficeScan Agent beschrieben.

Es werden folgende Themen behandelt:

- *Endpunktspeicherort auf Seite 15-2*
- *OfficeScan Agent Programmverwaltung auf Seite 15-6*
- *Agent-Server-Verbindung auf Seite 15-28*
- *OfficeScan Agent Proxy-Einstellungen auf Seite 15-53*
- *OfficeScan Agent-Informationen anzeigen auf Seite 15-60*
- *Agent-Einstellungen importieren und exportieren auf Seite 15-60*
- *Einhaltung von Sicherheitsrichtlinien auf Seite 15-62*
- *Unterstützung für Trend Micro Virtual Desktop auf Seite 15-84*
- *Globale Agent-Einstellungen auf Seite 15-99*
- *Agent-Berechtigungen und weitere Einstellungen konfigurieren auf Seite 15-101*

Endpunktspeicherort

OfficeScan unterstützt die Funktion "Location Awareness", mit der festgestellt wird, ob sich der OfficeScan Agent in einem internen oder externen Netzwerk befindet. Location Awareness wird in folgenden OfficeScan Funktionen und Services genutzt:

TABELLE 15-1. Funktionen und Services mit Location Awareness

FUNKTION/ SERVICE	BESCHREIBUNG
File-Reputation-Dienste	Für Agents der intelligenten Suche bestimmt der Standort des OfficeScan Agents die Smart Protection Quelle, an die der OfficeScan Agent Suchabfragen sendet. Externe OfficeScan Agents senden Abfragen an das Smart Protection Network, während interne OfficeScan Agents ihre Abfragen an die Quellen senden, die in der Liste der Smart Protection Quellen definiert sind. Weitere Informationen finden Sie unter *Smart Protection Quellen auf Seite 4-6*.
Web Reputation Prävention vor Datenverlust Gerätesteuerung	Der Standort des OfficeScan Agents bestimmt, ob der OfficeScan Agent interne oder externe Richtlinien anwendet. Bei externen OfficeScan Agents setzen Administratoren normalerweise eine strengere Richtlinie durch. Weitere Informationen finden Sie unter: • *Web-Reputation-Richtlinien auf Seite 12-5*. • *Richtlinien für 'Prävention vor Datenverlust' auf Seite 11-3* • *Gerätesteuerung auf Seite 10-2*

Standortkriterien

Legen Sie fest, ob der Standort auf der Gateway-IP-Adresse des OfficeScan Agent-Endpunkts basiert oder auf dem OfficeScan Agent-Verbindungsstatus mit dem OfficeScan Server oder einem Referenzserver.

- **Verbindungsstatus des Agents**: Kann sich der OfficeScan Agent mit dem OfficeScan Server oder einem festgelegten Referenzserver im Intranet verbinden,

ist der Endpunkt-Standort intern. Wenn darüber hinaus ein Endpunkt, der sich außerhalb des Unternehmensnetzwerks befindet, eine Verbindung mit dem OfficeScan Server/Referenzserver aufbauen kann, ist sein Standort auch intern. Trifft keine dieser Bedingungen zu, gilt der Endpunkt-Standort als extern.

- **Gateway-IP- und MAC-Adresse**: Wenn die Gateway-IP-Adresse des OfficeScan Agent-Endpunkts mit der Gateway-IP-Adresse übereinstimmt, die Sie im Fenster **Endpunktspeicherort** festgelegt haben, handelt es sich um einen internen Endpunkt-Standort. Andernfalls gilt der Endpunkt-Standort als extern.

Einstellungen für den Standort konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Endpunktspeicherort**.
2. Wählen Sie, ob der Standort auf dem **Verbindungsstatus des Agents** oder der **Gateway-IP- und MAC-Adresse** basiert.
3. Wenn Sie **Verbindungsstatus des Agents** auswählen, entscheiden Sie, ob Sie einen Referenzserver verwenden möchten.

   Weitere Informationen finden Sie unter *Referenzserver auf Seite 14-40*.

   a. Wenn Sie keinen Referenzserver festlegen, überprüft der OfficeScan Agent in den folgenden Fällen den Verbindungsstatus mit dem OfficeScan Server:

      - Der OfficeScan Agent wechselt vom unabhängigen Modus in den Normalmodus (online/offline).
      - Der OfficeScan Agent wechselt von einer Suchmethode zu einer anderen.

        Weitere Informationen finden Sie unter *Suchmethodentypen auf Seite 7-9*.
      - Der OfficeScan Agent erkennt eine IP-Adressänderungen für den Endpunkt.
      - Der OfficeScan Agent wird neu gestartet.

- Der Server startet eine Verbindungsüberprüfung.

  Weitere Informationen finden Sie unter *OfficeScan Agent Symbole auf Seite 15-29*.

- Standortkriterien der Web Reputation ändern sich während der Übernahme allgemeiner Einstellungen

- Die Ausbruchspräventionsrichtlinie ist nicht mehr aktiv, und die vorherigen Einstellungen werden wiederhergestellt

b. Wenn Sie einen Referenzserver festgelegt haben, überprüft der OfficeScan Agent den Verbindungsstatus zuerst mit dem OfficeScan Server und anschließend mit dem Referenzserver, falls die Verbindung zum OfficeScan Server fehlgeschlagen ist. Der OfficeScan Agent überprüft den Verbindungsstatus stündlich und bei Eintritt der oben genannten Ereignisse.

4. Wenn Sie **Gateway-IP- und MAC-Adresse** wählen:

   a. Geben Sie die IPv4/IPv6-Adresse des Gateways in das vorgesehene Textfeld ein.

   b. Geben Sie die MAC-Adresse ein.

   c. Klicken Sie auf **Hinzufügen**.

      Wenn Sie keine MAC-Adresse eingeben, fügt OfficeScan alle zur angegebenen IP-Adresse gehörigen MAC-Adressen hinzu.

   d. Wiederholen Sie die Schritte a bis c, bis Sie alle gewünschten Gateway-IP-Adressen hinzugefügt haben.

   e. Verwenden Sie das Tool für den Import von Gateway-Einstellungen, um eine Liste mit Gateway-Einstellungen in dieses Fenster zu importieren.

      Weitere Informationen finden Sie unter *Import von Gateway-Einstellungen auf Seite 15-5*.

5. Klicken Sie auf **Speichern**.

Import von Gateway-Einstellungen

OfficeScan überprüft den Standort des Endpunkts, um festzustellen, welche Web-Reputation-Richtlinie angewendet und mit welcher Smart Protection Quelle eine Verbindung aufgebaut werden soll. Zum Beispiel ermittelt OfficeScan den Standort durch Überprüfen der Gateway-IP-Adresse und der MAC-Adresse des Endpunkts.

Sie können die Gateway-Einstellungen im Fenster **Endpunktspeicherort** konfigurieren oder das Tool für den Import von Gateway-Einstellungen (Gateway Settings Importer) verwenden, um eine Liste der Gateway-Einstellungen in das Fenster **Endpunktspeicherort** zu importieren.

Gateway Settings Importer verwenden

Prozedur

1. Bereiten Sie eine Textdatei (`.txt`) vor, die die Liste der Gateway-Einstellungen enthält. Geben Sie in jede Zeile eine IPv4- oder eine IPv6-Adresse sowie optional eine MAC-Adresse ein.

   Trennen Sie IP-Adressen und MAC-Adressen mit Komma voneinander. Es sind maximal 4096 Einträge möglich.

   Beispiel:

   ```
   10.1.111.222,00:17:31:06:e6:e7

   2001:0db7:85a3:0000:0000:8a2e:0370:7334

   10.1.111.224,00:17:31:06:e6:e7
   ```

2. Navigieren Sie auf dem Server zu <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\GatewaySettingsImporter`.

3. Klicken Sie mit der rechten Maustaste auf die Datei `GSImporter.exe` und wählen Sie **Als Administrator ausführen** aus.

Hinweis

Der Gateway Settings Importer kann nicht über Terminal Services ausgeführt werden.

4. Navigieren Sie im Fenster **Import von Gateway-Einstellungen** zu der Datei, die Sie in Schritt 1 erstellt haben, und klicken Sie auf **Importieren**.

5. Klicken Sie auf **OK**.

   Die Gateway-Einstellungen werden im Fenster **Endpunktspeicherort** angezeigt, und der OfficeScan Server verteilt die Einstellungen an die OfficeScan Agents.

6. Klicken Sie auf **Alle löschen**, um alle Einträge zu löschen.

   Wenn Sie nur einen bestimmten Eintrag löschen möchten, entfernen Sie diesen aus dem Fenster **Endpunktspeicherort**.

7. Um die Einstellungen in eine Datei zu exportieren, klicken Sie auf **Alle exportieren**, und legen Sie Dateinamen und -typ fest.

OfficeScan Agent Programmverwaltung

Die folgenden Themen beschreiben, wie Sie das OfficeScan Agent-Programm verwalten und schützen können.

- *OfficeScan Agent Dienste auf Seite 15-7*
- *Neustart des OfficeScan Agent Dienstes auf Seite 15-12*
- *OfficeScan Agent Eigenschutz auf Seite 15-13*
- *Einschränkung des Zugriffs auf die OfficeScan Agent-Konsole auf Seite 15-18*
- *OfficeScan Agent Beenden und entsperren auf Seite 15-19*
- *Berechtigung "Unabhängiger Modus" von OfficeScan Agent auf Seite 15-20*
- *Agent Mover auf Seite 15-24*
- *Inaktive OfficeScan Agenten auf Seite 15-27*

OfficeScan Agent Dienste

Der OfficeScan Agent führt die in der folgenden Tabelle aufgelisteten Dienste aus. Sie können den Status dieser Dienste auf der Microsoft Management-Konsole sehen.

DIENST	KONTROLLIERTE FUNKTIONSMERKMALE
Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)	• Verhaltensüberwachung • Gerätesteuerung • Certified Safe Software Service
OfficeScan NT Firewall (`TmPfw.exe`)	OfficeScan firewall
OfficeScan Datenschutzdienst (`dsagent.exe`)	• Prävention vor Datenverlust • Gerätesteuerung
OfficeScan NT Listener (`tmlisten.exe`)	Kommunikation zwischen OfficeScan Agent und OfficeScan Server
OfficeScan NT Proxy-Dienst (`TmProxy.exe`)	• Web Reputation • POP3 mail scan
OfficeScan NT RealTime Scan (`ntrtscan.exe`)	• Echtzeitsuche • Zeitgesteuerte Suche • Manuelle Suche/Sofort durchsuchen
OfficeScan Common Client Solution Framework (`TmCCSF.exe`)	Erweiterter Schutzdienst • Verhinderung von Browser-Schwachstellen • Arbeitsspeichersuche

Die folgenden Dienste bieten zuverlässigen Schutz, aber ihre Überwachungsmechanismen können die Systemressourcen belasten, insbesondere auf Servern, auf denen Anwendungen laufen, die das System stark in Anspruch nehmen:

- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)
- OfficeScan NT Firewall (`TmPfw.exe`)

- OfficeScan Datenschutzdienst (`dsagent.exe`)

Aus diesem Grund sind diese Dienste auf Server-Plattformen (Windows Server 2003, Windows Server 2008 und Windows Server 2012) standardmäßig deaktiviert. So aktivieren Sie diese Dienste:

- Überwachen Sie ständig die Systemleistung und führen Sie die notwendigen Aktionen durch, wenn Sie einen Leistungsabfall bemerken.
- `TMBMSRV.exe` können Sie aktivieren, wenn Sie systemintensive Anwendungen aus den Richtlinien der Verhaltensüberwachung ausschließen. Sie können auch ein Performance Tuning Tool verwenden, um systemintensive Anwendungen zu identifizieren.

  Weitere Informationen finden Sie unter *Trend Micro Performance Tuning Tool verwenden auf Seite 15-10*.

Bei Desktop-Plattformen deaktivieren Sie die Dienste nur, wenn Sie einen deutlichen Leistungsabfall verzeichnen.

Die Agent-Dienste von der Webkonsole aus aktivieren oder deaktivieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Für OfficeScan Agents unter Windows XP, 7, 8, 8.1 oder 10:
   a. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.

Hinweis

Wenn Sie die Root-Domäne oder bestimmte Domänen auswählen, gilt die Einstellung nur für Agents, die auf Windows-Desktop-Plattformen ausgeführt werden. Diese Einstellung gilt nicht für Agents, die auf einer beliebigen Windows Server-Plattform ausgeführt werden, selbst wenn sie zu den Domänen gehören.

b. Klicken Sie auf **Einstellungen** > **Zusätzliche Diensteinstellungen**.

c. Wählen Sie in den folgenden Abschnitten die entsprechende Option aus, um den erforderlichen Dienst auf **Windows-Desktops** oder **Windows Server-Plattformen** zu aktivieren:

- **Unauthorized Change Prevention Service**
- **Firewall-Dienst**
- **Verdächtiger Verbindungsdienst**
- **Datenschutzdienst**
- **Erweiterter Schutzdienst**

d. Klicken Sie auf **Speichern**, um die Einstellungen auf die Domäne(n) anzuwenden. Wenn Sie das Root-Domänen-Symbol ausgewählt haben, können Sie aus folgenden Optionen auswählen:

- **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Windows-Desktop-Agents sowie auf alle neuen Agents an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden sind.
- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Windows-Desktop-Agents an, die zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

3. Für OfficeScan Agents unter Windows Server-Plattformen:

a. Wählen Sie in der Agent-Hierarchie einen einzelnen Agent aus, der auf einer Windows Server-Plattform ausgeführt wird.

b. Klicken Sie auf **Einstellungen** > **Zusätzliche Diensteinstellungen**.

c. Wählen Sie in den folgenden Abschnitten die entsprechende Option aus, um den erforderlichen Dienst auf **Windows-Desktops** oder **Windows Server-Plattformen** zu aktivieren:

- **Unauthorized Change Prevention Service**
- **Firewall-Dienst**
- **Verdächtiger Verbindungsdienst**
- **Datenschutzdienst**
- **Erweiterter Schutzdienst**

d. Klicken Sie auf **Speichern**.

Trend Micro Performance Tuning Tool verwenden

Prozedur

1. Trend Micro Performance Tuning Tool herunterladen:

   http://esupport.trendmicro.com/solution/en-us/1056425.aspx

2. Entpacken Sie die Datei `TMPerfTool.zip`, um `TMPerfTool.exe` zu extrahieren.

3. Platzieren Sie `TMPerfTool.exe` in den <*Installationsordner des Agents*> oder in den selben Ordner wie `TMBMCLI.dll`.

4. Klicken Sie mit der rechten Maustaste auf `TMPerfTool.exe`, und wählen Sie **Als Administrator ausführen**.

5. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung, und klicken Sie dann auf **OK**.

6. Klicken Sie auf **Analysieren**.

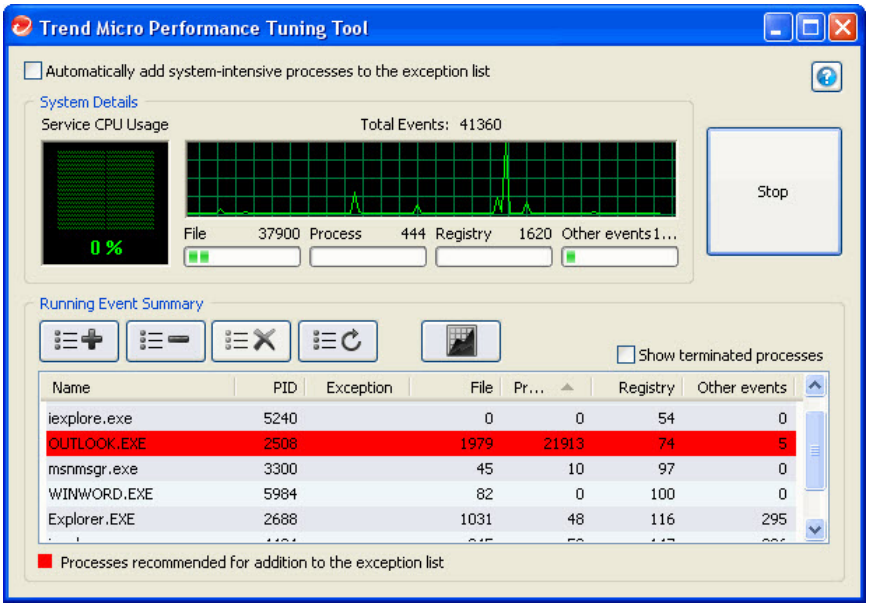


ABBILDUNG 15-1. Markierter systemintensiver Prozess

Das Tool startet die Überwachung der CPU-Nutzung und das Laden der Ereignisse. Ein systemintensiver Prozess erscheint rot markiert.

7. Wählen Sie einen systemintensiven Prozess, und klicken Sie auf die Schaltfläche **Zur Ausschlussliste hinzufügen (erlauben)** ( ).
8. Überprüfen Sie, ob sich die Leistung des Systems oder der Anwendung verbessert.
9. Wenn sich die Leistung verbessert, wählen Sie den Prozess erneut, und klicken Sie auf die Schaltfläche **Aus der Ausschlussliste entfernen** ( ).
10. Wenn die Leistung wieder abfällt, führen Sie die folgenden Schritte durch:
    a. Notieren Sie den Namen der Anwendung.
    b. Klicken Sie auf **Beenden**.
    c. Klicken Sie auf die Schaltfläche **Bericht erstellen** ( ), und speichern Sie anschließend die `.xml`-Datei.

d. Überprüfen Sie die Anwendungen, die einen Konflikt verursachen, und fügen Sie sie zur Ausschlussliste der Verhaltensüberwachung hinzu.

Weitere Informationen finden Sie unter *Ausschlussliste für Verhaltensüberwachung auf Seite 9-10*.

Neustart des OfficeScan Agent Dienstes

OfficeScan startet die OfficeScan Agent-Dienste neu, die unerwartet nicht mehr reagieren und nicht durch einen normalen Systemprozess angehalten wurden. Weitere Informationen zu agent Diensten finden Sie unter *OfficeScan Agent Dienste auf Seite 15-7*.

Konfigurieren Sie die notwendigen Einstellungen, um den Neustart der OfficeScan Agent-Dienste zu ermöglichen.

Einstellungen für den Neustart der Dienste konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Klicken Sie auf die Registerkarte **System**.
3. Wechseln Sie zum Abschnitt **Neustart der Dienste**.
4. Wählen Sie **OfficeScan Agent-Dienst beim unerwarteten Beenden des Diensts automatisch neu starten**.
5. Konfigurieren Sie das Folgende:
   - **Den Dienst neu starten nach __ Minuten**: Geben Sie an, wie viel Zeit (in Anzahl von Minuten) vergehen muss, bis OfficeScan einen Service neu startet.
   - **Schlägt erster Neustartversuch fehl, __ Wiederholungsversuche unternehmen**: Legt die maximale Anzahl von Neustartversuchen für einen Dienst fest. Starten Sie den Dienst manuell, wenn er nach Erreichen der maximalen Anzahl von Neustartversuchen weiterhin nicht läuft.

- **Den Neustart-Fehlerzähler zurücksetzen nach _ Stunde(n)**: Wenn ein Dienst weiterhin nach Erreichen der maximalen Anzahl von Neustartversuchen nicht läuft, wartet OfficeScan eine bestimmte Anzahl von Stunden, um den Fehlerzähler zurückzusetzen. Wenn ein Dienst weiterhin nach Erreichen der angegebenen Anzahl von Stunden nicht läuft, startet OfficeScan den Dienst neu.

OfficeScan Agent Eigenschutz

Der Eigenschutz des OfficeScan Agents ermöglicht dem OfficeScan Agent das Schützen der Prozesse und anderer Ressourcen, damit diese ordnungsgemäß funktionieren. Der Eigenschutz des OfficeScan Agents vereitelt Versuche von Programmen oder Benutzern, den Anti-Malware-Schutz zu deaktivieren.

OfficeScan Agent Der Eigenschutz von OfficeScan Agent bietet die folgenden Optionen:

- *OfficeScan Agent-Dienste schützen auf Seite 15-14*
- *Dateien im OfficeScan Agent-Installationsordner schützen auf Seite 15-15*
- *OfficeScan Agent-Registrierungsschlüssel schützen auf Seite 15-16*
- *OfficeScan Agent-Prozesse schützen auf Seite 15-17*

Eigenschutzeinstellungen des OfficeScan Agents konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Klicken Sie auf die Registerkarte **Andere Einstellungen**, und wechseln Sie zum Abschnitt **Eigenschutz des OfficeScan Agents**.

5. Aktivieren Sie die folgenden Optionen:

   - *OfficeScan Agent-Dienste schützen auf Seite 15-14*
   - *Dateien im OfficeScan Agent-Installationsordner schützen auf Seite 15-15*
   - *OfficeScan Agent-Registrierungsschlüssel schützen auf Seite 15-16*
   - *OfficeScan Agent-Prozesse schützen auf Seite 15-17*

6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

OfficeScan Agent-Dienste schützen

OfficeScan blockiert alle Versuche, die folgenden OfficeScan Agent-Dienste zu beenden:

- OfficeScan NT Listener (`TmListen.exe`)
- OfficeScan NT RealTime Scan (`NTRtScan.exe`)
- OfficeScan NT Proxy-Dienst (`TmProxy.exe`)
- OfficeScan NT Firewall (`TmPfw.exe`)
- OfficeScan Datenschutzdienst (`dsagent.exe`)
- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)

Hinweis

Wenn diese Option aktiviert ist, verhindert der OfficeScan Agent möglicherweise, dass Produkte anderer Hersteller erfolgreich auf den Endpunkten installiert werden. Wenn Sie dieses Problem feststellen, können Sie diese Option vorübergehend deaktivieren und nach der Installation des Fremdprodukts wieder aktivieren.

- Gemeinsames Client Solution Framework für Trend Micro (`TmCCSF.exe`)

Dateien im OfficeScan Agent-Installationsordner schützen

Um zu verhindern, dass andere Programme und sogar Benutzer OfficeScan Agent Dateien ändern oder löschen können, enthält OfficeScan diverse erweiterte Schutzfunktionen.

Nach der Aktivierung von **Dateien im OfficeScan Agent-Installationsordner schützen** sperrt OfficeScan die folgenden Dateien im Stamm-<*Installationsordner des Agents*>:

- Alle digital signierten Dateien mit den Dateinamenserweiterungen `.exe`, `.dll` und `.sys`
- Einige Dateien ohne digitale Signaturen, inkl.:
  - `bspatch.exe`
  - `bzip2.exe`
  - `INETWH32.dll`
  - `libcurl.dll`
  - `libeay32.dll`
  - `libMsgUtilExt.mt.dll`
  - `msvcm80.dll`
  - `MSVCP60.DLL`
  - `msvcp80.dll`
  - `msvcr80.dll`
  - `OfceSCV.dll`
  - `OFCESCVPack.exe`
  - `patchbld.dll`
  - `patchw32.dll`
  - `patchw64.dll`
  - `PiReg.exe`
  - `ssleay32.dll`
  - `Tmeng.dll`
  - `TMNotify.dll`
  - `zlibwapi.dll`

Nach der Aktivierung von **Dateien im OfficeScan Agent-Installationsordner schützen** und der Echtzeitsuche für Virus/Malware-Bedrohungen führt OfficeScan die folgenden Aktionen aus:

- Dateiintegritätsprüfung vor dem Starten von `.exe`-Dateien im Installationsordner

  Während ActiveUpdate-Updates überprüft OfficeScan, ob der Aussteller der Datei, die das Update ausgelöst hat, Trend Micro ist. Wird als Aussteller nicht Trend Micro erkannt und kann ActiveUpdate die falsche Datei nicht ersetzen, protokolliert OfficeScan den Vorfall im Windows-Ereignisprotokoll und sperrt das Update.

- Verhindert DLL-Diebstahl

  Einige Malwareverfasser kopieren Dynamic Link Library-Dateien in den Installationsordner von OfficeScan Agent oder in den Ordner der Verhaltensüberwachung, damit diese Dateien vor dem Agent geladen werden. Diese Dateien zielen darauf ab, den von OfficeScan gebotenen Schutz zu durchbrechen. Damit gestohlene Dateien nicht in die Ordner von OfficeScan Agent kopiert werden können, verhindert OfficeScan das Kopieren von Dateien in den Installationsordner und in den Ordner der Verhaltensüberwachung.

- Verhindert das Sperren von Dateien mit der Einstellung „SHARE:NONE“ in Windows

OfficeScan Agent-Registrierungsschlüssel schützen

Der OfficeScan Agent sperrt alle Versuche, unter den folgenden Registrierungsschlüsseln und Unterschlüsseln Einträge zu ändern, zu löschen oder neue Einträge hinzuzufügen:

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP`

OfficeScan Agent-Prozesse schützen

Der OfficeScan Agent blockiert alle Versuche, die Prozesse in der folgenden Tabelle zu beenden.

PROZESS	BESCHREIBUNG
TmListen.exe:	Empfängt Befehle und Benachrichtigungen vom OfficeScan Server und erleichtert die Kommunikation zwischen dem OfficeScan Agent und dem Server.
NTRtScan.exe:	Führt die Echtzeitsuche, die zeitgesteuerte oder die manuelle Suche auf den OfficeScan Agents durch.
TmProxy.exe	Durchsucht den Netzwerkdatenverkehr, bevor dieser an die Zielanwendung weitergeleitet wird.
TmPfw.exe	Bietet eine Firewall auf Paketebene, Netzwerkvirensuche und Funktionen zur Erkennung von Eindringlingen.
TMBMSRV.exe	Reguliert den Zugriff auf externe Speichergeräte und verhindert unbefugte änderungen an Registrierungsschlüsseln und Prozessen.
DSAgent.exe	überwacht die übertragung vertraulicher Daten und steuert den Zugriff auf Geräte
PccNTMon.exe	Dieser Prozess ist verantwortlich für den Start der OfficeScan Agent-Konsole.
TmCCSF.exe	Führt die Funktion zur Verhinderung von Browser-Schwachstellen und die Arbeitsspeichersuche aus.

Der OfficeScan Agent kann auch vor dem Hinzufügen von Prozessen in den Microsoft-Richtlinien für Softwareeinschränkungen (Software Restriction Policies, SRP) schützen. Durch Software Restriction Policies wird die Ausführung der aufgelisteten Anwendungen auf dem Endpunkt verhindert. So verhindern Sie das Hinzufügen von OfficeScan Agent Prozessen in der Software Restriction Policies-Liste:

1. Aktivieren Sie **OfficeScan Agent-Prozesse schützen**.
2. Aktivieren Sie den **Unauthorized Change Prevention Service**.

Weitere Informationen finden Sie unter *Die Agent-Dienste von der Webkonsole aus aktivieren oder deaktivieren auf Seite 15-8*.

Einschränkung des Zugriffs auf die OfficeScan Agent-Konsole

Diese Einstellung deaktiviert den Zugriff auf die OfficeScan Agent-Konsole von der Taskleiste oder dem Windows Start-Menü aus. Die einzige Möglichkeit, wie Benutzer auf die OfficeScan Agent-Konsole zugreifen können, besteht darin, einen Doppelklick auf die Datei `PccNTMon.exe` im <*Installationsordner des Agents*> auszuführen. Laden Sie nach dem Konfigurieren dieser Einstellung den OfficeScan Agent Agent erneut, damit die Einstellung wirksam wird.

Diese Einstellung deaktiviert nicht den OfficeScan Agent. Der OfficeScan Agent wird im Hintergrund ausgeführt und schützt so vor Sicherheitsrisiken.

Zugriff auf die OfficeScan Agent-Konsole einschränken

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Klicken Sie auf die Registerkarte **Andere Einstellungen**, und wechseln Sie zum Abschnitt **Einschränkung des Zugriffs auf OfficeScan Agent**.
5. Wählen Sie **Den Zugriff auf die OfficeScan Agent-Konsole über die Taskleiste oder das Windows Start-Menü für Benutzer einschränken**.
6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen

Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

OfficeScan Agent Beenden und entsperren

Die Berechtigung zum Beenden und Entsperren des OfficeScan Agents erlaubt dem Benutzer, den OfficeScan Agent vorübergehend anzuhalten oder mit oder ohne Kennwort auf erweiterte Webkonsolenfunktionen zuzugreifen.

Die Berechtigung zum Beenden und Entsperren des Agents gewähren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Wechseln Sie auf der Registerkarte **Berechtigungen** zum Abschnitt **Beenden und entsperren**.
5. Um das Beenden des OfficeScan Agents ohne Kennwort zu erlauben, wählen Sie **Kein Kennwort erforderlich** aus.
   - Ist ein Kennwort erforderlich, wählen Sie **Kennwort erforderlich**. Geben Sie das Kennwort ein, und bestätigen Sie es.
6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

- **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Berechtigung "Unabhängiger Modus" von OfficeScan Agent

Gewähren Sie bestimmten Benutzern die Berechtigung "Unabhängiger Modus" von OfficeScan Agent, wenn Agent-Server-Ereignisse die Aufgaben des Benutzers behindern. Wenn ein Benutzer beispielsweise häufig Präsentationen zeigt, kann er vor Beginn der Präsentation den unabhängigen Modus aktivieren und so verhindern, dass der OfficeScan Server OfficeScan Agent-Einstellungen verteilt und Suchläufe auf dem OfficeScan Agent startet.

Wenn für OfficeScan Agents der abhängige Modus aktiviert ist:

- OfficeScan Agents senden keine Protokolle an den OfficeScan Server, selbst wenn die Agents mit dem Server verbunden sind.
- Der OfficeScan Server startet keine Aufgaben und verteilt keine OfficeScan Agent-Einstellungen auf die Agents, selbst wenn die Agents mit dem Server verbunden sind.
- OfficeScan Agents aktualisieren Komponenten, wenn Sie eine Verbindung zu einer ihrer Update-Adressen herstellen können. Zu den Quellen zählen der OfficeScan Server, Update Agents oder eine benutzerdefinierte Update-Adresse.

  Die folgenden Ereignisse lösen ein Update auf unabhängigen Agents aus:

  - Der Benutzer führt ein manuelles Update aus.
  - Das automatische Agent-Update wird ausgeführt. Sie können automatische Agent-Updates auf unabhängigen Agents deaktivieren.

Weitere Informationen finden Sie unter *Deaktivieren automatischer Agent-Updates auf unabhängigen Agents auf Seite 15-22*.

- Ein zeitgesteuertes Update wird ausgeführt. Zeitgesteuerte Updates können nur von Agents mit den erforderlichen Berechtigungen ausgeführt werden. Sie können diese Berechtigung jederzeit widerrufen.

  Weitere Informationen finden Sie unter *Widerrufen der Berechtigung für zeitgesteuerte Updates auf unabhängigen Agents auf Seite 15-22*.

Gewähren der Agent-Berechtigung "Unabhängiger Modus"

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Wechseln Sie auf der Registerkarte **Berechtigungen** zum Abschnitt **Unabhängiger Modus**.
5. Wählen Sie die Option **Unabhängigen Modus aktivieren** aus.
6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Deaktivieren automatischer Agent-Updates auf unabhängigen Agents

Prozedur

1. Navigieren Sie zu **Updates** > **Agents** > **Automatisches Update**.
2. Navigieren Sie zum Abschnitt **Ereignisbedingtes Update**.
3. Deaktivieren Sie die Option **Unabhängige und Offline-Agents berücksichtigen**.

Hinweis

Diese Option wird automatisch deaktiviert, wenn Sie die Option **Komponenten-Update auf den Agents sofort nach dem Download einer neuen Komponente auf dem OfficeScan Server starten** deaktivieren.

Widerrufen der Berechtigung für zeitgesteuerte Updates auf unabhängigen Agents

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), oder wählen Sie bestimmte Domänen oder Agents aus.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Navigieren Sie auf der Registerkarte **Berechtigungen** zum Bereich **Komponenten-Updates**.
5. Deaktivieren Sie die Option **Zeitgesteuerte Updates aktivieren/deaktivieren**.
6. Klicken Sie auf **Speichern**.

Sprachkonfiguration für OfficeScan Agent

Sie können die Anzeige aller OfficeScan Agents unter Verwendung der OfficeScan Server-Spracheinstellungen basierend auf den Spracheinstellungen des lokal angemeldeten Benutzers konfigurieren. Nach der Installation oder dem Upgrade des OfficeScan Agent Programms wendet der Agent die auf dem Bildschirm **Globale Einstellungen** konfigurierten Spracheinstellungen an.

Wenn der OfficeScan Agent die Spracheinstellungen des angemeldeten Benutzers nicht unterstützt, wird die OfficeScan Serversprache zunächst als Standardsprache und dann Englisch verwendet.

OfficeScan Agent Spracheinstellungen konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Klicken Sie auf die Registerkarte **Agent Kontrolle**.
3. Gehen Sie zum Abschnitt **Sprachkonfiguration für Agent**.
4. Geben Sie an, wie OfficeScan Agent die Spracheinstellungen anwenden soll:
   - **Einstellungen für die lokale Sprache am Endpunkt**: Der OfficeScan Agent wird mit den Spracheinstellungen des angemeldeten Benutzers angezeigt.

     Hinweis

     Wenn der OfficeScan Agent die Spracheinstellungen des angemeldeten Benutzers nicht unterstützt, wendet der Agent die OfficeScan Server-Sprache an. Wenn der Endpunkt die OfficeScan Server-Sprache nicht unterstützt, wird die englische Sprache verwendet.

   - **OfficeScan Server-Sprache**: Der OfficeScan Agent wird mit der OfficeScan Server-Sprache angezeigt.

Hinweis

Wenn der Endpunkt die OfficeScan Server-Sprache nicht unterstützt, wird die englische Sprache verwendet.

5. Klicken Sie auf **Speichern**.

Agent Mover

Wenn es im Netzwerk mehr als einen OfficeScan Server gibt, verwenden Sie das Agent Mover-Tool, um OfficeScan Agents von einem OfficeScan Server zu einem anderen zu übertragen. Dies ist besonders dann hilfreich, wenn ein neuer OfficeScan Server eingerichtet wurde, dem OfficeScan Agents von einem vorhandenen Server zugeordnet werden sollen.

Hinweis

Beide Server müssen dieselbe Spracheinstellung haben. Wenn Sie mit Agent Mover einen OfficeScan Agent, der eine frühere Version ausführt, auf einen Server der aktuellen Version verschieben, wird der OfficeScan Agent automatisch aktualisiert.

Vergewissern Sie sich vor der Verwendung dieses Tools, dass das verwendete Konto über Administratorrechte verfügt.

Ausführen von Agent Mover

Prozedur

1. Navigieren Sie auf dem OfficeScan Server zu <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\IpXfer`.
2. Kopieren Sie die Datei `IpXfer.exe` auf den OfficeScan Agent-Endpunkt. Wenn der OfficeScan Agent-Endpunkt auf einer x64-Plattform ausgeführt wird, kopieren Sie die Datei `IpXfer_x64.exe`.
3. öffnen Sie auf dem OfficeScan Agent-Endpunkt die Eingabeaufforderung und wechseln Sie dann zu dem Ordner, in den Sie die ausführbare Datei kopiert haben.

4. Führen Sie den Agent Mover aus, indem Sie folgende Syntax eingeben:

```
<Name der ausführbaren Datei> -s <Servername> -p <Server-Listening-Port> -c <Agent-Listening-Port> -d <Domäne oder Domänenhierarchie> -e <Zertifikatsspeicherort und Dateiname> -pwd <Kennwort für die Berechtigung zum Beenden und Entsperren des Agents>
```

TABELLE 15-2. Agent Mover-Parameter

PARAMETER	ERKLÄRUNG
`<Name der ausführbaren Datei>`	`IpXfer.exe` oder `IpXfer_x64.exe`
`-s <Servername>`	Der Name des OfficeScan Zielservers (der Server, dem der OfficeScan Agent zugeordnet werden soll)
`-p <Server-Listening-Port>`	Der Listening-Port (oder vertrauenswürdige Port) des OfficeScan Zielservers (nur für lokale Server) Klicken Sie im Hauptmenü auf **Administration** > **Einstellungen** > **Agent-Verbindung**, um den Listening-Port auf der OfficeScan Webkonsole anzuzeigen.
`-sp <Server-HTTPS-Listening-Port>`	Der Listening-Port (oder vertrauenswürdige Port) des OfficeScan Zielservers (nur für SaaS-Server)
`-c <Agent-Listening-Port>`	Die Portnummer, die vom OfficeScan Agent-Endpunkt zur Kommunikation mit dem Server verwendet wird.
`-d <Domäne oder Domänenhierarchie>`	Die Domäne oder Subdomäne der Agent-Hierarchie, unter der der Agent gruppiert werden soll. Die Domänenhierarchie sollte die Subdomäne angeben.

PARAMETER	ERKLÄRUNG
`-e <Speicherort des Zertifikats und Dateiname>`	Importiert während des Verschiebungsprozesses ein neues Authentifizierungszertifikat für den OfficeScan Agent Wenn dieser Parameter nicht verwendet wird, ruft der OfficeScan Agent automatisch das aktuelle Authentifizierungszertifikat aus dem neuen Verwaltungsserver ab. **Hinweis** Der Speicherort für das Zertifikat liegt standardmäßig auf dem OfficeScan Server unter: <*Installationsordner des Servers*>`\PCCSRV\Pccnt\Common\OfcNTCer.dat`. Stellen Sie bei der Verwendung eines Zertifikats aus einer anderen Quelle als OfficeScan sicher, dass das Zertifikat im DER-Format (Distinguished Encoding Rules) vorliegt.
`-pwd <Kennwort für die Berechtigung zum Beenden und Entsperren des Agents>`	Das unter "Berechtigungen und andere Einstellungen" konfigurierte Kennwort für die Berechtigung zum Beenden und Entsperren des Agents **Hinweis** Wenn das Kennwort zum Beenden und Entsperren benötigt wird und Sie das Kennwort nicht bereitstellen, werden Sie von Agent Mover vor dem Verschieben der Agents zur Eingabe des Kennworts aufgefordert.
`-dbg`	Ermöglicht die Debug-Protokollierung der Verbindung

Beispiele:

- Für lokale OfficeScan Server-Installationen:

```
ipXfer.exe -s Server01 -p 8080 -c 21112 -d Workgroup -
pwd unlock
```

```
ipXfer_x64.exe -s Server02 -p 8080 -c 21112 -d Workgroup
\Group01 -pwd unlock
```

- Für OfficeScan SaaS-Server:

```
ipXfer.exe -s Server01 -sp 443 -p 8080 -c 21112 -d
Workgroup -pwd unlock -dbg 1
```

5. Bestätigen Sie, dass der OfficeScan Agent ab jetzt an den anderen Server berichtet. Gehen Sie dazu folgendermaßen vor:

   a. Klicken Sie auf dem OfficeScan Agent-Endpunkt mit der rechten Maustaste auf das Symbol des OfficeScan Agent-Programms in der Taskleiste.

   b. Wählen Sie **Komponentenversionen** aus.

   c. Aktivieren Sie im Feld **Servername/-port** den OfficeScan Server, an den der OfficeScan Agent berichtet.

Hinweis

Wird der OfficeScan Agent nicht in der Agent-Hierarchie des neuen OfficeScan Servers angezeigt, der ihn nun verwaltet, starten Sie den Master Service (`ofservice.exe`) des neuen Servers neu.

Inaktive OfficeScan Agenten

Wenn Sie das OfficeScan Agent-Deinstallationsprogramm zum Entfernen des OfficeScan Agent-Programms vom Endpunkte verwenden, wird der Server automatisch durch das Programm benachrichtigt. Wenn der Server diese Benachrichtigung empfängt, wird das OfficeScan Agent-Symbol aus der agent-Hierarchie entfernt, um anzuzeigen, dass der agent nicht mehr vorhanden ist.

Wenn Sie jedoch andere Methoden zum Entfernen des OfficeScan Agents verwenden, wie beispielsweise durch die erneute Formatierung der Endpunkt-Festplatte oder das manuelle Entfernen der OfficeScan Agent-Dateien, erfolgt keine Benachrichtigung an OfficeScan und der OfficeScan Agent wird als inaktiv angezeigt. Deaktiviert der Benutzer den OfficeScan Agent über einen längeren Zeitraum, zeigt der Server den OfficeScan Agent ebenfalls als inaktiv an.

Damit in der agent-Hierarchie nur aktive agents angezeigt werden, können Sie OfficeScan so konfigurieren, dass inaktive agents automatisch aus der agent-Hierarchie gelöscht werden.

Inaktive Agents automatisch entfernen

Prozedur

1. Navigieren Sie zu **Administration** > **Einstellungen** > **Inaktive Agents**.
2. Wählen Sie **Automatisches Entfernen inaktiver Agents aktivieren**.
3. Legen Sie fest, nach wie vielen Tagen OfficeScan den OfficeScan Agent als inaktiv einstufen soll.
4. Klicken Sie auf **Speichern**.

Agent-Server-Verbindung

Der OfficeScan Agent muss ständig mit seinem übergeordneten Server verbunden sein, damit er seine Komponenten aktualisieren, Benachrichtigungen erhalten und Konfigurationsänderungen rechtzeitig übernehmen kann. Die folgenden Themen geben Auskunft darüber, wie der Verbindungsstatus des OfficeScan Agents überprüft und Verbindungsprobleme behoben werden können:

- *Agent IP-Adressen auf Seite 5-10*
- *OfficeScan Agent Symbole auf Seite 15-29*
- *Verbindung des Agents zum Server überprüfen auf Seite 15-47*
- *Verbindungsüberprüfungsprotokolle auf Seite 15-48*
- *Nicht erreichbar Agents auf Seite 15-49*

OfficeScan Agent Symbole

Das OfficeScan Agent-Symbol in der Taskleiste zeigt anhand visueller Hinweise den aktuellen Status des OfficeScan Agents an und fordert Benutzer auf, bestimmte Aktionen auszuführen. Das Symbol kann jederzeit eine entsprechende Kombination der folgenden visuellen Hinweise anzeigen.

TABELLE 15-3. Mit dem OfficeScan Agent-Symbol angezeigter OfficeScan Agent-Status

AGENT-STATUS	BESCHREIBUNG	VISUELLER HINWEIS
Agent-Verbindung mit dem OfficeScan Server	Online-Agents sind mit dem OfficeScan Server verbunden. Der Server kann Aufgaben starten und Einstellungen auf diese Agents verteilen.	Das Symbol zeigt ein Sinnbild, das einem Herzschlag ähnlich ist. Die Hintergrundfarbe ist je nach Status des Echtzeitsuchdienstes ein blauer oder roter Farbton.
	Offline-Agents wurden vom OfficeScan Server getrennt. Der Server kann diese Agents nicht verwalten.	Das Symbol zeigt ein Sinnbild, das einem ausgesetzten Herzschlag ähnlich ist. Die Hintergrundfarbe ist je nach Status des Echtzeitsuchdienstes ein blauer oder roter Farbton. Es ist möglich, den agent offline zu setzen, auch wenn dieser mit dem Netzwerk verbunden ist. Weitere Informationen zu diesem Problem finden Sie unter *Lösungen für Probleme, die durch OfficeScan Agent-Symbole angezeigt werden auf Seite 15-43*.
	Die unabhängigen Agents können möglicherweise nicht immer mit dem OfficeScan Server kommunizieren.	Das Symbol zeigt den Desktop und Signalzeichen. Die Hintergrundfarbe ist je nach Status des Echtzeitsuchdienstes ein blauer oder roter Farbton. Weitere Informationen zu agents im unabhängigen Modus finden Sie unter *Berechtigung "Unabhängiger Modus" von OfficeScan Agent auf Seite 15-20*.

Agent-Status	Beschreibung	Visueller Hinweis
Verfügbarkeit von Smart Protection Quellen	Zu den Smart Protection Quellen zählen Smart Protection Server und Trend Micro Smart Protection Network. Agents der herkömmlichen Suche verbinden sich für Web-Reputation-Abfragen mit Smart Protection Quellen. Agents der intelligenten Suche verbinden sich für Such- und Web-Reputation-Abfragen mit Smart Protection Quellen.	Das Symbol zeigt ein Häkchen, wenn eine Smart Protection Quelle verfügbar ist.
		Das Symbol zeigt einen Fortschrittsbalken, wenn keine Smart Protection Quelle verfügbar ist und der Agent versucht, eine Verbindung zu den Quellen herzustellen. Weitere Informationen zu diesem Problem finden Sie unter *Lösungen für Probleme, die durch OfficeScan Agent-Symbole angezeigt werden auf Seite 15-43*.
		Für Agents der herkömmlichen Suche wird weder ein Häkchen noch ein Fortschrittsbalken angezeigt, wenn Web Reputation auf dem Agent deaktiviert wurde.

Agent-Status	Beschreibung	Visueller Hinweis
Echtzeitsuchdienst - Status	OfficeScan verwendet den Echtzeitdienst nicht nur für die Echtzeitsuche, sondern auch für die manuelle und die zeitgesteuerte Suche. Der Dienst muss funktionieren, ansonsten ist der Agent anfällig für Sicherheitsrisiken.	Das gesamte Symbol ist blau unterlegt, wenn der Echtzeitsuchdienst funktioniert. Zur Anzeige der Suchmethode des Agents werden zwei Blautöne verwendet. • Für die herkömmliche Suche: • Für die intelligente Suche:
		Das gesamte Symbol ist rot unterlegt, wenn der Echtzeitsuchdienst deaktiviert wurde oder nicht funktioniert. Zur Anzeige der Suchmethode des Agents werden zwei Rottöne verwendet. • Für die herkömmliche Suche: • Für die intelligente Suche: Weitere Informationen zu diesem Problem finden Sie unter *Lösungen für Probleme, die durch OfficeScan Agent-Symbole angezeigt werden auf Seite 15-43*.

Agent-Status	Beschreibung	Visueller Hinweis
Echtzeitsuche - Status	Die Echtzeitsuche bietet einen proaktiven Schutz, indem Dateien auf Sicherheitsrisiken durchsucht werden, während sie erstellt, geändert oder abgerufen werden.	Es gibt keine visuellen Hinweise, wenn die Echtzeitsuche aktiviert ist.
		Wenn die Echtzeitsuche deaktiviert ist, wird das ganze Symbol mit einer roten Umrandung und einer roten diagonalen Linie dargestellt. Weitere Informationen zu diesem Problem finden Sie unter *Lösungen für Probleme, die durch OfficeScan Agent-Symbole angezeigt werden auf Seite 15-43*.
Pattern-Update - Status	Agents müssen das Pattern regelmäßig aktualisieren, um den Agent vor den neuesten Bedrohungen zu schützen.	Es gibt keine visuellen Hinweise, wenn das Pattern nicht aktuell oder leicht veraltet ist.
		Dieses Symbol zeigt ein Ausrufezeichen, wenn das Pattern stark veraltet ist. Dies bedeutet, dass das Pattern über einen längeren Zeitraum nicht aktualisiert wurde. Weitere Informationen zum Update von Agents finden Sie unter *OfficeScan Agent-Updates auf Seite 6-29*.
Status der Testlizenz für OfficeScan-Server	Online-Agents sind mit einem OfficeScan Server verbunden, der eine abgelaufene Testlizenz verwendet.	Dieses Symbol zeigt an, dass die Testlizenz auf dem OfficeScan-Server abgelaufen ist.

Intelligente Suchsymbole

Wenn OfficeScan Agents die intelligente Suche verwenden, werden entsprechend die nachfolgenden Symbole angezeigt.

TABELLE 15-4. Intelligente Suchsymbole

SYMBOL	VERBINDUNG MIT OFFICESCAN SERVER	VERFÜGBARKEIT VON SMART PROTECTION QUELLEN	ECHTZEITSUCHDIENST	ECHTZEITSUCHE
	Online	Verfügbar	Funktioniert	Aktiviert
	Online	Verfügbar	Funktioniert	Deaktiviert
	Online	Verfügbar	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig
	Online	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert
	Online	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Deaktiviert
	Online	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig
	Offline	Verfügbar	Funktioniert	Aktiviert
	Offline	Verfügbar	Funktioniert	Deaktiviert
	Offline	Verfügbar	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig

Symbol	Verbindung mit OfficeScan Server	Verfügbarkeit von Smart Protection Quellen	Echtzeitsuchdienst	Echtzeitsuche
	Offline	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert
	Offline	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Deaktiviert
	Offline	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig
	Unabhängig	Verfügbar	Funktioniert	Aktiviert
	Unabhängig	Verfügbar	Funktioniert	Deaktiviert
	Unabhängig	Verfügbar	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig
	Unabhängig	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert
	Unabhängig	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Deaktiviert
	Unabhängig	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig

Herkömmliche Suchsymbole

Wenn OfficeScan Agents die herkömmliche Suche verwenden, werden entsprechend die nachfolgenden Symbole angezeigt.

TABELLE 15-5. Herkömmliche Suchsymbole

SYMBOL	VERBINDUNG MIT OFFICESCAN SERVER	WEB-REPUTATION-DIENSTE ZUR VERFÜGUNG GESTELLT VON SMART PROTECTION QUELLEN	ECHTZEITSUCHDIENST	ECHTZEITSUCHE	VIREN-PATTERN
	Online	Verfügbar	Funktioniert	Aktiviert	Aktuell oder leicht veraltet
	Online	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert	Aktuell oder leicht veraltet
	Online	Verfügbar	Funktioniert	Aktiviert	Stark veraltet
	Online	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert	Stark veraltet
	Online	Verfügbar	Funktioniert	Deaktiviert	Aktuell oder leicht veraltet
	Online	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Deaktiviert	Aktuell oder leicht veraltet
	Online	Verfügbar	Funktioniert	Deaktiviert	Stark veraltet

Symbol	Verbindung mit OfficeScan Server	Web-Reputation-Dienste zur Verfügung gestellt von Smart Protection Quellen	Echtzeitsuchdienst	Echtzeitsuche	Viren-Pattern
	Online	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Deaktiviert	Stark veraltet
	Online	Verfügbar	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Aktuell oder leicht veraltet
	Online	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Aktuell oder leicht veraltet
	Online	Verfügbar	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Stark veraltet
	Online	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Stark veraltet
	Offline	Verfügbar	Funktioniert	Aktiviert	Aktuell oder leicht veraltet
	Offline	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert	Aktuell oder leicht veraltet
	Offline	Verfügbar	Funktioniert	Aktiviert	Stark veraltet

Symbol	Verbindung mit OfficeScan Server	Web-Reputation-Dienste zur Verfügung gestellt von Smart Protection Quellen	Echtzeitsuchdienst	Echtzeitsuche	Viren-Pattern
	Offline	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert	Stark veraltet
	Offline	Verfügbar	Funktioniert	Deaktiviert	Aktuell oder leicht veraltet
	Offline	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Deaktiviert	Aktuell oder leicht veraltet
	Offline	Verfügbar	Funktioniert	Deaktiviert	Stark veraltet
	Offline	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Deaktiviert	Stark veraltet
	Offline	Verfügbar	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Aktuell oder leicht veraltet
	Offline	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Aktuell oder leicht veraltet
	Offline	Verfügbar	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Stark veraltet

Symbol	Verbindung mit OfficeScan Server	Web-Reputation-Dienste zur Verfügung gestellt von Smart Protection Quellen	Echtzeitsuchdienst	Echtzeitsuche	Viren-Pattern
	Offline	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Stark veraltet
	Unabhängig	Verfügbar	Funktioniert	Aktiviert	Aktuell oder leicht veraltet
	Unabhängig	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert	Aktuell oder leicht veraltet
	Unabhängig	Verfügbar	Funktioniert	Aktiviert	Stark veraltet
	Unabhängig	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert	Stark veraltet
	Unabhängig	Verfügbar	Funktioniert	Deaktiviert	Aktuell oder leicht veraltet
	Unabhängig	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Deaktiviert	Aktuell oder leicht veraltet
	Unabhängig	Verfügbar	Funktioniert	Deaktiviert	Stark veraltet

Symbol	Verbindung mit OfficeScan Server	Web-Reputation-Dienste zur Verfügung gestellt von Smart Protection Quellen	Echtzeitsuchdienst	Echtzeitsuche	Viren-Pattern
	Unabhängig	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Deaktiviert	Stark veraltet
	Unabhängig	Verfügbar	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Aktuell oder leicht veraltet
	Unabhängig	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Aktuell oder leicht veraltet
	Unabhängig	Verfügbar	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Stark veraltet
	Unabhängig	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Stark veraltet
	Online	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Funktioniert	Aktiviert	Aktuell oder leicht veraltet
	Online	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Funktioniert	Aktiviert	Stark veraltet

Symbol	Verbindung mit OfficeScan Server	Web-Reputation-Dienste zur Verfügung gestellt von Smart Protection Quellen	Echtzeitsuchdienst	Echtzeitsuche	Viren-Pattern
	Online	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Funktioniert	Deaktiviert	Aktuell oder leicht veraltet
	Online	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Funktioniert	Deaktiviert	Stark veraltet
	Online	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Aktuell oder leicht veraltet
	Online	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Stark veraltet
	Offline	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Funktioniert	Aktiviert	Aktuell oder leicht veraltet
	Offline	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Funktioniert	Aktiviert	Stark veraltet
	Offline	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Funktioniert	Deaktiviert	Aktuell oder leicht veraltet

Symbol	Verbindung mit OfficeScan Server	Web-Reputation-Dienste zur Verfügung gestellt von Smart Protection Quellen	Echtzeitsuchdienst	Echtzeitsuche	Viren-Pattern
	Offline	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Funktioniert	Deaktiviert	Stark veraltet
	Offline	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Aktuell oder leicht veraltet
	Offline	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Stark veraltet
	Unabhängig	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Funktioniert	Aktiviert	Aktuell oder leicht veraltet
	Unabhängig	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Funktioniert	Aktiviert	Stark veraltet
	Unabhängig	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Funktioniert	Deaktiviert	Aktuell oder leicht veraltet
	Unabhängig	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Funktioniert	Deaktiviert	Stark veraltet

Symbol	Verbindung mit OfficeScan Server	Web-Reputation-Dienste zur Verfügung gestellt von Smart Protection Quellen	Echtzeitsuchdienst	Echtzeitsuche	Viren-Pattern
	Unabhängig	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Aktuell oder leicht veraltet
	Unabhängig	Nicht zutreffend (Web-Reputation-Funktion auf Agent deaktiviert)	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Stark veraltet

Lösungen für Probleme, die durch OfficeScan Agent-Symbole angezeigt werden

Führen Sie die notwendigen Aktionen durch, wenn das OfficeScan Agent-Symbol einen der folgenden Zustände anzeigt:

Bedingung:	Beschreibung
Die Pattern-Datei wurde seit längerem nicht aktualisiert	OfficeScan Agent Benutzer müssen die Komponenten aktualisieren. über die Webkonsole können Sie die Einstellungen für das Komponenten-Update unter **Updates** > **Agents** > **Automatisches Update** konfigurieren oder den Benutzern unter **Agents** > **Agent-Verwaltung > Einstellungen** > **Berechtigungen und andere Einstellungen** > **Berechtigungen (Registerkarte)** > **Komponenten-Updates** die Berechtigung zum Aktualisieren erteilen.
Der Echtzeitsuchdienst wurde deaktiviert oder funktioniert nicht	Wenn der Echtzeitsuchdienst (OfficeScan NT RealTime Scan) deaktiviert wurde oder nicht funktioniert, müssen Benutzer den Dienst manuell über die Microsoft Management-Konsole starten.

BEDINGUNG:	BESCHREIBUNG
Die Echtzeitsuche wurde deaktiviert	Aktivieren Sie die Echtzeitsuche über die Webkonsole (**Agents** > **Agent-Verwaltung > Einstellungen** > **Sucheinstellungen** > **Echtzeitsuche - Einstellungen**).
Die Echtzeitsuche wurde deaktiviert und der OfficeScan Agent befindet sich im unabhängigen Modus	Benutzer müssen zuerst den unabhängigen Modus deaktivieren. Danach kann die Echtzeitsuche über die Webkonsole aktiviert werden.
Der OfficeScan Agent ist mit dem Netzwerk verbunden, wird aber als offline angezeigt.	überprüfen Sie über die Webkonsole zunächst die Verbindung (**Agents** > **Verbindungsüberprüfung**) und dann die Verbindungsüberprüfungsprotokolle (**Protokolle** > **Agents** > **Verbindungsüberprüfungsprotokolle**). Ist der OfficeScan Agent nach dieser überprüfung weiterhin offline: 1. Lautet der Verbindungsstatus sowohl auf dem Server als auch auf dem OfficeScan Agent „offline“, überprüfen Sie die Netzwerkverbindung. 2. Lautet der Verbindungsstatus auf dem OfficeScan Agent „offline“ und auf dem Server „online“, hat sich der Domänenname des Servers unter Umständen geändert und der OfficeScan Agent stellt eine Verbindung zum Server unter Verwendung dieses Namens her (wenn Sie den Domänennamen während der Installation ausgewählt haben). Registrieren Sie den Domänennamen des OfficeScan Servers beim DNS- bzw. WINS-Server oder fügen Sie den Domänennamen und die IP-Angaben zur Datei "Hosts" in folgendem Ordner auf dem Agent-Endpunkt hinzu:`<Windows-Ordner>\system32\drivers\etc` 3. Lautet der Verbindungsstatus auf dem OfficeScan Agent „online“, aber auf dem Server „offline“, überprüfen Sie die Einstellungen der OfficeScan Firewall. Die Firewall sperrt möglicherweise die Server-Agent-Kommunikation, während sie die Agent-Server-Kommunikation zulässt. 4. Lautet der Verbindungsstatus auf dem OfficeScan Agent „online“, aber auf dem Server „offline“, hat sich möglicherweise die IP-Adresse des OfficeScan Agents

BEDINGUNG:	BESCHREIBUNG
	geändert, ohne dass dessen Status auf dem Server aktualisiert wurde (beispielsweise beim Neustart des agents). Versuchen Sie, den OfficeScan Agent erneut zu verteilen.
Smart Protection Quellen sind nicht verfügbar	Führen Sie die nachfolgenden Aufgaben aus, wenn die Verbindung des Agents zu Smart Protection Quellen getrennt wird: 1. Navigieren Sie auf der Webkonsole zum Fenster **Endpunktspeicherort** (**Agents** > **Endpunktspeicherort**), und überprüfen Sie, ob die folgenden Einstellungen des Endpunkt-Standorts richtig konfiguriert sind: • Referenzserver und Portnummern • Gateway-IP-Adressen 2. Navigieren Sie auf der Webkonsole zum Fenster „Smart Protection Quellen“ (**Administration** > **Smart Protection** > **Smart Protection Quellen**), und führen Sie anschließend die folgenden Aufgaben aus: a. überprüfen Sie, ob die Einstellungen des Smart Protection Servers auf der standardmäßigen oder der benutzerdefinierten Liste der Quellen korrekt sind. b. überprüfen Sie, ob eine Verbindung zu den Servern hergestellt werden kann. c. Klicken Sie nach der Konfiguration der Liste der Quellen auf **Alle Agents benachrichtigen**. 3. überprüfen Sie, ob die folgenden Konfigurationsdateien auf dem Smart Protection Server und dem OfficeScan Agent synchronisiert wurden: • `sscfg.ini` • `ssnotify.ini` 4. öffnen Sie den Registrierungseditor, und überprüfen Sie, ob der Agent mit dem Unternehmensnetzwerk verbunden ist. Schlüssel: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\iCRC Scan\Scan Server`

BEDINGUNG:	BESCHREIBUNG
	• Bei `LocationProfile=1` ist der OfficeScan Agent mit dem Netzwerk verbunden und sollte mit einem Smart Protection Server eine Verbindung herstellen können. • Bei `LocationProfile=2` ist der OfficeScan Agent nicht mit dem Netzwerk verbunden und sollte mit dem Smart Protection Network eine Verbindung herstellen können. überprüfen Sie von Internet Explorer aus, ob der OfficeScan Agent-Endpunkt Webseiten im Internet aufrufen kann. 5. überprüfen Sie interne und externe Proxy-Einstellungen, die zur Verbindung mit dem Smart Protection Network und den Smart Protection Servern verwendet werden. Weitere Informationen finden Sie unter *Proxy-Einstellungen für internen Agent konfigurieren auf Seite 15-56* und *Proxy-Einstellungen für externen Agent konfigurieren auf Seite 15-57*. 6. Stellen Sie für Agents der herkömmlichen Suche unter Windows XP, Server 2003 und Server 2008 sicher, dass der OfficeScan NT Proxy Service (`TmProxy.exe`) ausgeführt wird. Wenn dieser Dienst angehalten wird, können sich Agents nicht mit Smart Protection Quellen für Web Reputation verbinden. Stellen Sie für Agents der herkömmlichen Suche unter Windows 7, Server 2012 und neueren Versionen sicher, dass der tmusa-Treiber ausgeführt wird. Wenn dieser Treiber angehalten wird, können sich Agents nicht mit Smart Protection Quellen für Web Reputation verbinden.

Verbindung des Agents zum Server überprüfen

Der Verbindungsstatus des agents mit dem OfficeScan Server wird in der agent-Hierarchie der OfficeScan Webkonsole angezeigt.

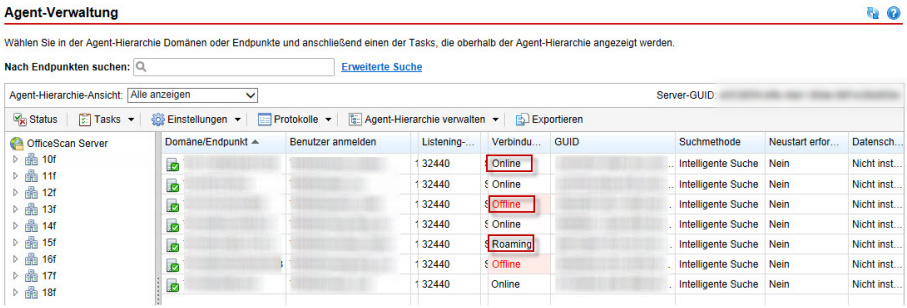


ABBILDUNG 15-2. Agent-Hierarchie mit der Anzeige des Verbindungsstatus des agents mit dem OfficeScan Server

Bestimmte Umstände können jedoch dazu führen, dass der agent-Verbindungsstatus in der agent-Hierarchie nicht richtig angezeigt wird. Wenn Sie beispielsweise versehentlich die Netzwerkverbindung des agent-Endpunkts trennen, kann der agent den Server nicht darüber informieren, dass er offline ist. Dieser agent erscheint somit in der agent-Ansicht weiterhin als online.

Überprüfen Sie die agent-Server-Verbindung manuell oder lassen Sie OfficeScan eine zeitgesteuerte Überprüfung durchführen. Es ist nicht möglich, bestimmte Domänen oder agents auszuwählen und dann ihren Verbindungsstatus zu überprüfen. OfficeScan überprüft den Verbindungsstatus aller registrierten agents.

Verbindungen des Agents zum Server überprüfen

Prozedur

1. Navigieren Sie zu **Agents** > **Verbindungsüberprüfung**.
2. Um die agent-Server-Verbindung manuell zu überprüfen, öffnen Sie die Registerkarte **Manuelle Überprüfung**, und klicken Sie auf **Jetzt überprüfen**.

3. Um die agent-Server-Verbindung automatisch zu überprüfen, wechseln Sie zur Registerkarte **Zeitgesteuerte Überprüfung**.

   a. Klicken Sie auf **Zeitgesteuerte Überprüfung aktivieren**.

   b. Wählen Sie das Überprüfungsintervall und die Startzeit.

   c. Mit **Speichern** wird der Zeitplan gespeichert.

4. Überprüfen Sie den Status in der agent-Hierarchie, oder zeigen Sie die Protokolle zur Verbindungsüberprüfung an.

Verbindungsüberprüfungsprotokolle

Anhand der Verbindungsüberprüfungsprotokolle von OfficeScan können Sie feststellen, ob der OfficeScan Server mit allen registrierten agents kommunizieren kann. OfficeScan erstellt bei jeder Überprüfung der agent-Server-Verbindung über die Webkonsole einen Protokolleintrag.

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell, oder konfigurieren Sie eine zeitgesteuerte Löschung der Protokolle. Weitere Informationen zur Protokollverwaltung finden Sie unter *Protokollmanagement auf Seite 14-47*.

Verbindungsüberprüfungsprotokolle anzeigen

Prozedur

1. Navigieren Sie zu **Protokolle** > **Agents** > **Verbindungsüberprüfungsprotokolle**.

2. Die Ergebnisse der Verbindungsüberprüfung können Sie in der Spalte **Status** anzeigen.

3. Wenn Sie das Protokoll als komma-separierte Datei (`CSV-Datei`) speichern möchten, klicken Sie auf **In CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Nicht erreichbar Agents

OfficeScan Agents Agents in nicht erreichbaren Netzwerken, z. B. solche in Netzwerksegmenten hinter einem NAT-Gateway, sind fast immer offline, da der Server keine direkte Verbindung zu diesen agents aufbauen kann. Demzufolge kann der Server diese agents nicht über folgende durchzuführende Aktionen benachrichtigen:

- Neueste Komponenten herunterladen.
- Auf der Webkonsole konfigurierte agent-Einstellungen übernehmen. Wenn Sie beispielsweise auf der Webkonsole die Häufigkeit der zeitgesteuerten Suche ändern, benachrichtigt der Server die agents umgehend und fordert sie auf, die neuen Einstellungen zu übernehmen.

Nicht erreichbare agents können diese Aufgaben daher nicht zeitnah durchführen. Sie führen sie nur dann durch, wenn sie eine Verbindung zum Server herstellen. Dies geschieht:

- Wenn sie sich beim Server nach der Installation registrieren.
- Wenn sie neu gestartet oder geladen werden. Dieses Ereignis tritt nicht regelmäßig ein und erfordert in der Regel das Eingreifen des Benutzers.
- Wenn auf dem agent ein manuelles oder zeitgesteuertes Update ausgelöst wird. Auch dieses Ereignis tritt nicht regelmäßig ein.

Nur während der Registrierung, des Neustarts oder des Neuladens "erkennt" der Server die Konnektivität der agents und behandelt sie als online. Da der Server jedoch noch immer keine Verbindung zu den agents herstellen kann, ändert er ihren Status umgehend in "Offline".

OfficeScan stellt Rückmeldungs- und Serverabfragefunktionen zur Verfügung, um Probleme mit nicht erreichbaren agents zu beheben. Auf Grund dieser Funktionen unterlässt der Server es, agents über Komponenten-Updates und Einstellungsänderungen zu benachrichtigen. Stattdessen übernimmt der Server eine passive Rolle und wartet darauf, dass die agents Rückmeldungen senden oder Abfragen initiieren. Wenn der Server eines dieser Ereignisse erkennt, behandelt er die agents als online.

Hinweis

AgentAndere Agent-initiierte Ereignisse als Rückmeldungen und Serverabfragen, beispielsweise manuelles agent-Update und Senden der Protokolle, lösen im Server nicht die Aktualisierung des agents-Status "Nicht erreichbar" aus.

Rückmeldung

OfficeScan Agents senden Rückmeldenachrichten, um den Server zu informieren, dass die Verbindung vom agent aus funktionstüchtig bleibt. Nach dem Erhalt einer Rückmeldung behandelt der Server den agent als online. In der agent-Hierarchie kann der agent-Status wie folgt lauten:

- **Online**: Bei regulären Online-agents
- **Nicht erreichbar/Online**: Bei Online-agents im nicht erreichbaren Netzwerk

Hinweis

OfficeScan Agents aktualisieren keine Komponente und wenden keine neuen Einstellungen an, wenn sie Rückmeldungen senden. Reguläre agents führen diese Aufgaben bei Routine-Updates durch (siehe *OfficeScan Agent-Updates auf Seite 6-29*). Agents im nicht erreichbaren Netzwerk führen diese Aufgaben während der Serverabfragen durch.

Mit der Rückmeldefunktion wird das Problem behoben, dass OfficeScan Agents in nicht erreichbaren Netzwerken auch dann als offline erscheinen, wenn sie eine Verbindung zum Server aufbauen können.

Eine Einstellung auf der Webkonsole steuert, wie oft agents Rückmeldungen senden. Falls der Server keine Rückmeldung erhält, behandelt er den agent nicht sofort als offline. Eine andere Einstellung steuert, wie viel Zeit ohne Rückmeldung vergehen muss, bis der agent folgende Status annimmt:

- **Offline**: Bei regulären Offline-OfficeScan Agents
- **Nicht erreichbar/Offline**: Bei Offline-OfficeScan Agents im nicht erreichbaren Netzwerk

Bei der Einstellung der Rückmeldungen ist zu berücksichtigen, dass einerseits die neuesten Statusinformationen des agents angezeigt, andererseits aber auch die

Systemressourcen effizient gehandhabt werden müssen. Für die meisten Situationen genügt die Standardeinstellung. Berücksichtigen Sie jedoch Folgendes, wenn Sie Änderungen an den Rückmeldeeinstellungen vornehmen:

TABELLE 15-6. Empfehlungen für Rückmeldungen

ZEITINTERVALL FÜR RÜCKMELDUNGEN	EMPFEHLUNG
Lange Intervalle zwischen Rückmeldungen (mehr als 60 Minuten)	Je länger das Intervall zwischen den Rückmeldungen ist, desto größer ist die Anzahl der Ereignisse, die eintreten können, bevor der Server den agent-Status auf der Webkonsole anzeigt.
Kurze Intervalle zwischen Rückmeldungen (weniger als 60 Minuten)	Kurze Intervalle liefern einen aktuelleren agent-Status, können jedoch zu einer höheren Bandbreitenauslastung führen.

Serverabfrage

Mit der Serverabfragefunktion wird das Problem behoben, dass Benachrichtigungen über Komponenten-Updates und Änderungen an agent-Einstellungen von nicht erreichbaren OfficeScan Agents nicht zeitnah empfangen werden. Diese Funktion arbeitet unabhängig von der Rückmeldefunktion.

Mit der Serverabfragefunktion:

- OfficeScan Agents initiieren automatisch in regelmäßigen Intervallen eine Verbindung zum OfficeScan Server. Wenn der Server bemerkt, dass eine Abfrage stattgefunden hat, behandelt er den agent als "Nicht erreichbar/Online".

- OfficeScan Agents stellen eine Verbindung zu einer oder mehreren ihrer Update-Adressen her, um alle aktualisierten Komponenten herunterzuladen und neue agent-Einstellungen zu übernehmen. Wenn es sich bei der primären Update-Adresse um den OfficeScan Server oder einen Update-Agent handelt, beziehen die agents sowohl aktualisierte Komponenten als auch neue Einstellungen. Handelt es sich bei der Update-Adresse nicht um den OfficeScan Server oder einen Update-Agent, beziehen die agents nur die aktualisierten Komponenten und verbinden sich

dann mit dem OfficeScan Server oder dem Update-Agent, um die neuen Einstellungen abzurufen.

Rückmeldungs- und Serverabfragefunktionen konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Klicken Sie auf die Registerkarte **Netzwerk**.
3. Gehen Sie zum Abschnitt **Nicht erreichbares Netzwerk**.
4. Konfigurieren Sie die Server-Abfrage-Einstellungen.

   Weitere Informationen zum Abfragen des Servers finden Sie unter *Serverabfrage auf Seite 15-51*.

   a. Wenn der OfficeScan Server sowohl über eine IPv4- als auch über eine IPv6-Adresse verfügt, können Sie einen IPv4-Adressraum sowie ein IPv6-Präfix und eine IPv6-Länge angeben.

      Geben Sie einen IPv4-Adressraum an, wenn es ein reiner IPv4-Server ist, oder ein IPv6-Präfix und eine IPv6-Länge, wenn es sich um einen reinen IPv6-Server handelt.

      Wenn die IP-Adresse eines Agents mit einer IP-Adresse in dem Bereich übereinstimmt, wendet der Agent die Einstellung zu Rückmeldung und Serverabfrage an und der Server behandelt den Agent als Teil des nicht erreichbaren Netzwerks.

      Hinweis

      Agents mit einer IPv4-Adresse können sich mit einem reinen IPv4- oder Dual-Stack-OfficeScan Server verbinden.

      Agents mit einer IPv6-Adresse können sich mit einem reinen IPv6- oder Dual-Stack-OfficeScan Server verbinden.

      Dual-Stack-Agents können sich mit einem Dual-Stack-, einem reinen IPv4- oder einem reinem IPv6-OfficeScan Server verbinden.

b. Geben Sie unter **Agents fragen den Server alle __ Minute(n) nach aktualisierten Komponenten und Einstellungen ab** die Häufigkeit der Abfrage an. Geben Sie einen Wert zwischen 1 und 129600 Minuten ein.

Tipp

Trend Micro empfiehlt, das Serverabfrageintervall dreimal so groß wie das Rückmeldeintervall zu definieren.

5. Konfigurieren Sie die Rückmeldungseinstellungen.

   Weitere Informationen über die Rückmeldungsfunktion finden Sie unter *Rückmeldung auf Seite 15-50*.

   a. Wählen Sie **Agents dürfen Rückmeldungen an den Server senden** aus.

   b. Wählen Sie **Alle Agents** oder **Nur Agents im nicht erreichbaren Netzwerk** aus.

   c. Geben Sie unter **Agents senden Rückmeldungen alle __ Minute(n)** an, wie oft Agents eine Rückmeldung senden sollen. Geben Sie einen Wert zwischen 1 und 129600 Minuten ein.

   d. Geben Sie unter **Der Agent ist offline, wenn keine Rückmeldung eingeht nach __ Minute(n)** an, wie viel Zeit ohne eine Rückmeldung vergehen muss, bis der OfficeScan Server einen Agent als offline einstuft. Geben Sie einen Wert zwischen 1 und 129600 Minuten ein.

6. Klicken Sie auf **Speichern**.

OfficeScan Agent Proxy-Einstellungen

In der folgenden Tabelle sind die OfficeScan Agent-Proxy-Einstellungen aufgeführt, die für die Verbindung mit internen und externen Servern verfügbar sind.

Proxy-Konfiguration	Beschreibung
Interne Agents	Konfigurieren Sie die Proxy-Einstellungen für interne Agents für Verbindungen zu den folgenden Servern: • OfficeScan Server: Auf dem Servercomputer befinden sich der OfficeScan Server und der integrierte Smart Protection Server. OfficeScan Agents bauen eine Verbindung zum OfficeScan Server auf, um Komponenten zu aktualisieren, Konfigurationseinstellungen abzurufen und Protokolle zu senden. OfficeScan Agents bauen eine Verbindung zum integrierten Smart Protection Server auf, um Suchanfragen zu senden. • Smart Protection Server: Smart Protection Server umfassen alle eigenständigen Smart Protection Server und den integrierten Smart Protection Server anderer OfficeScan Server. OfficeScan Agents stellen eine Verbindung zu den Servern her, um Such- und Web-Reputation-Abfragen zu senden. Weitere Informationen finden Sie unter *Proxy-Einstellungen für internen Agent konfigurieren auf Seite 15-56*.
Externe Agents	Externe OfficeScan Agents verwenden die Proxy-Einstellungen, die in Internet Explorer konfiguriert wurden, um eine Verbindung zum Trend Micro Smart Protection Network herzustellen. Weitere Informationen finden Sie unter *Proxy-Einstellungen für externen Agent konfigurieren auf Seite 15-57*.

Proxy-Konfiguration	Beschreibung
Global Smart Protection Service	OfficeScan Agents verwenden die konfigurierten Proxy-Einstellungen für den Smart Protection Dienst, wenn Smart Protection Quellen auf folgende Funktionen abgefragt werden: • Vorausschauendes Maschinenlernen • Verhaltensüberwachung **Hinweis** Wenn der integrierte Smart Protection Server nicht verfügbar ist, stellen OfficeScan Agents beim Durchführen von Abfragen eine Verbindung zum Trend Micro Smart Protection Network her. Weitere Informationen finden Sie unter *Konfigurieren der Proxy-Einstellungen des Global Smart Protection Service auf Seite 15-58*.
Proxy-Berichtigung für Agent-Benutzer	Sie können agent-Benutzern die Berechtigung zur Konfiguration der Proxy-Einstellungen erteilen. OfficeScan Agents verwenden benutzerdefinierte Proxy-Einstellungen nur in folgenden Fällen: • Wenn OfficeScan Agents "Jetzt aktualisieren" ausführen. • Wenn die automatischen Proxy-Einstellungen von den Benutzern deaktiviert oder vom OfficeScan Agent nicht erkannt werden. **Warnung!** Vom Benutzer fehlerhaft konfigurierte Proxy-Einstellungen können zu Update-Problemen führen. Gehen Sie mit Bedacht vor, wenn Sie Benutzern die Erlaubnis zur Konfiguration der Proxy-Einstellungen geben. Weitere Informationen finden Sie unter *Proxy-Konfiguration, Berechtigungen gewähren auf Seite 15-59*.

Proxy-Einstellungen für internen Agent konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Einstellungen** > **Proxy**.
2. Klicken Sie auf die Registerkarte **Agent**.
3. Gehen Sie zum Abschnitt **Interner Proxy**.
4. Wählen Sie den Typ der Proxy-Einstellungen aus, den interne OfficeScan Agents verwenden, wenn sie eine Verbindung zum OfficeScan Server oder zu Smart Protection Servern herstellen.

   - **Kein Proxy**: Interne OfficeScan Agents benötigen keinen Proxy-Server, um eine Verbindung zum OfficeScan Server oder zu Smart Protection Servern herzustellen.
   - **Windows-Proxy-Einstellungen verwenden**: Interne Agents verwenden die in den Windows-Internetoptionen konfigurierten Proxy-Servereinstellungen, wenn sie eine Verbindung zum OfficeScan Server oder zu den Smart Protection Servern herstellen.

     Hinweis

     Geben Sie bei Bedarf Proxy-Authentifizierungsdaten an.

   - **Mehrere Proxy-Server verwenden**: Interne Agents verwenden verschiedene Proxy-Server, wenn sie eine Verbindung zum OfficeScan Server oder zu Smart Protection Servern herstellen.

     Für OfficeScan Server-Verbindungen:

     a. Wählen Sie **OfficeScan Agent-Proxy für die Verbindung zum internen OfficeScan Server** aus.

     b. Geben Sie den Namen des Proxy-Servers oder eine IPv4-/IPv6-Adresse und eine Portnummer an.

     c. Geben Sie bei Bedarf Proxy-Authentifizierungsdaten an.

     Für eigenständige Smart Protection Server-Verbindungen:

a. Wählen Sie **OfficeScan Agent-Proxy für die Verbindung zu eigenständigen Smart Protection Servern** aus.

b. Geben Sie den Namen des Proxy-Servers oder eine IPv4-/IPv6-Adresse und eine Portnummer an.

c. Geben Sie bei Bedarf Proxy-Authentifizierungsdaten an.

- **Automatische Proxy-Konfiguration verwenden (einschließlich PAC)**: Wählen Sie diese Option aus, um vom Administrator konfigurierte Proxy-Einstellungen über DHCP, DNS oder ein automatisches Konfigurationsskript zu verwenden.
  - **Proxy-Einstellungen des Netzwerks automatisch erkennen**: Interne Agents erkennen vom Administrator konfigurierte Proxy-Einstellungen über DHCP oder DNS.
  - **Angegebene PAC-Skriptdatei (Proxy Auto-Configuration, automatische Proxy-Konfiguration) verwenden**: Interne Agents verwenden das vom Netzwerkadministrator eingerichtete PAC-Skript (Proxy Auto-Configuration, automatische Proxy-Konfiguration), um den entsprechenden Proxy-Server zu erkennen.

Hinweis

Geben Sie die URL-Adresse für das PAC-Skript ein.

5. Klicken Sie auf **Speichern**.

Proxy-Einstellungen für externen Agent konfigurieren

Externe Agents können nur die in den Windows-Internetoptionen konfigurierten Proxy-Servereinstellungen konfigurieren, wenn sie eine Verbindung zum OfficeScan Server oder den Smart Protection Servern herstellen.

Prozedur

1. Navigieren Sie zu **Administration** > **Einstellungen** > **Proxy**.

2. Klicken Sie auf die Registerkarte **Agent**.
3. Gehen Sie zum Abschnitt **Externer Proxy**.
4. Geben Sie bei Bedarf Proxy-Authentifizierungsdaten an.
5. Klicken Sie auf **Speichern**.

Konfigurieren der Proxy-Einstellungen des Global Smart Protection Service

OfficeScan Agents verwenden die konfigurierten Proxy-Einstellungen für den Smart Protection Dienst, wenn Smart Protection Quellen auf folgende Funktionen abgefragt werden:

- Vorausschauendes Maschinenlernen
- Verhaltensüberwachung

Hinweis

Wenn der integrierte Smart Protection Server nicht verfügbar ist, stellen OfficeScan Agents beim Durchführen von Abfragen eine Verbindung zum Trend Micro Smart Protection Network her.

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Klicken Sie auf die Registerkarte **System**.
3. Wechseln Sie zum Abschnitt **Proxy für den Smart Protection Dienst**.
4. Aktivieren Sie **Smart Protection Quellen für Dienstanfragen verwenden**.

Wichtig

Der Proxy für den Smart Protection Dienst unterstützt für File Reputation-Abfragen nur das HTTPS-Protokoll. Sie müssen sicherstellen, dass alle konfigurierten Smart Protection Server, die File Reputation-Dienste bereitstellen, das HTTPS-Protokoll verwenden.

Standardmäßig verwendet der integrierte Smart Protection Server keine HTTPS-Kommunikation. Informationen zum Ändern der Kommunikationsmethode finden Sie unter *Einstellungen eines integrierten Smart Protection Servers konfigurieren auf Seite 4-22*.

Informationen zur Überprüfung der von eigenständigen Smart Protection Servern verwendeten Kommunikationsmethode finden Sie unter *Benutzerdefinierte Listen der Smart Protection Quellen konfigurieren auf Seite 4-28*.

5. Klicken Sie auf **Speichern**.

Proxy-Konfiguration, Berechtigungen gewähren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol ( ), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Navigieren Sie auf der Registerkarte **Berechtigungen** zum Abschnitt **Proxy-Einstellungen**.
5. Wählen Sie **Benutzern die Konfiguration der Proxy-Einstellungen erlauben** aus.
6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen

Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

OfficeScan Agent-Informationen anzeigen

Das Fenster "Status anzeigen" enthält u. a. wichtige Informationen zu den OfficeScan Agents, z. B. Berechtigungen, Informationen zur agent Software und Systemereignissen.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der agent-Hierarchie auf das Stammsymbol ( ), um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
3. Klicken Sie auf **Status**.
4. Erweitern Sie den Namen des agent-Endpunkt, um dessen Status anzuzeigen. Wenn mehrere agents ausgewählt sind, klicken Sie auf **Alle einblenden**, um Statusinformationen zu allen ausgewählten agents anzuzeigen.
5. (Optional) Über die Schaltfläche **Zurücksetzen** kann der Sicherheitsrisiken-Zähler auf Null zurückgesetzt werden.

Agent-Einstellungen importieren und exportieren

Mit OfficeScan können Sie Einstellungen der agent-Hierarchie, die von einem bestimmten OfficeScan Agent oder einer Domäne angewendet werden, in eine Datei

exportieren. Diese Datei können Sie dann importieren, damit die Einstellungen auf andere agents und Domänen oder einen anderen OfficeScan Server mit derselben Version angewendet werden können.

Alle Einstellungen der agent-Hierarchie, mit Ausnahme der Update-Agent-Einstellungen, werden exportiert.

Agent-Einstellungen exportieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der agent-Hierarchie auf das Stammsymbol ( ), um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen exportieren**.
4. Um die Einstellungen für die ausgewählten OfficeScan Agents oder Domänen anzuzeigen, klicken Sie auf den entsprechenden Link.
5. Klicken Sie auf **Exportieren**, um die Einstellungen zu speichern.

   Die Einstellungen werden in einer `DAT`-Datei gespeichert.
6. Klicken Sie auf **Speichern**, und geben Sie anschließend den Speicherort für die `.DAT`-Datei an.
7. Klicken Sie auf **Speichern**.

Agent-Einstellungen importieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der agent-Hierarchie auf das Stammsymbol ( ), um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.

3. Klicken Sie auf **Einstellungen** > **Einstellungen importieren**.

4. Klicken Sie auf **Durchsuchen**, um die `.dat`-Datei auf dem Endpunkt ausfindig zu machen, und klicken Sie auf **Importieren**.

   Die Seite **Einstellungen importieren** mit einer Übersicht der Einstellungen wird angezeigt.

5. Klicken Sie auf einen der Links, um Einzelheiten über die zu importierenden Sucheinstellungen oder Berechtigungen anzuzeigen.

6. Importieren Sie die Einstellungen.

   - Wenn Sie das Root-Domänen-Symbol angeklickt haben, wählen Sie **Auf alle Domänen anwenden** und dann **Auf Zielcomputer anwenden**.
   - Wenn Sie Domänen ausgewählt haben, wählen Sie **Auf alle Computer der ausgewählten Domäne(n) anwenden** und dann **Auf Ziel anwenden**.
   - Wenn Sie mehrere agents ausgewählt haben, klicken Sie auf **Auf Ziel anwenden**.

Einhaltung von Sicherheitsrichtlinien

Verwenden Sie die Einhaltung von Sicherheitsrichtlinien, um Schwachstellen zu ermitteln, Lösungen zu verteilen und die Sicherheitsinfrastruktur zu verwalten. Diese Funktion vermindert die erforderliche Zeit, um die Netzwerkumgebung zu sichern und einen Ausgleich zwischen dem Wunsch nach Sicherheit und Funktionalität in einem Unternehmen zu finden.

Einhaltung der Sicherheitsrichtlinien für zwei Endpunktetypen erzwingen:

- **Verwaltet**: Endpunkte bei OfficeScan Agents, die vom OfficeScan Server verwaltet werden. Weitere Informationen finden Sie unter *Einhaltung der Sicherheitsrichtlinien für verwaltete Agents auf Seite 15-63*.
- **Nicht verwaltet**: Darin enthalten:
  - OfficeScan Agents , die nicht vom OfficeScan Server verwaltet werden

- Endpunkte , auf denen OfficeScan Agents nicht installiert ist
- Endpunkte , die der OfficeScan Server nicht erreichen kann
- Endpunkte , deren Sicherheitsstatus nicht überprüft werden kann

Weitere Informationen finden Sie unter *Einhaltung der Sicherheitsrichtlinien für nicht verwaltete Endpunkte auf Seite 15-78*.

Einhaltung der Sicherheitsrichtlinien für verwaltete Agents

Die Einhaltung der Sicherheitsrichtlinien erstellt einen Bericht zur Einhaltung von Richtlinien, der Ihnen dabei hilft, den Sicherheitsstatus der vom OfficeScan Server verwalteten OfficeScan Agents einzuschätzen. Die Einhaltung der Sicherheitsrichtlinien erstellt diesen Bericht auf Anforderung oder gemäß Zeitplan.

Im Fenster **Manuelle Bewertung** werden die folgenden Registerkarten angezeigt:

- **Dienste**: Verwenden Sie diese Registerkarte, um zu überprüfen, ob die Agent-Dienste funktionieren.

  Weitere Informationen finden Sie unter *Dienste auf Seite 15-64*.

- **Komponenten**: Verwenden Sie diese Registerkarte, um zu überprüfen, ob die OfficeScan Agents über Update-Komponenten verfügen.

  Weitere Informationen finden Sie unter *Komponenten auf Seite 15-66*.

- **Einhaltung von Suchrichtlinien**: Verwenden Sie diese Registerkarte, um zu überprüfen, ob auf den OfficeScan Agents regelmäßig die Suchfunktion ausgeführt wird.

  Weitere Informationen finden Sie unter *Einhaltung von Suchrichtlinien auf Seite 15-68*.

- **Einstellungen**: Verwenden Sie diese Registerkarte, um zu überprüfen, ob die Agent-Einstellungen mit den Einstellungen auf dem Server übereinstimmen.

  Weitere Informationen finden Sie unter *Einstellungen auf Seite 15-71*.

Hinweis

Die Registerkarte **Komponenten** zeigt OfficeScan Agents, auf denen aktuelle und frühere Produktversionen ausgeführt werden. Auf den anderen Registerkarten werden nur OfficeScan Agents angezeigt, auf denen Version 10.5, 10.6 oder OfficeScan Agents ausgeführt wird.

Wichtig

- Bei der Einhaltung der Sicherheitsrichtlinien wird der Verbindungsstatus von OfficeScan Agents abgefragt, bevor ein Bericht zur Einhaltung von Richtlinien erstellt wird. Der Bericht umfasst Online- und Offline-Agents, jedoch keine Agents im unabhängigen Modus.
- Bei rollenbasierten Benutzerkonten:
  - Für jedes Webkonsolen-Benutzerkonto gelten völlig unterschiedliche Einstellungen für den Bericht zur Einhaltung von Richtlinien. Änderungen an den Einstellungen für den Bericht zur Einhaltung von Richtlinien haben keine Auswirkung auf die Einstellungen der anderen Benutzerkonten.
  - Der Umfang des Berichts ist abhängig von den Berechtigungen der Agent-Domäne für dieses Benutzerkonto. Wenn beispielsweise das Dashboard eines Benutzerkontos die Berechtigung zur Verwaltung der Domänen A und B aufweist, werden in den Berichten des Benutzerkontos nur Daten von Agents angezeigt, die zu den Domänen A und B gehören.

    Weitere Informationen zu Benutzerkonten finden Sie unter *Rollenbasierte Administration auf Seite 14-3*.

Dienste

Die Einhaltung der Sicherheitsrichtlinien überprüft, ob die folgenden OfficeScan Agent-Dienste funktionieren:

- Virenschutz
- Anti-spyware
- Firewall
- Web Reputation

- Verhaltensüberwachung/Gerätekontrolle (auch bezeichnet als Trend Micro Unauthorized Change Prevention Service)
- Datenschutz
- Verdächtige Verbindung

Ein nicht richtlinienkonformer agent wird im Bericht zur Einhaltung von Richtlinien mindestens zwei Mal gezählt.

ABBILDUNG 15-3. Registerkarte Bericht zur Einhaltung von Richtlinien - Dienste

- In der Kategorie **Endpunkte mit nicht kompatiblen Diensten**
- In der Kategorie, in welcher der OfficeScan Agent nicht richtlinienkonform ist. Wenn zum Beispiel der Antiviren-Dienst des OfficeScan Agents nicht funktioniert, wird der agent in der Kategorie **Virenschutz** gezählt. Wenn mehr als ein Dienst nicht funktioniert, wird der agent in jeder Kategorie gezählt, in welcher er nicht richtlinienkonform ist.

Starten Sie die nicht funktionierenden Dienste über die Webkonsole oder über den OfficeScan Agent neu. Wenn die Dienste nach dem Neustart funktionieren, wird der agent bei der nächsten Bewertung nicht mehr als nicht richtlinienkonform angezeigt.

Komponenten

Die Einhaltung der Sicherheitsrichtlinien ermittelt, ob die Komponenten auf dem OfficeScan Server und den OfficeScan Agents übereinstimmen. Inkonsistenzen treten üblicherweise dann auf, wenn die Agents keine Verbindung zum Server aufbauen können, um die Komponenten zu aktualisieren. Wenn der Agent Updates von einer anderen Quelle erhält (wie etwa dem Trend Micro ActiveUpdate Server), kann es vorkommen, dass die Version der Komponente auf dem Agent neuer ist als die Version auf dem Server.

Die Einhaltung der Sicherheitsrichtlinien überprüft folgende Komponenten:

- Smart Scan Agent Pattern
- Viren-Pattern
- IntelliTrap Pattern
- IntelliTrap Ausnahme-Pattern
- Viren-Scan-Engine (32/64 Bit)
- Spyware/Grayware-Pattern
- Spyware-Aktivmonitor-Pattern
- Spyware/Grayware Scan Engine (32/64 Bit)
- Damage Cleanup Template
- Damage-Cleanup Engine 32/64 Bit
- Pattern der allgemeinen Firewall
- Allgemeiner Firewall-Treiber 32-/64-Bit
- Kerntreiber der Verhaltensüberwachung 32/64 Bit
- Kerndienst der Verhaltensüberwachung 32/64 Bit
- Pattern zur Konfiguration der Verhaltensüberwachung
- Pattern für digitale Signaturen
- Pattern der Richtliniendurchsetzung
- Erkennungs-Pattern der Verhaltensüberwachung (32/64 Bit)
- Allgemeine C&C-IP-Liste
- Pattern-Relevanzregeln
- Early Boot Cleanup Driver 32-/64-Bit
- Auslöse-Pattern zum Durchsuchen des Speichers (32/64 Bit)
- Speicher-Inspektions-Pattern
- Pattern für die Prävention von Angriffen auf Browser
- Einheitliches Skriptanalysemuster
- Muster der Programmsinspektionsüberwachung
- Schadensbehebungsmuster
- Frühstart Anti-Malware Muster 32-/64-Bit
- Maschine für Kontextbezogene Intelligenz 32/64-Bit
- Muster für kontextbezogene Intelligenz
- Abfragehandhabung für kontextbezogene Intelligenz 32/64-Bit
- Fortgeschrittenes Bedrohungssuchmaschine 32/64-Bit
- Fortgeschrittenes Bedrohungskorrelationsmuster
- Programmversion

Ein nicht richtlinienkonformer Agent wird im Bericht zur Einhaltung von Richtlinien mindestens zwei Mal gezählt.

ABBILDUNG 15-4. Registerkarte Bericht zur Einhaltung der Richtlinien - Komponenten

- In der Kategorie **Endpunkte mit inkonsistenten Komponentenversionen**
- In der Kategorie, in welcher der Agent nicht richtlinienkonform ist. Wenn beispielsweise die Version des Agent-Patterns der intelligenten Suche nicht mit der Version auf dem Server übereinstimmt, wird der Agent in der Kategorie **Agent-Pattern der intelligenten Suche** gezählt. Wenn mehr als eine Komponente nicht übereinstimmt, wird der Agent in jeder Kategorie gezählt, in welcher er nicht richtlinienkonform ist.

Um inkonsistente Komponentenversionen zu vermeiden, aktualisieren Sie veraltete Komponenten auf den Agents oder dem Server.

Einhaltung von Suchrichtlinien

Die Einhaltung von Sicherheitsrichtlinien überprüft, ob die Sofort- oder die zeitgesteuerte Suche regelmäßig ausgeführt und diese Suchläufe innerhalb einer angemessenen Zeit abgeschlossen werden.

Hinweis

Die Einhaltung der Sicherheitsrichtlinien kann den Status der zeitgesteuerten Suche nur berichten, wenn die zeitgesteuerte Suche auf den agents aktiviert ist.

Die Einhaltung der Sicherheitsrichtlinien verwendet folgende Kriterien der Einhaltung der Suchrichtlinien:

- **In den letzten (x) Tagen wurde weder eine "Jetzt durchsuchen"-Suche noch eine zeitgesteuerte Suche durchgeführt**: Der OfficeScan Agent ist nicht richtlinienkonform, wenn er innerhalb der angegebenen Anzahl von Tagen keine "Jetzt durchsuchen"-Suche oder zeitgesteuerte Suche durchgeführt hat.
- **"Jetzt durchsuchen" oder zeitgesteuerte Suche dauert länger als (x) Stunde(n)**: Der OfficeScan Agent ist nicht richtlinienkonform, wenn die "Jetzt durchsuchen"-Suche oder zeitgesteuerte Suche länger als die angegebene Anzahl von Stunden gedauert hat.

Ein nicht richtlinienkonformer agent wird im Bericht zur Einhaltung von Richtlinien mindestens zwei Mal gezählt.

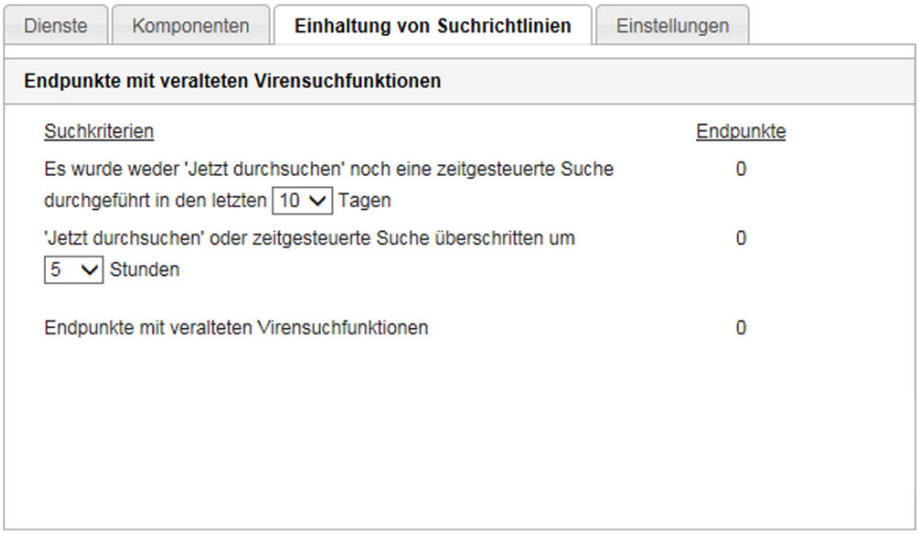


ABBILDUNG 15-5. Registerkarte Bericht zur Einhaltung von Richtlinien - Einhaltung der Suchrichtlinien

- In der Kategorie **Endpunkte mit veralteten Virensuchfunktionen**
- In der Kategorie, in welcher der agent nicht richtlinienkonform ist. Wenn die letzte zeitgesteuerte Suche zum Beispiel länger als die angegebene Anzahl von Stunden gedauert hat, wird der agent in der Kategorie **Sofortsuche oder zeitgesteuerte Suche wurde überschritten um <x> Stunden** gezählt. Wenn der agent mehr als ein Kriterium der Einhaltung von Suchrichtlinien erfüllt, wird er in jeder Kategorie gezählt, in welcher er nicht richtlinienkonform ist.

Führen Sie "Jetzt durchsuchen" oder die zeitgesteuerte Suche auf agents aus, auf denen die Suchaufgaben noch nicht ausgeführt wurden oder die nicht in der Lage waren, die Suche abzuschließen.

Einstellungen

Die Einhaltung von Sicherheitsrichtlinien stellt fest, ob Agents oder deren übergeordnete Domänen in der Agent-Hierarchie dieselben Einstellungen haben. Die Einstellungen stimmen möglicherweise nicht überein, wenn Sie einen Agent in eine andere Domäne mit anderen Einstellungen verschieben oder wenn ein Agent-Benutzer mit bestimmten Berechtigungen die Einstellungen auf der OfficeScan Agent-Konsole manuell konfiguriert hat.

OfficeScan überprüft die folgenden Einstellungen:

- Suchmethode
- Einstellungen für manuelle Suche
- Einstellungen für Echtzeitsuche
- Einstellungen für die zeitgesteuerte Suche
- Einstellungen für Jetzt durchsuchen
- Berechtigungen und andere Einstellungen
- Zusätzliche Diensteinstellungen
- Web Reputation
- Verhaltensüberwachung
- Gerätesteuerung
- Liste der zugelassenen Spyware/ Grayware
- Einstellungen für 'Prävention vor Datenverlust'
- Verdächtige Verbindung
- Liste der vertrauenswürdigen Programme
- Exemplar Zusendung
- Vorausschauendes Maschinenlernen

Ein nicht richtlinienkonformer Agent wird im Bericht zur Einhaltung von Richtlinien mindestens zwei Mal gezählt.

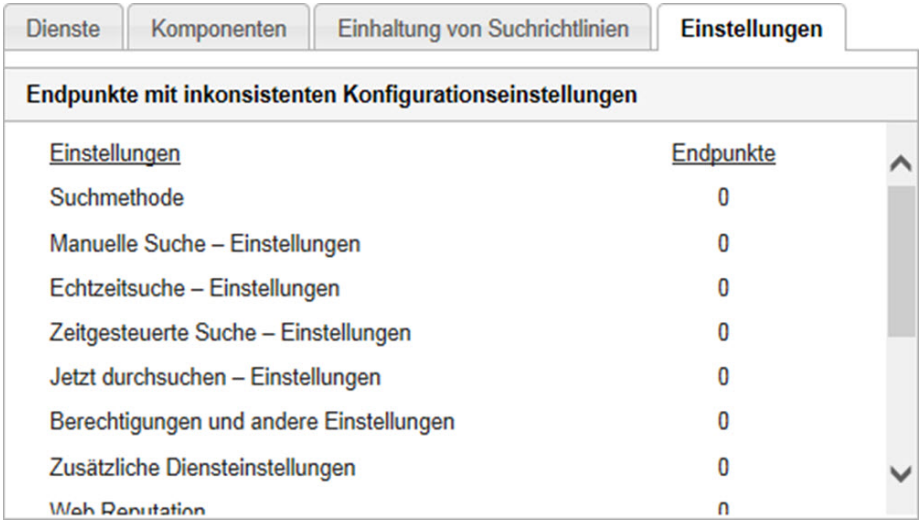


ABBILDUNG 15-6. Registerkarte Bericht zur Einhaltung der Richtlinien - Einstellungen

- In der Kategorie **Endpunkte mit inkonsistenten Konfigurationseinstellungen**
- In der Kategorie, in welcher der Agent nicht richtlinienkonform ist. Wenn zum Beispiel die Einstellungen der Suchmethode in der Agent-Domäne und seiner übergeordneten Domäne nicht übereinstimmen, wird der Agent in der Kategorie **Suchmethode** gezählt. Wenn mehr als ein Einstellungssatz nicht übereinstimmt, wird der Agent in jeder Kategorie gezählt, in welcher er nicht richtlinienkonform ist.

Um inkonsistente Einstellungen zu vermeiden, wenden Sie die Domäneneinstellungen auf den Agent an.

Bedarfsgesteuerte Berichte zur Einhaltung von Richtlinien

Einhaltung der Sicherheitsrichtlininen kann bei Bedarf Berichte zur Einhaltung von Richtlinien erstellen. Berichte helfen Ihnen dabei, den Sicherheitsstatus der vom OfficeScan Server verwalteten OfficeScan Agents einzuschätzen.

Weitere Informationen zu Berichten zur Einhaltung von Richtlinien finden Sie unter *Einhaltung der Sicherheitsrichtlinien für verwaltete Agents auf Seite 15-63*.

Einen bedarfsgesteuerten Bericht zur Einhaltung von Richtlininen erstellen

Prozedur

1. Navigieren Sie zu **Bewertung** > **Einhaltung von Sicherheitsrichtlinien** > **Manueller Bericht**.
2. Wechseln Sie zum Abschnitt **Agent-Hierarchiebereich**.
3. Wählen Sie die Root-Domäne oder eine andere Domäne, und klicken Sie auf **Bewerten**.
4. Zeigen Sie Berichte zur Einhaltung von Richtlinien für Agent-Dienste an.

   Weitere Informationen zu Agent-Diensten finden Sie unter *Dienste auf Seite 15-64*.

   a. Klicken Sie auf die Registerkarte **Services**.

   b. Überprüfen Sie unter **Endpunkte mit nicht kompatiblen Diensten** die Anzahl der Agents mit nicht kompatiblen Diensten.

   c. Klicken Sie auf eine verlinkte Zahl, um alle in der Agent-Hierarchie betroffenen Agents anzuzeigen.

   d. Wählen Sie die Agents im Abfrageergebnis aus.

   e. Klicken Sie auf **OfficeScan Agent neu starten**, um den Dienst neu zu starten.

Hinweis

Wenn nach der Durchführung einer weiteren Bewertung der Agent immer noch als nicht richtlinienkonform angezeigt wird, starten Sie den Dienst auf dem Agent-Endpunkt manuell neu.

f. Klicken Sie auf **Exportieren**, um die Liste der Agents in einer Datei zu speichern.

5. Zeigen Sie den Bericht zur Einhaltung von Richtlinien für Agent-Komponenten an.

   Weitere Informationen zu Agent-Komponenten finden Sie unter *Komponenten auf Seite 15-66*.

   a. Klicken Sie auf die Registerkarte **Komponenten**.

   b. Überprüfen Sie unter **Endpunkte mit inkonsistenten Komponentenversionen** die Anzahl der Agents mit Komponentenversionen, die mit den Versionen auf dem Server nicht übereinstimmen.

   c. Klicken Sie auf eine verlinkte Zahl, um alle in der Agent-Hierarchie betroffenen Agents anzuzeigen.

   Hinweis

   Wenn mindestens ein Agent über eine aktuellere Komponente als der OfficeScan Server verfügt, aktualisieren Sie den OfficeScan Server manuell.

   d. Wählen Sie die Agents im Abfrageergebnis aus.

   e. Klicken Sie auf **Jetzt aktualisieren**, um durchzusetzen, dass die Agents die Komponenten herunterladen.

Hinweis

- So stellen Sie sicher, dass Agents ein Upgrade des Agent-Programms durchführen können:
  i. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
  ii. Klicken Sie auf die Registerkarte **Einstellungen** > **Berechtigungen und andere Einstellungen** > **Andere Einstellungen**.
  iii. Gehen Sie zum Abschnitt **Update-Einstellungen**.
  iv. Wählen Sie im Listenfeld **OfficeScan Agents aktualisieren nur die folgenden Komponenten** die Option **Alle Komponenten (einschließlich Hotfixes und Agent-Programm)** aus.
  v. Klicken Sie auf **Auf alle Agents anwenden**.
- Starten Sie den Endpunkt neu und klicken Sie nicht auf **Jetzt aktualisieren**, um den allgemeinen Firewall-Treiber zu aktualisieren.

f. Klicken Sie auf **Exportieren**, um die Liste der Agents in einer Datei zu speichern.

6. Berichte zur Richtlinieneinhaltung für Suchvorgänge anzeigen.

Weitere Informationen zu Suchvorgängen finden Sie unter *Einhaltung von Suchrichtlinien auf Seite 15-68*.

a. Klicken Sie auf die Registerkarte **Einhaltung von Suchrichtlinien**.

b. Konfigurieren Sie unter **Endpunkte mit veralteten Virensuchfunktionen** Folgendes:

- Die Anzahl der Tage, die ein Agent die Sofortsuche ("Jetzt durchsuchen") oder die zeitgesteuerte Suche nicht durchgeführt hat
- Die Anzahl der Stunden, in denen eine Sofortsuche oder eine zeitgesteuerte Suche durchgeführt wurde

Hinweis

Wenn die Anzahl der Tage bzw. Stunden überschritten ist, wird der Agent als nicht konform betrachtet.

c. Klicken Sie auf **Bewerten** neben dem Abschnitt **Agent-Hierarchiebereich**.

d. Überprüfen Sie unter **Endpunkte mit veralteten Virensuchfunktionen** die Anzahl der Agents, die die Suchkriterien erfüllen.

e. Klicken Sie auf eine verlinkte Zahl, um alle in der Agent-Hierarchie betroffenen Agents anzuzeigen.

f. Wählen Sie die Agents im Abfrageergebnis aus.

g. Klicken Sie auf **Jetzt durchsuchen**, um die Agents sofort zu durchsuchen.

Hinweis

Um zu verhindern, dass die Suche wiederholt wird, wird die Option **Sofort durchsuchen** deaktiviert, wenn sie länger als die angegebene Anzahl von Stunden dauert.

h. Klicken Sie auf **Exportieren**, um die Liste der Agents in einer Datei zu speichern.

7. Berichte zur Richtlinieneinhaltung für Einstellungen anzeigen.

Weitere Informationen zu Einstellungen finden Sie unter *Einstellungen auf Seite 15-71*.

a. Klicken Sie auf die Registerkarte **Einstellungen**.

b. Überprüfen Sie unter **Computer mit inkonsistenten Konfigurationseinstellungen** die Anzahl der Agents mit Einstellungen, die nicht mit den Domäneneinstellungen der Agent-Hierarchie übereinstimmen.

c. Klicken Sie auf eine verlinkte Zahl, um alle in der Agent-Hierarchie betroffenen Agents anzuzeigen.

d. Wählen Sie die Agents im Abfrageergebnis aus.

e. Klicken Sie auf **Domäneneinstellungen übernehmen**.

f. Klicken Sie auf **Exportieren**, um die Liste der Agents in einer Datei zu speichern.

Zeitgesteuerte Berichte zur Einhaltung von Richtlinien

Einhaltung der Sicherheitsrichtlinien kann zeitgesteuerte Berichte zur Einhaltung von Richtlinien erstellen. Berichte helfen Ihnen dabei, den Sicherheitsstatus der vom OfficeScan Server verwalteten OfficeScan Agents einzuschätzen.

Weitere Informationen zu Berichten zur Einhaltung von Richtlinien finden Sie unter *Einhaltung der Sicherheitsrichtlinien für verwaltete Agents auf Seite 15-63*.

Einstellungen für zeitgesteuerte Berichte zur Einhaltung von Richtlinien konfigurieren

Prozedur

1. Navigieren Sie zu **Bewertung** > **Einhaltung von Sicherheitsrichtlinien** > **Zeitgesteuerter Bericht**.
2. Wählen Sie die Option **Zeitgesteuerte Berichterstellung aktivieren**.
3. Geben Sie einen Titel für den Bericht an.
4. Wählen Sie eine oder alle der folgenden Einstellungen:
   - *Dienste auf Seite 15-64*
   - *Komponenten auf Seite 15-66*
   - *Einhaltung von Suchrichtlinien auf Seite 15-68*
   - *Einstellungen auf Seite 15-71*
5. Geben Sie die E-Mail-Adresse(n) an, die Benachrichtigungen über zeitgesteuerte Berichte zur Einhaltung von Richtlinien erhalten sollen.

Hinweis

Konfigurieren Sie E-Mail-Benachrichtigungseinstellungen, um sicherzustellen, dass die E-Mail-Benachrichtigungen erfolgreich versendet werden können. Weitere Informationen finden Sie unter *Einstellungen für die Administratorbenachrichtigungen auf Seite 14-43*.

6. Geben Sie den Zeitplan an.

7. Klicken Sie auf **Speichern**.

Einhaltung der Sicherheitsrichtlinien für nicht verwaltete Endpunkte

Die Einhaltung der Sicherheitsrichtlinien kann nicht verwaltete Endpunkte im Netzwerk, in dem sich der OfficeScan Server befindet, abfragen. Verwenden Sie Active Directory und IP-Adressen zur Abfrage von Endpunkten.

Folgende Sicherheitszustände nicht verwalteter Endpunkte sind möglich:

TABELLE 15-7. Sicherheitsstatus nicht verwalteter Endpunkte

STATUS	BESCHREIBUNG
Von einem anderen OfficeScan Server verwaltet	Die OfficeScan Agents, die auf den Computern installiert wurden, werden von einem anderen OfficeScan Server verwaltet. OfficeScan Agents sind online, und auf ihnen wird entweder diese oder eine frühere Version von OfficeScan ausgeführt.
Kein OfficeScan Agent installiert	Der OfficeScan Agent ist nicht auf diesem Endpunkt installiert.
Nicht erreichbar	Der OfficeScan Server kann keine Verbindung zum Endpunkt aufbauen und dessen Sicherheitsstatus ermitteln.

STATUS	BESCHREIBUNG
Ungelöste Active Directory-Auswertung	Der Endpunkt befindet sich in einer Active Directory-Domäne, aber der OfficeScan Server kann dessen Sicherheitsstatus nicht ermitteln. **Hinweis** Die OfficeScan Server-Datenbank enthält eine Liste der agents, die der Server verwaltet. Der Server fragt Active Directory nach der GUID der Computer ab und vergleicht die erhaltenen Werte mit den GUIDs, die in der Datenbank gespeichert sind. Wenn eine GUID nicht in der Datenbank enthalten ist, fällt der Endpunkt in die Kategorie "Ungelöste Active Directory-Bewertung".

Um eine Sicherheitsbewertung zu starten, führen Sie folgende Aufgaben durch:

1. Legen Sie den Abfragebereich fest. Weitere Informationen finden Sie unter *Active Directory/IP-Adressbereich und Abfrage definieren auf Seite 15-79*.
2. Überprüfen Sie ungeschützte Computer anhand der Suchabfrageergebnisse. Weitere Informationen finden Sie unter *Abfrageergebnisse anzeigen auf Seite 15-82*.
3. Installieren Sie den OfficeScan Agent. Weitere Informationen finden Sie unter *Installation bei Einhaltung von Sicherheitsrichtlinien auf Seite 5-64*.
4. Konfigurieren Sie zeitgesteuerte Abfragen. Weitere Informationen finden Sie unter *Bewertung zeitgesteuerter Abfragen konfigurieren auf Seite 15-83*.

Active Directory/IP-Adressbereich und Abfrage definieren

Definieren Sie bei der ersten Abfrage den Active-Directory-/IP-Adressbereich, der die Active-Directory-Objekte und die IP-Adressen enthält, die der OfficeScan Server bei Bedarf periodisch abfragt. Starten Sie nach der Definition des Bereichs den Abfrageprozess.

Hinweis

Um einen Active-Directory-Bereich festzulegen, muss OfficeScan zuerst in Active Directory integriert werden. Weitere Informationen zur Integration finden Sie unter *Active Directory-Integration auf Seite 2-36*.

Prozedur

1. Navigieren Sie zu **Bewertung** > **Nicht verwaltete Endpunkte**.
2. Klicken Sie im Abschnitt **Active Directory/IP-Adressenbereich** auf **Bereich definieren**.

   Es öffnet sich ein neues Fenster.
3. Einen Active-Directory-Bereich festlegen:
   a. Wechseln Sie zum Abschnitt **Active-Directory-Bereich**.
   b. Wählen Sie **Bedarfsgesteuerte Bewertung verwenden**, um Echtzeitabfragen durchzuführen und genauere Ergebnisse zu erhalten. Wenn Sie diese Option deaktivieren, fragt OfficeScan die Datenbank ab und nicht jeden OfficeScan Agent. Nur die Datenbank abzufragen, ist zwar möglicherweise schneller, aber weniger genau.
   c. Wählen Sie die Objekte, die abgefragt werden sollen. Wenn Sie die Abfrage zum ersten Mal ausführen, wählen Sie ein Objekt mit weniger als 1.000 Konten, und notieren Sie dann, wie lange die Abfrage gedauert hat. Verwenden Sie diesen Wert als Leistungsbenchmark.
4. Einen IP-Adressbereich festlegen:
   a. Gehen Sie zum Abschnitt **IP-Adressbereich**.
   b. Wählen Sie **IP-Adressbereich aktivieren**.
   c. Geben Sie einen IP-Adressbereich an. Klicken Sie auf die Plus- oder Minus-Schaltfläche, um IP-Adressbereiche hinzuzufügen oder zu löschen.
   - Für einen reinen IPv4-OfficeScan Server geben Sie einen IPv4-Adressbereich an.

- Für einen reinen IPv6-OfficeScan Server geben Sie ein IPv6-Präfix und eine IPv6-Länge an.
- Für einen Dual-Stack-OfficeScan Server geben Sie einen IPv4-Adressbereich und/oder ein IPv6-Präfix und eine IPv6-Länge an.

  Der IPv6-Adressbereich ist auf 16 Bit begrenzt und damit ähnlich begrenzt wie IPv4-Adressbereiche. Die Präfixlänge sollte deshalb zwischen 112 und 128 Zeichen liegen.

TABELLE 15-8. Präfixlängen und Anzahl von IPv6-Adressen

LÄNGE	ANZAHL VON IPV6-ADRESSEN
128	2
124	16
120	256
116	4,096
112	65,536

5. Geben Sie unter "Erweiterte Einstellungen" die von den OfficeScan Servern für die Kommunikation mit den Agents verwendeten Ports an. Setup erzeugt die Portnummern während der Installation des OfficeScan Servers nach dem Zufallsprinzip.

   Um den vom OfficeScan Server verwendeten Kommunikationsport anzuzeigen, navigieren Sie zu **Agents** > **Agent-Verwaltung** und wählen Sie eine Domäne aus. Die Portnummer steht neben der Spalte für die IP-Adresse. Trend Micro empfiehlt, eine Liste der Portnummern aufzubewahren.

   a. Klicken Sie auf **Ports angeben**.

   b. Geben Sie die Portnummer ein, und klicken Sie auf **Hinzufügen**. Wiederholen Sie diesen Schritt, bis Sie alle Portnummern haben, die hinzugefügt werden sollen.

   c. Klicken Sie auf **Speichern**.

6. Um die Konnektivität des Endpunkts mit Hilfe einer bestimmten Portnummer zu überprüfen, wählen Sie **Endpunkt durch Überprüfen des Ports <x> als nicht**

erreichbar deklarieren aus. Wenn die Verbindung nicht aufgebaut wird, stuft OfficeScan den Endpunkt sofort als nicht erreichbar ein. Die Standardportnummer lautet 135.

Wenn Sie diese Einstellung aktivieren, wird die Abfrage beschleunigt. Wenn eine Verbindung zu Endpunkten nicht aufgebaut werden kann, muss der OfficeScan Server nicht mehr alle anderen Aufgaben zur Verbindungsüberprüfung durchführen, bevor Endpunkte als nicht erreichbar eingestuft werden.

7. Um den Bereich zu speichern und die Abfrage zu starten, klicken Sie auf **Speichern und erneut bewerten**. Um die Einstellungen nur zu speichern, klicken Sie auf **Nur speichern**.

   Im Fenster **Ausgelagerte Serververwaltung** wird das Ergebnis der Abfrage angezeigt.

Hinweis

Die Abfrage nimmt u. U. viel Zeit in Anspruch, besonders bei einem großen Abfrageumfang. Führen Sie keine andere Abfrage durch, bis im Fenster "Ausgelagerte Serververwaltung" das Ergebnis angezeigt wird. Andernfalls wird die aktuelle Abfragesitzung beendet, und der Abfrageprozess startet erneut.

Abfrageergebnisse anzeigen

Das Ergebnis der Abfrage wird im Abschnitt **Sicherheitsstatus** angezeigt. Ein nicht verwalteter Endpunkt kann einen der folgenden Zustände annehmen:

- Von einem anderen OfficeScan Server verwaltet
- Kein OfficeScan Agent installiert
- Nicht erreichbar
- Ungelöste Active Directory-Auswertung

Prozedur

1. Klicken Sie im Abschnitt **Sicherheitsstatus** auf einen Link mit einer Anzahl, um alle betroffenen Computer anzuzeigen.

2. Durchsuchen Sie mit der Suchfunktion und der erweiterten Suchfunktion nur die Computer, die die Suchkriterien erfüllen, und zeigen Sie diese an.

   Wenn Sie die erweiterte Suchfunktion verwenden, geben Sie die folgenden Informationen an:

   - IPv4-Adressbereich
   - IPv6-Präfix und -Länge (Präfix sollte zwischen 112 und 128 Zeichen lang sein)
   - Endpunkt name
   - OfficeScan Server-Name
   - Active Directory-Struktur
   - Sicherheitsstatus

   OfficeScan gibt kein Ergebnis zurück, wenn der Name unvollständig ist. Verwenden Sie das Platzhalterzeichen (*), wenn Sie den vollständigen Namen nicht genau kennen.

3. Klicken Sie auf **Exportieren**, um die Liste der Computer in einer Datei zu speichern.

4. Bei OfficeScan Agents, die von einem anderen OfficeScan Server verwaltet werden, verwenden Sie das Agent Mover-Tool, damit diese OfficeScan Agents vom aktuellen OfficeScan Server verwaltet werden. Weitere Informationen zu diesem Tool finden Sie unter *Agent Mover auf Seite 15-24*.

Bewertung zeitgesteuerter Abfragen konfigurieren

Konfigurieren Sie den OfficeScan Server für periodische Abfragen von Active Directory und IP-Adressen, um sicherzustellen, dass die Sicherheitsrichtlinien implementiert wurden.

Prozedur

1. Navigieren Sie zu **Bewertung** > **Nicht verwaltete Endpunkte**.

2. Klicken Sie oben in der Agent-Hierarchie auf **Zeitplan definieren**.
3. Aktivieren Sie die zeitgesteuerte Abfrage.
4. Geben Sie den Zeitplan an.
5. Klicken Sie auf **Speichern**.

Unterstützung für Trend Micro Virtual Desktop

Sie können den Schutz virtueller Desktop durch Verwenden von Trend Micro Virtual Desktop Support optimieren. Diese Funktion steuert Aufgaben auf OfficeScan Agents, die sich auf einem einzelnen virtuellen Server befinden.

Wenn mehrere Desktops auf einem einzelnen Server ausgeführt und On-Demand-Suche oder Komponenten-Updates durchgeführt werden, wird ein signifikanter Teil der Systemressourcen verbraucht. Verwenden Sie diese Funktion, um Agents daran zu hindern, Suchläufe und Komponenten-Updates gleichzeitig auszuführen.

Wenn z. B. auf einem VMware vCenter Server drei virtuelle Desktops mit OfficeScan Agents ausgeführt werden, kann OfficeScan gleichzeitig auf allen drei Agents die Funktion "Jetzt durchsuchen" aufrufen und Updates installieren. Virtual Desktop Support erkennt, dass sich alle Agents auf demselben physischen Server befinden. Mit Virtual Desktop Support ist es möglich, dass eine Aufgabe auf dem ersten Agent ausgeführt wird und dieselbe Aufgabe auf den beiden anderen Agents aufgeschoben wird, bis auf dem ersten Agent die Aufgabe beendet wurde.

Virtual Desktop Support kann auf den folgenden Plattformen verwendet werden:

- VMware vCenter™ (VMware View™)
- Citrix™ XenServer™ (Citrix XenDesktop™)
- Microsoft Hyper-V™ Server

Für Administratoren, die andere Virtualisierungsanwendungen verwenden, kann der OfficeScan Server auch als emulierter Hypervisor zur Verwaltung von virtuellen Agents dienen.

Weitere Informationen über diese Plattformen finden Sie auf den Websites zu VMware View, Citrix XenDesktop bzw. Microsoft Hyper-V.

Verwenden Sie das VDI Tool zur Generierung von Prescan-Vorlagen von OfficeScan, um die On-Demand-Suche zu optimieren oder GUIDs von Basis- oder Golden Images zu entfernen.

Installation von Virtual Desktop Support

Virtual Desktop Support ist eine native Funktion in OfficeScan, die aber separat lizenziert wird. Nach der Installation des OfficeScan Servers ist diese Funktion zwar vorhanden, aber sie ist noch nicht funktionsfähig. Zur Installation dieser Funktion muss eine Datei vom ActiveUpdate Server (oder, falls vorhanden, von einer benutzerdefinierten Update-Adresse) heruntergeladen werden. Sobald diese Datei in den OfficeScan Server integriert ist, können Sie Virtual Desktop Support aktivieren, um alle Funktionen zu nutzen. Installation und Aktivierung erfolgen über den Plug-in Manager.

Hinweis

Virtual Desktop Support wird in reinen IPv6-Umgebungen nicht vollständig unterstützt. Weitere Informationen finden Sie unter *Einschränkungen bei reinen IPv6-Servern auf Seite A-3*.

Unterstützung von Virtual Desktop installieren

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
2. Navigieren Sie im Fenster **Plug-in Manager** zum Abschnitt **Unterstützung für Trend Micro Virtual Desktop**, und klicken Sie auf **Download**.

   Die Größe des Pakets wird neben der Schaltfläche **Download** angezeigt.

   Der Plug-in Manager speichert das heruntergeladene Paket unter <*Installationsordner des Servers*>`\PCCSRV\Download\Product`.

Hinweis

Wenn der Plug-in Manager die Datei nicht herunterladen kann, wiederholt er den Versuch automatisch nach 24 Stunden. Um den Download manuell zu starten, muss der OfficeScan Plug-in Manager Dienst über die Microsoft Management Console neu gestartet werden.

3. Verfolgen Sie den Download-Fortschritt. Sie können während des Downloads zu anderen Fenstern navigieren.

   Treten beim Download des Pakets Probleme auf, überprüfen Sie die Server-Update-Protokolle auf der OfficeScan Produktkonsole. Klicken Sie im Hauptmenü auf **Protokolle** > **Server-Update**.

   Nachdem der Plug-in Manager die Datei heruntergeladen hat, wird Virtual Desktop Support in einem neuen Fenster angezeigt.

Hinweis

Wenn Virtual Desktop Support nicht angezeigt wird, finden Sie unter *Fehlersuche in Plug-in Manager auf Seite 17-13* mögliche Ursachen und Lösungen.

4. Um Virtual Desktop Support sofort zu installieren, klicken Sie auf **Jetzt installieren**. Die Installation zu einem späteren Zeitpunkt durchführen:

   a. Klicken Sie auf **Später installieren**.

   b. Öffnen Sie das Fenster **Plug-in Manager**.

   c. Gehen Sie zum Abschnitt **Trend Micro Virtual Desktop Support**, und klicken Sie auf **Installieren**.

5. Lesen Sie die Lizenzvereinbarung und akzeptieren Sie die Bedingungen, indem Sie auf **Stimme zu** klicken.

   Die Installation wird gestartet.

6. Überwachen Sie den Installationsfortschritt. Nach der Installation wird die entsprechende Version von Virtual Desktop Support angezeigt.

Virtual Desktop Support Lizenz

Verwenden Sie Plug-in Manager, um die Lizenz für Virtual Desktop Support anzuzeigen, zu aktivieren und zu verlängern.

Fordern Sie von Trend Micro den Aktivierungscode an, um damit den vollständigen Funktionsumfang von Virtual Desktop Support zu aktivieren.

Unterstützung von Virtual Desktop aktivieren oder erneuern

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
2. Navigieren Sie im Fenster **Plug-in Manager** zum Abschnitt **Unterstützung für Trend Micro Virtual Desktop**, und klicken Sie auf **Programm verwalten**.
3. Klicken Sie auf **Lizenzdaten anzeigen**.
4. Klicken Sie im geöffneten Fenster **Einzelheiten zur Produktlizenz** auf **Neuer Aktivierungscode**.
5. Geben Sie den Aktivierungscode in das daraufhin angezeigte Fenster ein, und klicken Sie auf **Speichern**.
6. Klicken Sie im Fenster "Informationen über Produktlizenz" auf **Informationen aktualisieren**, um das Fenster mit den neuen Informationen über die Produktlizenz und den Status der Funktion zu aktualisieren. In diesem Fenster wird auch ein Link zur Trend Micro Website angezeigt, auf der Sie detaillierte Informationen über die Lizenz finden.

Lizenzdaten für Unterstützung von Virtual Desktop anzeigen

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins** > **Programm [Trend Micro Virtual Desktop Support] verwalten**.

2. Klicken Sie auf **Lizenzdaten anzeigen**.

3. Ein Fenster mit Informationen zur Lizenz wird geöffnet.

   Der Abschnitt Einzelheiten zur Lizenz für Virtual Desktop Support enthält folgende Informationen:

   - **Status**: Wird entweder als "Aktiviert", "Nicht aktiviert" oder "Abgelaufen" angezeigt.
   - **Version**: Wird entweder als "Vollversion" oder "Testversion" angezeigt. Wenn Sie die Voll- und die Testversion besitzen, wird "Vollversion" angezeigt.
   - **Ablaufdatum**: Wenn es für Virtual Desktop Support mehrere Lizenzen gibt, wird das am weitesten in der Zukunft liegende Ablaufdatum angezeigt. Laufen die Lizenzen am 31.12.10 und am 30.06.10 ab, wird das Datum 31.12.10 angezeigt.
   - **Arbeitsplätze**: Zeigt an, wie viele OfficeScan Agents Virtual Desktop Support verwenden können
   - **Aktivierungscode**: Zeigt den Aktivierungscode an

   In folgenden Fällen werden Hinweise zu Lizenzen angezeigt:

   Wenn Sie eine Lizenz der Vollversion haben:

   - Während der Übergangsfrist der Funktion. Die Dauer der Übergangsfrist ist regional verschieden. Erkunden Sie sich bei Ihrem Trend Micro Vertriebspartner über die Länge der Übergangsfrist.
   - Bei Ablauf der Lizenz und der Übergangsfrist. Während dieser Zeit erhalten Sie keine technische Unterstützung.

   Wenn Sie eine Testversionslizenz haben

   - Bei Ablauf der Lizenz Während dieser Zeit erhalten Sie keine technische Unterstützung.

4. Klicken Sie auf **Einzelheiten zur Lizenz online anzeigen**, um Informationen über Ihre Lizenz auf der Trend Micro Website anzuzeigen.

5. Um die aktuellsten Lizenzdaten anzuzeigen, klicken Sie auf **Informationen aktualisieren**.

Virtual Server-Verbindungen

Sie können die On-Demand-Suche oder Komponenten-Updates optimieren, indem Sie VMware vCenter 4 (VMware View 4), Citrix XenServer 5.5 (Citrix XenDesktop 4) oder Microsoft Hyper-V Server hinzufügen. OfficeScan Server kommuniziert mit den angegebenen virtuellen Servern, um OfficeScan Agents zu finden, die sich auf demselben physischen Server befinden.

Für andere VDI-Server bietet der OfficeScan Server einen emulierten virtuellen Hypervisor, um die virtuellen agents auf anderen Plattformen zu verwalten. Der OfficeScan Hypervisor verarbeitet Anfragen von virtuellen agent in der Reihenfolge, in der der Server die Anfragen empfängt. Der OfficeScan Server verarbeitet jeweils immer eine Anfrage und platziert die anderen Anfragen in einer Warteschlange.

Serververbindungen hinzufügen

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins** > **Programm [Trend Micro Virtual Desktop Support] verwalten**.
2. Wählen Sie **VMware vCenter Server**, **Citrix XenServer**, **Microsoft Hyper-V** oder **Andere Virtualisierungsanwendungen**.

   Hinweis

   Wenn Sie **Andere Virtualisierungsanwendungen** auswählen, sind keine weiteren Angaben erforderlich. Der OfficeScan Server verarbeitet Anfragen von virtuellen agent in der Reihenfolge, in der der Server die Anfragen empfängt.

3. Aktivieren Sie die Verbindung zum Server.
4. Geben Sie die folgenden Informationen an:

- Für VMware vCenter- und Citrix XenServer-Server:
  - IP-Adresse
  - Port
  - Verbindungsprotokoll (HTTP oder HTTPS)
  - Benutzername
  - Kennwort
- Für Microsoft Hyper-V-Server:
  - Hostname oder IP-Adresse:
  - Domäne\Benutzername

  Hinweis

  Das Anmeldekonto muss ein Domänenkonto in der Administratorgruppe sein.

  - Kennwort

5. Aktivieren Sie optional die Proxy-Verbindung für VMware vCenter oder Citrix XenServer.
   a. Geben Sie den Namen oder die IP-Adresse und den Port des Proxy-Servers ein.
   b. Falls der Proxy-Server eine Authentifizierung verlangt, geben Sie den Benutzernamen und das Kennwort ein.
6. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob der OfficeScan Server eine Verbindung zum Server aufbauen kann.

Hinweis

Weitere Informationen zur Fehlerbehebung bei Microsoft Hyper-V-Verbindungen finden Sie unter *Fehlerbehebung bei Microsoft Hyper-V-Verbindungen auf Seite 15-93*.

7. Klicken Sie auf **Speichern**.

Zusätzliche Serververbindungen hinzufügen

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins** > **Programm [Trend Micro Virtual Desktop Support] verwalten**.
2. Klicken Sie auf **Neue vCenter-Verbindung hinzufügen**, **Neue XenServer-Verbindung hinzufügen** oder auf **Neue Hyper-V-Verbindung hinzufügen**.
3. Wiederholen Sie die Schritte, um die korrekten Serverinformationen bereitzustellen.
4. Klicken Sie auf **Speichern**.

Verbindungseinstellung löschen

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und navigieren Sie im Hauptmenü zu **Plug-ins** > **Programm [Trend Micro Virtual Desktop Support] verwalten**.
2. Klicken Sie auf **Diese Verbindung löschen**.
3. Klicken Sie auf **Ok**, um das Löschen dieser Einstellung zu bestätigen.
4. Klicken Sie auf **Speichern**.

VDI-Scan-Kapazität ändern

Administratoren können die Anzahl der VDI-Endpunkte beschleunigen, die gleichzeitig ausgeführt werden, indem die `vdi.ini`-Datei geändert wird. Trend Micro empfiehlt, die Änderung der VDI-Kapazität streng zu überwachen, sodass die Systemressourcen auf jegliche verstärkte Suche reagieren können.

Prozedur

1. Navigieren Sie auf dem OfficeScan Server-Computer zu <*Installationsordner des Servers*>`PCCSRV\Private\vdi.ini`.

2. Wechseln Sie in die `[TaskController]`-Einstellungen.

   Beim Folgenden handelt es sich um die Standardeinstellungen von TaskController:

   - Für OfficeScan 10.5 Clients:

     ```
     [TaskController]

     Controller_00_MaxConcurrentGuests=1

     Controller_01_MaxConcurrentGuests=3
     ```

     Wobei gilt:

     - `Controller_00_MaxConcurrentGuests=1` entspricht der maximalen Anzahl von Clients, die gleichzeitig Suchvorgänge durchführen können.
     - `Controller_01_MaxConcurrentGuests=3` entspricht der maximalen Anzahl von Clients, die gleichzeitig Suchvorgänge durchführen können.

   - Für OfficeScan 10.6 Clients und OfficeScan 11.0 (oder höher) agents:

     ```
     [TaskController]

     Controller_02_MaxConcurrentGuests=1

     Controller_03_MaxConcurrentGuests=3
     ```

     Wobei gilt:

     - `Controller_02_MaxConcurrentGuests=1` entspricht der maximalen Anzahl von Clients, die gleichzeitig Suchvorgänge durchführen können.
     - `Controller_03_MaxConcurrentGuests=3` entspricht der maximalen Anzahl von Clients, die gleichzeitig Suchvorgänge durchführen können.

3. Erhöhen oder verringern Sie den Zähler in jedem Controller soweit erforderlich.

   Der Mindestwert für alle Einstellungen ist 1.

   Der Höchstwert für alle Einstellungen ist 65536.

4. Speichern und schließen Sie die `vdi.ini`-Datei.

5. Starten Sie den OfficeScan Master Service neu.

6. Überwachen Sie die CPU-Auslastung, den Speicherbedarf und die Festplattennutzung der VDI-Endpunkte. Ändern Sie die Controller-Einstellungen, um die Anzahl der gleichzeitigen Suchvorgänge zu erhöhen/verringern und die VDI-Umgebung durch das Wiederholen der Schritte 1 bis 5 am besten anzupassen.

Fehlerbehebung bei Microsoft Hyper-V-Verbindungen

Die Microsoft Hyper-V-Verbindung verwendet die Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI) und DCOM für die agent-Server-Kommunikation. Die Firewall-Richtlinien blockieren möglicherweise diese Kommunikation, wodurch keine Verbindung zum Hyper-V-Server hergestellt werden kann.

Für den Listening-Port des Hyper-V-Servers wird standardmäßig auf Port 135 zurückgegriffen, und anschließend wird ein zufällig konfigurierter Port zur weiteren Kommunikation verwendet. Wenn die Firewall den WMI-Datenverkehr oder einen der beiden Ports blockiert, kann keine Kommunikation mit dem Server stattfinden. Administratoren können die Firewall-Richtlinie ändern, um eine Kommunikation mit dem Hyper-V-Server zu ermöglichen.

Vergewissern Sie sich, dass alle Verbindungseinstellungen, einschließlich IP-Adresse, Domäne\Benutzername und Kennwort, korrekt sind, bevor Sie die folgenden Änderungen an der Firewall vornehmen.

WMI-Kommunikation über die Windows-Firewall zulassen

Prozedur

1. Öffnen Sie auf dem Hyper-V-Server das Fenster **Windows-Firewall - Zugelassene Programme**.

   Navigieren Sie auf Windows 2008 R2-Systemen zu **Systemsteuerung** > **System und Sicherheit** > **Windows-Firewall** > **Ein Programm oder Feature durch die Windows-Firewall zulassen**.

2. Wählen Sie **Windows-Verwaltungsinstrumentation**.

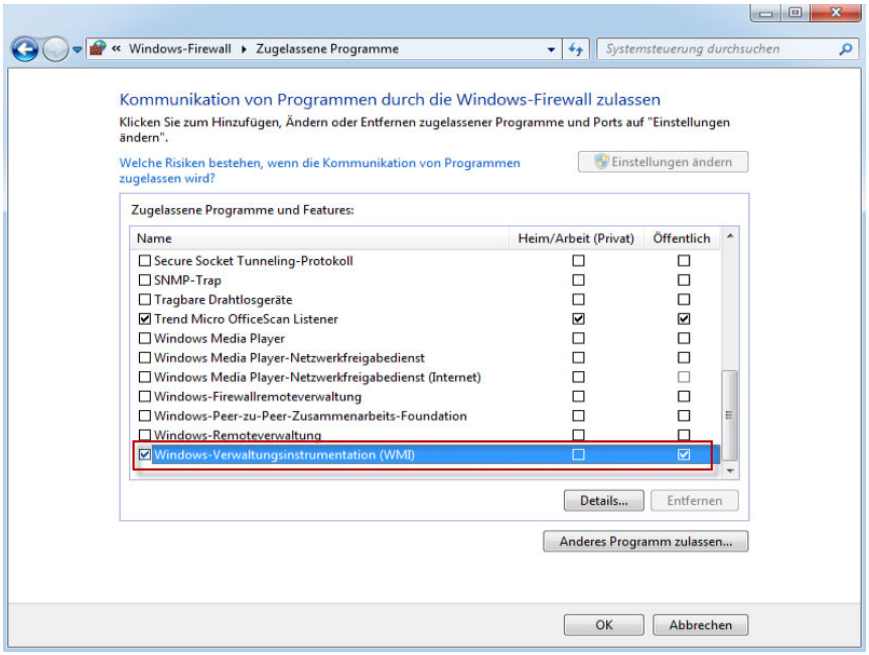


ABBILDUNG 15-7. Fenster "Windows-Firewall - Zugelassene Programme"

3. Klicken Sie auf **Speichern**.

4. Testen Sie die Hyper-V-Verbindung erneut.

Port-Kommunikation über die Windows-Firewall oder eine Firewall eines anderen Anbieters öffnen

Prozedur

1. Stellen Sie auf dem Hyper-V-Server sicher, dass die Firewall die Kommunikation über Port 135 zulässt, und testen Sie die Hyper-V-Verbindung erneut.

   Detaillierte Hinweise zum Öffnen von Ports finden Sie in der Firewall-Dokumentation.

2. Falls die Verbindung zum Hyper-V-Server nicht hergestellt werden kann, konfigurieren Sie WMI so, dass ein fester Port verwendet wird.

   Details zum *Einrichten eines festen Ports für WMI* finden Sie unter:

   http://msdn.microsoft.com/en-us/library/windows/desktop/bb219447(v=vs.85).aspx

3. Öffnen Sie den Port 135 und den neu erstellten Port (24158) für die Kommunikation über die Firewall.

4. Testen Sie die Hyper-V-Verbindung erneut.

VDI Tool zur Generierung von Prescan-Vorlagen

Verwenden Sie das VDI Tool zur Generierung von Prescan-Vorlagen von OfficeScan, um die On-Demand-Suche zu optimieren oder GUIDs aus Basis Images oder Golden Images zu entfernen. Dieses Werkzeug durchsucht das Basis-Image oder das Golden Image und zertifiziert das Image. Wenn Duplikate dieses Images durchsucht werden, überprüft OfficeScan nur die Teile, die geändert wurden. Dadurch wird eine kürzere Suchzeit gewährleistet.

Tipp

Trend Micro empfiehlt, eine Prescan-Vorlage nach der Anwendung eines Windows Updates oder der Installation einer neuen Anwendung zu erstellen.

Eine Prescan-Vorlage erstellen

Prozedur

1. Navigieren Sie auf dem OfficeScan Server-Computer zu <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\TCacheGen`.

2. Wählen Sie eine Version des VDI Tools zur Generierung von Prescan-Vorlagen. Die folgenden Versionen sind verfügbar:

   TABELLE 15-9. Versionen des VDI Tools zur Generierung von Prescan-Vorlagen

DATEINAME	ANWEISUNG
TCacheGen.exe	Wählen Sie diese Datei, wenn Sie das Tool direkt auf einer 32-Bit-Plattform ausführen möchten.
TCacheGen_x64.exe	Wählen Sie diese Datei, wenn Sie das Tool direkt auf einer 64-Bit-Plattform ausführen möchten.
TCacheGenCli.exe	Wählen Sie diese Datei, wenn Sie das Tool über die Befehlszeilenschnittstelle einer 32-Bit-Plattform ausführen möchten.
TCacheGenCli_x64.exe	Wählen Sie diese Datei, wenn Sie das Tool über die Befehlszeilenschnittstelle einer 64-Bit-Plattform ausführen möchten.

3. Kopieren Sie die Version des Tools, die Sie im vorherigen Schritt gewählt haben, auf den Endpunkt.

4. Führen Sie das Tool aus.

   - So führen Sie das Tool direkt aus:

     a. Doppelklicken Sie auf `TCacheGen.exe` oder `TCacheGen_x64.exe`.

b. Wählen Sie **Prescan-Vorlage generieren** aus, und klicken Sie dann auf **Weiter**.

- So führen Sie das Tool über die Befehlszeilenschnittstelle aus:

  a. Öffnen Sie die Eingabeaufforderung, und wechseln Sie zum `<Installationsordner des Agents>`.

  b. Geben Sie folgenden Befehl ein:

  ```
  TCacheGenCli Generate_Template
  ```

  Oder

  ```
  TcacheGenCli_x64 Generate_Template
  ```

Hinweis

Dieses Dienstprogramm durchsucht das Image nach Sicherheitsbedrohungen, bevor die Prescan-Vorlage generiert und die GUID entfernt wird.

Nachdem die Prescan-Vorlage generiert wurde, wird der OfficeScan Agent vom Dienstprogramm entladen. Laden Sie den OfficeScan Agent nicht erneut. Wird der OfficeScan Agent erneut geladen, müssen Sie die Prescan-Vorlage erneut erstellen.

GUIDs aus der Vorlage entfernen

Prozedur

1. Navigieren Sie auf dem OfficeScan Server-Computer zu <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\TCacheGen`.
2. Wählen Sie eine Version des VDI Tools zur Generierung von Prescan-Vorlagen. Die folgenden Versionen sind verfügbar:

TABELLE 15-10. Versionen des VDI Tools zur Generierung von Prescan-Vorlagen

DATEINAME	ANWEISUNG
TCacheGen.exe	Wählen Sie diese Datei, wenn Sie das Tool direkt auf einer 32-Bit-Plattform ausführen möchten.
TCacheGen_x64.exe	Wählen Sie diese Datei, wenn Sie das Tool direkt auf einer 64-Bit-Plattform ausführen möchten.
TCacheGenCli.exe	Wählen Sie diese Datei, wenn Sie das Tool über die Befehlszeilenschnittstelle einer 32-Bit-Plattform ausführen möchten.
TCacheGenCli_x64.exe	Wählen Sie diese Datei, wenn Sie das Tool über die Befehlszeilenschnittstelle einer 64-Bit-Plattform ausführen möchten.

3. Kopieren Sie die Version des Tools, die Sie im vorherigen Schritt gewählt haben, auf den Endpunkt.

4. Führen Sie das Tool aus.

   - So führen Sie das Tool direkt aus:

     a. Doppelklicken Sie auf `TCacheGen.exe` oder `TCacheGen_x64.exe`.

     b. Wählen Sie **GUID aus Vorlage entfernen** aus, und klicken Sie dann auf **Weiter**.

   - So führen Sie das Tool über die Befehlszeilenschnittstelle aus:

     a. Öffnen Sie die Eingabeaufforderung, und wechseln Sie zum `<Installationsordner des Agents>`.

     b. Geben Sie folgenden Befehl ein:

     ```
     TCacheGenCli Remove GUID
     ```

     Oder

     ```
     TcacheGenCli_x64 Remove GUID
     ```

Globale Agent-Einstellungen

OfficeScan wendet globale Agent-Einstellungen auf alle Agents oder nur auf Agents mit bestimmten Berechtigungen an.

Prozedur

1. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen**.
2. Konfigurieren Sie die folgenden Einstellungen:

TABELLE 15-11. Globale Agent-Einstellungen

REGISTERKARTEN	EINSTELLUNG	NACHSCHLAGEWERKE
Sicherheitseinstellungen	Sucheinstellungen	*Abschnitt "Sucheinstellungen" auf Seite 7-81*
	Einstellungen für die zeitgesteuerte Suche	*Abschnitt "Einstellungen für die zeitgesteuerte Suche" auf Seite 7-87*
	Firewall-Einstellungen	*Allgemeine Firewall-Einstellungen auf Seite 13-28*
	Verdächtige Verbindungseinstellungen	*Globale Einstellungen für die benutzerdefinierte IP-Liste konfigurieren auf Seite 8-7*
	Einstellungen der Verhaltensüberwachung	*Einstellungen der globalen Verhaltensüberwachung konfigurieren auf Seite 9-19*

REGISTER KARTEN	EINSTELLUNG	NACHSCHLAGEWERKE
System	Einstellungen für Certified Safe Software Service	*Allgemeine Sucheinstellungen konfigurieren auf Seite 7-79*
	Proxy für den Smart Protection Dienst	*Konfigurieren der Proxy-Einstellungen des Global Smart Protection Service auf Seite 15-58*
	Updates	• *ActiveUpdate Server als OfficeScan Agent-Update-Adresse auf Seite 6-40* • *Reservierten Festplattenspeicher für OfficeScan Agenten-Updates konfigurieren auf Seite 6-52*
	Neustart der Dienste	*Neustart des OfficeScan Agent Dienstes auf Seite 15-12*
Netzwerk	Bevorzugte IP-Adresse	*Agent IP-Adressen auf Seite 5-10*
	Kommunikation zwischen Server und Agents	*Erweiterte Verschlüsselung der Kommunikation zwischen Server und Agent auf Seite 14-67*
	Bandbreiteneinstellungen des Viren-/Malware-Protokolls	*Allgemeine Sucheinstellungen konfigurieren auf Seite 7-79*
	Nicht erreichbares Netzwerk	*Nicht erreichbar Agents auf Seite 15-49*
Agent Kontrolle	Allgemeine Einstellungen	*Allgemeine Sucheinstellungen konfigurieren auf Seite 7-79*
	Warneinstellungen	*OfficeScan Agent-Update-Benachrichtigungen konfigurieren auf Seite 6-54*
	Sprachkonfiguration für Agent	*Sprachkonfiguration für OfficeScan Agent auf Seite 15-23*

3. Klicken Sie auf **Speichern**.

Agent-Berechtigungen und weitere Einstellungen konfigurieren

Sie können Benutzer zur Änderung bestimmter Einstellungen und zur Durchführung von Aufgaben mit hoher Sicherheitsstufe auf dem OfficeScan Agent berechtigen.

Hinweis

Antivirus-Einstellungen werden nur angezeigt, wenn die Antivirus-Funktion von OfficeScan aktiviert wurde.

Tipp

Um einheitliche Einstellungen und Richtlinien innerhalb des Unternehmens durchzusetzen, gewähren Sie den Benutzern begrenzte Berechtigungen.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents einzuschließen oder nur bestimmte Domänen oder Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**.
4. Konfigurieren Sie auf der Registerkarte **Berechtigungen** folgende Benutzerberechtigungen:

TABELLE 15-12. Agent-Berechtigungen

AGENT-BERECHTIGUNGEN	NACHSCHLAGEWERKE
Berechtigung "Unabhängiger Modus"	*Berechtigung "Unabhängiger Modus" von OfficeScan Agent auf Seite 15-20*

AGENT-BERECHTIGUNGEN	NACHSCHLAGEWERKE
Suchberechtigungen	*Berechtigungen für die Sucharten auf Seite 7-63*
Berechtigungen für die zeitgesteuerte Suche	*Zeitgesteuerte Suchberechtigungen und andere Einstellungen auf Seite 7-65*
Firewall-Berechtigungen	*Firewall-Berechtigungen auf Seite 13-26*
Verhaltensüberwachungsberechtigungen	*Verhaltensüberwachungsberechtigungen auf Seite 9-21*
Liste der vertrauenswürdigen Programme	*Berechtigung für die Liste der vertrauenswürdigen Programme auf Seite 7-77*
Mail Scan Berechtigungen	*Mail-Scan-Berechtigungen und andere Einstellungen auf Seite 7-71*
Berechtigungen für die Proxy-Einstellungen	*Proxy-Konfiguration, Berechtigungen gewähren auf Seite 15-59*
Berechtigungen für Komponenten-Updates	*Update-Berechtigungen und weitere Einstellungen konfigurieren auf Seite 6-49*
Beenden und entsperren	*Die Berechtigung zum Beenden und Entsperren des Agents gewähren auf Seite 15-19*
Deinstallation	*Gewähren der Berechtigung zum Deinstallieren von OfficeScan Agent auf Seite 5-76*

5. Klicken Sie auf die Registerkarte **Weitere Einstellungen**, und konfigurieren Sie die folgenden Einstellungen:

TABELLE 15-13. Andere Agent-Einstellungen

EINSTELLUNG	NACHSCHLAGEWERKE
Update-Einstellungen	*Update-Berechtigungen und weitere Einstellungen konfigurieren auf Seite 6-49*

EINSTELLUNG	NACHSCHLAGEWERKE
Web-Reputation-Einstellungen	*Benachrichtigungen über Internet-Bedrohungen für Agent-Benutzer auf Seite 12-14*
Einstellungen der Verhaltensüberwachung	*Verhaltensüberwachungsberechtigungen auf Seite 9-21*
C&C-Kontakt – Alarmeinstellungen	*C&C-Kontaktalarmbenachrichtigungen für Agent-Benutzer auf Seite 12-19*
Warneinstellungen der zentralen Quarantänewiederherstellung	Zeigt nach der Wiederherstellung einer unter Quarantäne gestellten Datei eine Benachrichtigung auf dem Endpunkt an
Einstellungen für "Vorausschauendes Maschinenlernen"	Zeigt nach der Erkennung einer unbekannten Bedrohung eine Benachrichtigung auf dem Endpunkt an.
Eigenschutz des OfficeScan Agents	*OfficeScan Agent Eigenschutz auf Seite 15-13*
Einstellungen für die zeitgesteuerte Suche	*Berechtigungen für die zeitgesteuerte Suche gewähren und die Berechtigungsbenachrichtigung anzeigen auf Seite 7-66*
Cache-Einstellungen für die Suche	*Cache-Einstellungen für die Suche auf Seite 7-73*
Einstellungen für die Suche in POP3-Mails	*Mail Scan-Berechtigungen gewähren und POP3 Mail Scan aktivieren auf Seite 7-72*
Einschränkung des Zugriffs auf OfficeScan Agent	*Einschränkung des Zugriffs auf die OfficeScan Agent-Konsole auf Seite 15-18*
Aufforderung zum Neustart	*Benachrichtigungen bei Sicherheitsrisiken für OfficeScan Agent Benutzer auf Seite 7-97*

6. Klicken Sie bei der Auswahl von Domäne(n) oder Agent(s) in der Agent-Hierarchie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

- **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf solche Agents an, die neu zu einer vorhandenen/zukünftigen Domäne hinzukommen. Zukünftige Domänen sind Domänen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
- **Nur auf zukünftige Domänen anwenden**: Wendet die Einstellungen nur auf Agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf Agents angewendet, die neu zu einer vorhandenen Domäne hinzukommen.

Teil IV

Zusätzlichen Schutz bereitstellen

Kapitel 16

Schützen externer Agents

In diesem Kapitel werden die Installation des Edge-Relais-Servers und die Konfigurationsschritte beschrieben, die zum Schützen von OfficeScan Agents notwendig sind, die das Firmenintranet verlassen.

Es werden folgende Themen behandelt:

- *Edge-Relais-Server auf Seite 16-2*
- *Systemanforderungen des Edge-Relais-Servers auf Seite 16-3*
- *Installieren des Edge-Relais-Servers auf Seite 16-4*
- *Herstellen einer Verbindung zum Edge-Relais-Server auf Seite 16-13*
- *Verwalten der Edge-Relais-Server-Verbindung auf Seite 16-15*
- *Verwalten von Edge-Relais-Server-Zertifikaten auf Seite 16-16*

Edge-Relais-Server

Der OfficeScan Edge-Relais-Server bietet Administratoren Transparenz und erhöhten Schutz auf Endpunkten, die von Benutzern außerhalb des Firmenintranets betrieben werden. Durch Installation des Edge-Relais-Servers in der entmilitarisierten Zone (Demilitarized Zone, DMZ) können externe OfficeScan Agents, die keine funktionierende Verbindung zum OfficeScan Server herstellen können, weiterhin die in der folgenden Tabelle aufgeführten Aufgaben durchführen.

Wichtig

Der Edge-Relais-Server unterstützt keine IPv6-Kommunikation.

AUFGABE	BESCHREIBUNG
Synchronisierung der Listen der verdächtigen Objekte	Der Edge-Relais-Server erhält die Listen der verdächtigen Objekte gemäß dem konfigurierten Zeitplan vom OfficeScan Server und verteilt die Listen an externe Agents. Weitere Informationen finden Sie unter *Einstellungen für Liste der verdächtigen Objekte auf Seite 14-38*.
Exemplar Zusendung	Externe Agenten, die eine unbekannte Bedrohung erkennen, können das verdächtige Objekt an den konfigurierten Virtual Analyzer senden. Die Weiterleitung verdächtiger Objekte von externen Agents an den Virtual Analyzer erfolgt folgendermaßen: 1. Externe Agents senden das Objekt an den Edge-Relais-Server. 2. Der Edge-Relais-Server übergibt das Objekt während der nächsten konfigurierten Synchronisierung an den OfficeScan Server. 3. Der OfficeScan Server übergibt das Objekt dann zu Analysezwecken an den Virtual Analyzer. Weitere Informationen finden Sie unter *Exemplar Zusendung auf Seite 8-11*.

Aufgabe	Beschreibung
Protokollweiterleitung	Der Edge-Relais-Server sammelt die Protokolle der externen Agents und sendet die Protokolldaten gemäß dem konfigurierten Zeitplan in regelmäßigen Abständen an den OfficeScan Server.
Statusbericht	Externe Agents senden Statusaktualisierungen an den Edge-Relais-Server, wie z. B. aktuelles Pattern und Komponentenversionen.

Nach der Konfiguration des Edge-Relais-Servers empfangen OfficeScan Agents die Einstellungen und senden automatisch Berichte an den Edge-Relais-Server, sobald die Verbindung zum OfficeScan Server nicht mehr verfügbar ist.

Die Kommunikation zwischen dem Edge-Relais-Server, dem OfficeScan Server und den OfficeScan Agents wird mit Hilfe von Zertifikatsauthentifizierung verschlüsselt.

Weitere Informationen finden Sie unter *Verwalten von Edge-Relais-Server-Zertifikaten auf Seite 16-16*.

Systemanforderungen des Edge-Relais-Servers

Stellen Sie vor der Installation des Edge-Relais-Servers sicher, dass der Zielserver die Mindestsystemanforderungen erfüllt.

Ressource	Voraussetzungen
Prozessor	2 GHz Doppelkern
Arbeitsspeicher	4 GB
Festplattenspeicher	50 GB
Betriebssystem	• Windows Server 2016 • Windows Server 2012 R2

RESSOURCE	VORAUSSETZUNGEN

Netzwerkkarte	• 2 Netzwerkkarten
	  • Eine für Intranetverbindungen zum OfficeScan Server
	  • Eine für externe Verbindungen zu externen OfficeScan Agents
	• 1 zur Verwendung verschiedener Ports für Intranet- und Internetverbindungen konfigurierte Netzwerkkarte

Datenbank	• SQL Server™ 2008 R2 Express (oder höher) • SQL Server™ 2008 R2 (oder höher) **Hinweis** Das Setup-Programm des OfficeScan Edge-Relais-Servers bietet die Möglichkeit, SQL Server 2016 SP1 Express während der Installation zu installieren.

Installieren des Edge-Relais-Servers

Stellen Sie vor der Installation des Edge-Relais-Servers sicher, dass der Zielserver die Mindestsystemanforderungen erfüllt.

Weitere Informationen finden Sie unter *Systemanforderungen des Edge-Relais-Servers auf Seite 16-3*.

Wichtig

Der Edge-Relais-Server unterstützt keine IPv6-Kommunikation.

Prozedur

1. Suchen Sie nach dem Ordner <*Installationsordner des Servers*>`\PCCSRV\Admin\Utility\EdgeServer` auf dem OfficeScan Server und kopieren Sie den Ordner auf den Edge-Relais Zielserver.

2. Öffnen Sie auf dem Edge-Relais Zielserver den Ordner `EdgeServer` und führen Sie die Datei `setup.exe` aus, um die Installation zu starten.

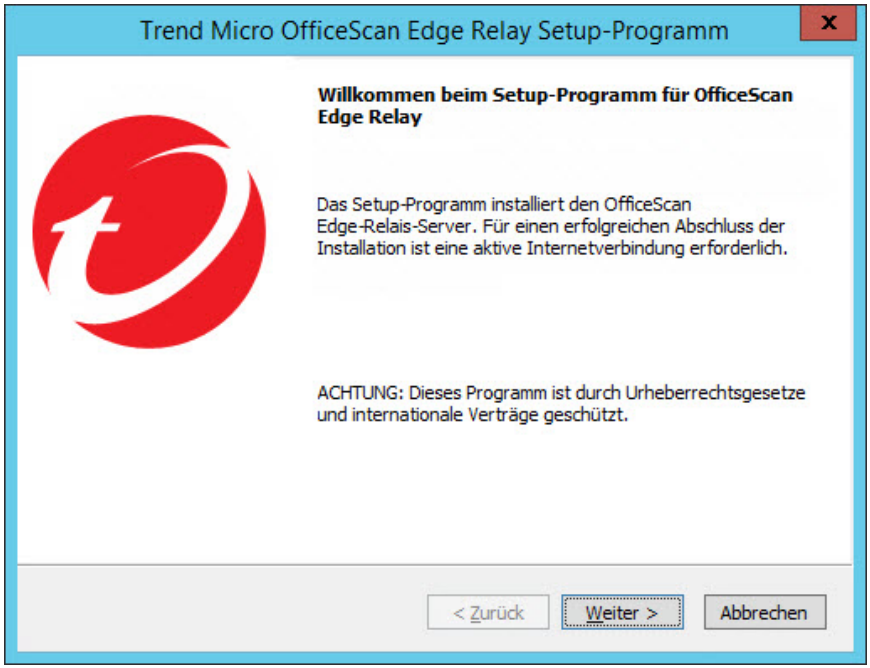
   Das Setup-Paket überprüft den Server auf erforderliche Komponenten.

3. Wenn eine der folgenden Komponenten nicht auf dem Server vorhanden ist, klicken Sie auf **Installieren**, um das Setup-Programm zu veranlassen, die fehlenden Komponenten während der Installation des Edge-Relais-Servers zu installieren.

   - Microsoft .NET Framework 4.6.1
   - Microsoft Visual C++ 2012 Update 4 Wiederverteilungspaket (x64)
   - Microsoft SQL Server System CLR Types 13.0.1601 (x64)
   - SQL Server Transact-SQL ScriptDom 13.0.1061 (x64)
   - Microsoft SQL Server Data-Tier Application Framework (x64)
   - Microsoft ODBC Driver 13 for SQL Server (x64)
   - Microsoft SQL Server 2012 Native Client 11.2.5058.0 (x64)

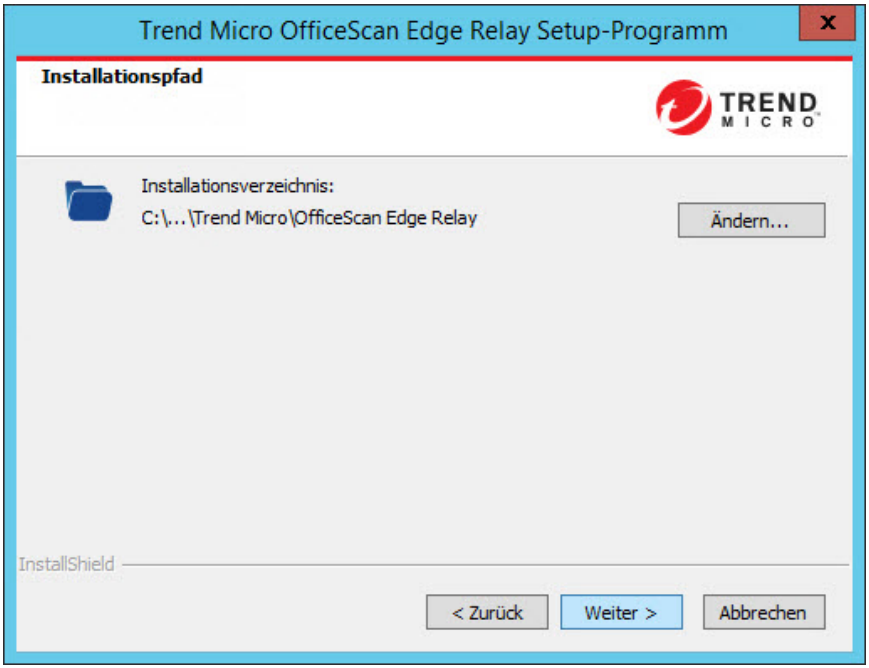
   Das Begrüßungsfenster wird angezeigt.

4. Klicken Sie auf **Weiter**.



Das Fenster **Installationspfad** wird angezeigt.

5. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf **Ändern...**, um einen anderen Speicherort auszuwählen.



6. Klicken Sie auf **Weiter>**.

   Das Fenster **Edge-Relais-Server - OfficeScan Agent-Verbindung** wird geöffnet.

7. Geben Sie die folgenden Einstellungen an, die von externen OfficeScan Agents zum Herstellen einer Verbindung zum Edge-Relais-Server verwendet werden:

   - **Vollqualifizierter Domänenname (FQDN)**: Geben Sie den FQDN des Edge-Relais-Servers ein.
   - **IP-Adresse**: Wählen Sie das IP-Adressformat aus.

     Wichtig

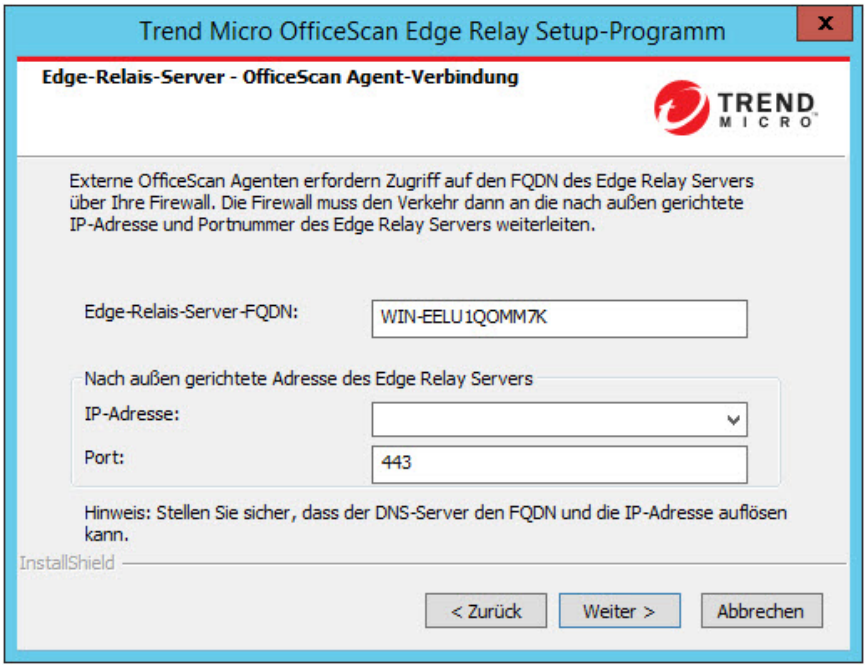
     Der Edge-Relais-Server unterstützt keine IPv6-Kommunikation.

   - **Port**: Übernehmen Sie den Standardport oder geben Sie einen Port an.

Wichtig

Sie müssen die Firewall und das Gateway konfigurieren, um Folgendes zuzulassen:

- Umleitung der OfficeScan Agent-Kommunikation aus dem Internet an den Edge-Relais-Server
- Kommunikation über den angegebenen Port



8. Klicken Sie auf **Weiter>**.

   Das Fenster **Edge-Relais-Server - OfficeScan Server-Verbindung** wird geöffnet.

9. Geben Sie die folgenden Einstellungen an, die vom OfficeScan Server zum Herstellen einer Verbindung zum Edge-Relais-Server verwendet werden:

- **IP-Adresse**: Wählen Sie das IP-Adressformat aus.

Wichtig

Der Edge-Relais-Server unterstützt keine IPv6-Kommunikation.

- **Port**: Übernehmen Sie den Standardport oder geben Sie einen Port an.

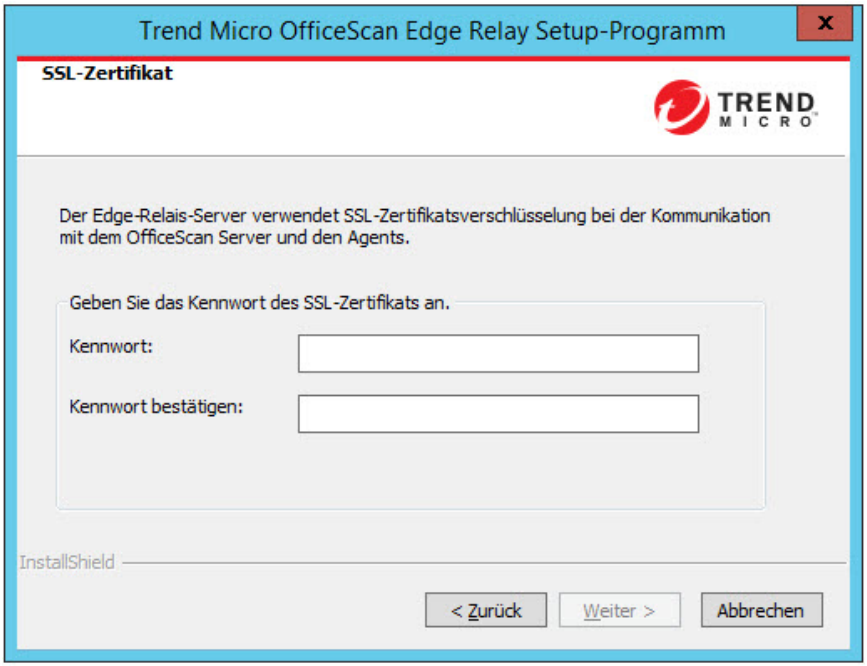
Wichtig

- Der Port für den OfficeScan Server muss sich von dem für externe OfficeScan Agents konfigurierten Port unterscheiden.
- Stellen Sie sicher, dass die Firewall Kommunikation über den angegebenen Port zulässt.

10. Klicken Sie auf **Weiter>**.

    Das Fenster **SSL-Zertifikat** wird angezeigt.

11. Geben Sie das für das Edge-Relais-Server-Zertifikat verwendete Kennwort an und bestätigen Sie es.

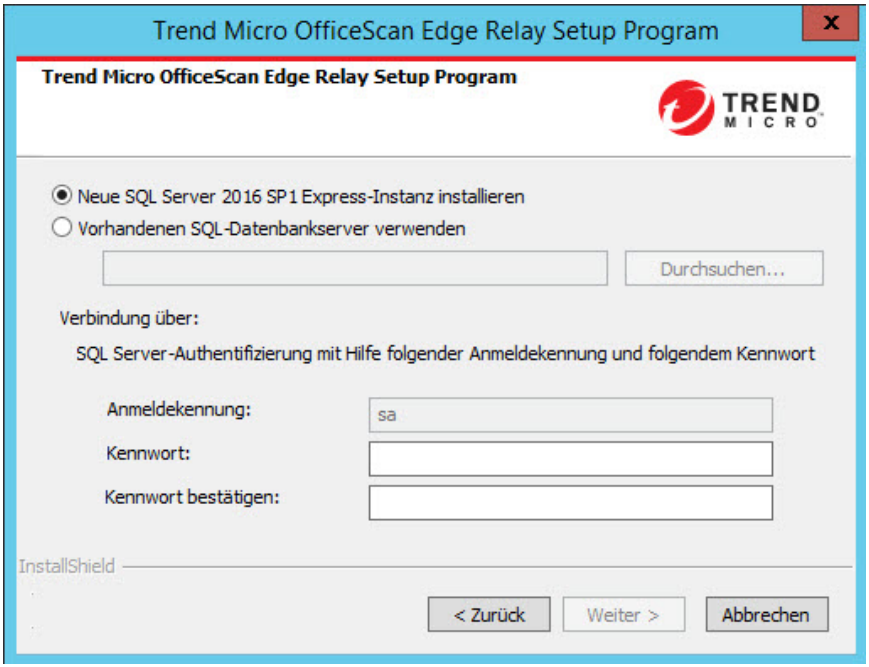


12. Klicken Sie auf **Weiter>**.

    Das Fenster **Datenbankserver** wird angezeigt.

13. Geben Sie die vom Edge-Relais-Server verwendete SQL Server-Datenbank an:

    - **Neue SQL Server 2016 SP1 Express-Instanz installieren**
    - **Vorhandenen SQL-Datenbankserver verwenden**: Klicken Sie auf **Durchsuchen...**, um einen der verfügbaren Server in der Liste auszuwählen.

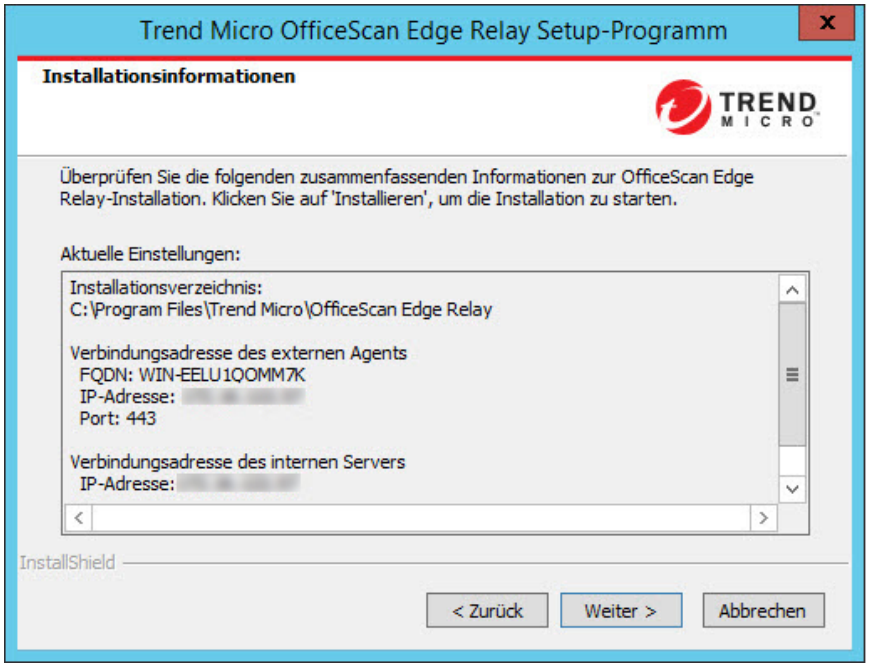


14. Geben Sie das zum Herstellen einer Verbindung mit der SQL Server-Datenbank verwendete Kennwort an. Wenn Sie eine neue SQL Server Express-Datenbank installieren, bestätigen Sie das Kennwort.

15. Klicken Sie auf **Weiter>**.

    Das Fenster **Installationsdaten** wird angezeigt.

16. Klicken Sie auf **Weiter >**, um mit der Installation zu beginnen.



Nach Abschluss der Installation wird das Fenster **Der InstallShield Wizard ist abgeschlossen** geöffnet.

17. Klicken Sie auf **Fertig stellen**.

Der Edge-Relais-Server kann nun verwendet werden. Sie können den OfficeScan Server konfigurieren, um eine Verbindung mit dem Edge-Relais-Server herzustellen.

Weitere Informationen finden Sie unter *Herstellen einer Verbindung zum Edge-Relais-Server auf Seite 16-13*.

Herstellen einer Verbindung zum Edge-Relais-Server

Nach der Installation des Edge-Relais-Servers müssen Sie dessen Verbindungseinstellungen auf dem OfficeScan Server konfigurieren. Nach dem Herstellen einer Verbindung zum Edge-Relais-Server erhalten OfficeScan Agents, die an

den OfficeScan Server berichten, die Verbindungseinstellungen. Nach dem Verlassen des Firmenintranets können diese dann automatisch mit dem Edge-Relais-Server kommunizieren.

Prozedur

1. Navigieren Sie in der OfficeScan Webkonsole zu **Administration** > **Einstellungen** > **Edge-Relais**.

   Das Fenster **Edge-Relais-Einstellungen** wird angezeigt.

2. Geben Sie die **IP-Adresse** und den **Port** des Edge-Relais-Servers ein.

   Hinweis

   Stellen Sie die IP-Adresse und den Port bereit, die Sie für die Intranetkommunikation mit dem Edge-Relais-Server konfiguriert haben.

3. Wenn die Umgebung einen Proxy-Server benötigt, um mit dem Edge-Relais-Server in der entmilitarisierten Zone zu kommunizieren, aktivieren Sie **Mit Hilfe der Einstellungen des externen Proxyservers eine Verbindung herstellen**.

   Klicken Sie zum Konfigurieren der externen Proxy-Einstellungen auf **Einstellungen des externen Proxyservers**, um das Fenster **Proxy-Einstellungen** zu öffnen. Konfigurieren Sie die notwendigen Proxyinformationen im Abschnitt **OfficeScan Server-Updates**.

   Weitere Informationen finden Sie unter *Proxy-Einstellungen für Server konfigurieren auf Seite 6-20*.

4. Klicken Sie auf **Verbinden**.

   Nach der erfolgreichen Herstellung einer Verbindung mit dem Edge-Relais-Server wird das Fenster mit den Verbindungsinformationen aktualisiert.

   Weitere Informationen finden Sie unter *Verwalten der Edge-Relais-Server-Verbindung auf Seite 16-15*.

Verwalten der Edge-Relais-Server-Verbindung

Nach dem Herstellen einer Verbindung zum Edge-Relais-Server erhalten OfficeScan Agents, die an den OfficeScan Server berichten, die Verbindungseinstellungen. Nach dem Verlassen des Firmenintranets können diese dann automatisch mit dem Edge-Relais-Server kommunizieren. Sie können den Status der Edge-Relais-Server-Verbindung dann überwachen, den Synchronisierungszeitplan konfigurieren und eine sofortige Synchronisierung über das Fenster **Edge-Relais-Einstellungen** durchführen.

Prozedur

1. Navigieren Sie in der OfficeScan Webkonsole zu **Administration** > **Einstellungen** > **Edge-Relais**.

   Das Fenster **Edge-Relais-Einstellungen** wird angezeigt.

2. Überwachen oder konfigurieren Sie die Einstellungen des Edge-Relais-Servers.

EINSTELLUNG	BESCHREIBUNG
IP-Adresse	Die aktuelle IP-Adresse des Edge-Relais-Servers Zum Konfigurieren neuer Verbindungseinstellungen für den Edge-Relais-Server klicken Sie auf **Verbindung trennen** und konfigurieren Sie die Verbindungseinstellungen neu. Weitere Informationen finden Sie unter *Herstellen einer Verbindung zum Edge-Relais-Server auf Seite 16-13*.
Status	Der Verbindungsstatus „Online“ oder „Offline“ zwischen dem OfficeScan Server und dem Edge-Relais-Server
Synchronisiert	Der Zeitpunkt der letzten Synchronisierung des Edge-Relais-Servers mit dem OfficeScan Server Klicken Sie auf **Jetzt synchronisieren**, um eine sofortige Synchronisierung zwischen dem OfficeScan Server und dem Edge-Relais-Server durchzuführen.

EINSTELLUNG	BESCHREIBUNG
Zeitgesteuerte Synchronisierung	Die Häufigkeit, mit der der OfficeScan Server mit dem Edge-Relais-Server synchronisiert wird Legen Sie unter Berücksichtigung der Bandbreite die Synchronisierungshäufigkeit auf **Stündlich** oder **Alle 15 Minuten** fest.

3. Klicken Sie auf **Speichern**.

Verwalten von Edge-Relais-Server-Zertifikaten

OfficeScan stellt ein Befehlszeilentool bereit, mit dem Sie das Zertifikat des Edge-Relais-Servers, das von Agents zur Kommunikation verwendet wird, erstellen oder erneuern können. Nach dem Erstellen eines neuen Zertifikats sendet der Edge-Relais-Server das neue Zertifikat an den OfficeScan Server, der bei der nächsten Verbindungsherstellung zwischen Agents und dem OfficeScan Server die Zertifikate auf die Agents verteilt.

Wichtig

Externe OfficeScan Agents müssen eine Verbindung zum OfficeScan Server herstellen, um das neue Edge-Relais-Server-Zertifikat zu erhalten. Alle externen Agents, die das aktualisierte Zertifikat nicht erhalten, können erst dann wieder mit dem Edge-Relais-Server kommunizieren, wenn die Verbindung mit dem OfficeScan Server hergestellt wird.

Prozedur

1. Öffnen Sie auf dem Edge-Relais-Server einen Befehlszeileneditor und navigieren Sie zu folgendem Verzeichnis:

   ```
   C:\Programme\Trend Micro\OfficeScan Edge\OfcEdgeSvc\web
   \service
   ```

2. Führen Sie das Zertifikatstool aus, indem Sie folgenden Befehl verwenden:

   `OfcEdgeCfg.exe --renewcert -certpwd <password>`

   Wobei gilt:

- **`--renewcert`**: Erstellt das neue Zertifikat.
- **`-certpwd <password>`**: Gibt das Kennwort für das Zertifikatspaket an.

Der Edge-Relais-Server erstellt das neue Zertifikatspaket und sendet das Zertifikat automatisch an den OfficeScan Server. Der OfficeScan Server stellt den OfficeScan Agents das neue Zertifikat bereit, wenn die OfficeScan Agents das nächste Mal einen Bericht für den OfficeScan Server erstellen.

Kapitel 17

Plug-in Manager verwenden

In diesem Kapitel wird beschrieben, wie Sie Plug-in Manager einrichten. Außerdem erhalten Sie eine übersicht über die mit Plug-in Manager bereitgestellten Plug-in-Lösungen.

Es werden folgende Themen behandelt:

- *Info über den Plug-in Manager auf Seite 17-2*
- *Plug-in Manager Installation auf Seite 17-3*
- *Verwaltung nativer OfficeScan Funktionen auf Seite 17-4*
- *Plug-in-Programme verwalten auf Seite 17-5*
- *Plug-in Manager deinstallieren auf Seite 17-12*
- *Fehlersuche in Plug-in Manager auf Seite 17-13*

Info über den Plug-in Manager

OfficeScan umfasst ein Framework mit der Bezeichnung Plug-in Manager, das neue Lösungen in die bestehende OfficeScan Umgebung integriert. Um die Verwaltung dieser Lösungen zu vereinfachen, stellt Plug-in Manager die Daten dieser Lösungen in Form von Widgets übersichtlich dar.

Hinweis

Keine der Plug-in-Lösungen unterstützt zurzeit IPv6. Der Server kann diese Lösungen zwar herunterladen, er kann sie aber nicht auf reine IPv6-OfficeScan Agents oder reine IPv6-Hosts verteilen.

Der Plug-in Manager bietet Folgendes:

- **Native Produktfunktionen**

  Einige native OfficeScan Funktionen werden über Plug-in Manager separat lizenziert und aktiviert. In dieser Version fallen zwei Funktionen unter diese Kategorie, nämlich **Trend Micro Virtual Desktop Support** und **OfficeScan Datentschutz**.

- **Plug-in-Programme**

  Plug-in-Programme sind nicht Teil des OfficeScan Programms. Die Plug-in-Programme weisen separate Lizenzen und Management-Konsolen auf. Auf die Management-Konsolen greifen Sie über die OfficeScan Webkonsole zu. Zu den Beispielen für Plug-in-Programme gehören **Trend Micro OfficeScan ToolBox** und **Trend Micro Security (für Mac)**.

- **Dashboard-Registerkarten und -Widgets**

  Im OfficeScan-Fenster **Dashboard** muss Plug-in Manager die Registerkarten und Widgets anzeigen, die zum Überwachen des Schutzstatus des OfficeScan-Servers und -Agents verwendet werden.

Diese Dokumente geben einen allgemeinen Überblick über Installation und Verwaltung von Plug-in-Programmen und erklären die in Widgets dargestellten Informationen über

die Plug-in-Programme. Die Dokumentation enthält außerdem ausführliche Hinweise zur Konfiguration und Verwaltung des jeweiligen Plug-in-Programms.

Plug-in-Programm-Agents auf Endpunkten

Bestimmte Plug-in-Programme (wie z. B. Trend Micro Security (für Mac)) verfügen über Agents, die auf den Windows-Betriebssystemen des Endpunkts installiert werden. Der OfficeScan Agent Plug-in Manager, der unter dem Prozessnamen `CNTAoSMgr.exe` ausgeführt wird, verwaltet diese Agents.

OfficeScan installiert `CNTAoSMgr.exe` zusammen mit OfficeScan Agent. Die einzige zusätzliche Systemvoraussetzung für `CNTAoSMgr.exe` ist Microsoft XML Parser (MSXML) Version 3.0 oder höher.

Hinweis

Andere Plug-in-Programme mit Agents, die nicht unter Windows Betriebssystemen installiert werden, werden nicht über den OfficeScan Agent Plug-in Manager verwaltet. Der Trend Micro Security (für Mac) Agent ist ein Beispiel für diese Agents.

Widgets

Verwenden Sie Widgets, um die verteilten Plug-in-Lösungen übersichtlich darzustellen. Widgets werden im Fenster **Dashboard** von OfficeScan Server zur Verfügung gestellt. Ein besonderes Widget mit der Bezeichnung **OfficeScan- und Plug-in-Mashup** kombiniert Daten der OfficeScan Agents und Plug-in-Lösungen und stellt sie in der agent-Hierarchie dar.

Das Administratorhandbuch enthält eine Übersicht über Widgets und Lösungen, in denen Widgets unterstützt werden.

Plug-in Manager Installation

In früheren Versionen von Plug-in Manager wird das Plug-in Manager-Installationspaket vom Trend Micro ActiveUpdate Server heruntergeladen und dann auf dem Computer installiert, auf dem der OfficeScan Server gehostet wird. In dieser Version ist das

Installationspaket im Installationspaket des OfficeScan Servers an folgendem Speicherort enthalten:

<*Installationsordner des Servers*>\PCCSRV\Admin\Utility\PLM\PLMSetup.exe

Führen Sie die Datei `PLMSetup.exe` aus, um Plug-in Manager zu installieren.

Bei Benutzern, die OfficeScan zum ersten Mal verwenden, werden sowohl der OfficeScan Server als auch der Plug-in Manager nach Abschluss der OfficeScan-Installation installiert. Benutzer, die auf diese Version von OfficeScan upgraden und bereits Plug-in Manager verwenden, müssen den Plug-in Manager Dienst beenden, bevor sie das Installationspaket ausführen.

Aufgaben nach der Installation ausführen

Führen Sie nach der Installation von Plug-in Manager die folgenden Schritte durch:

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
2. Verwalten Sie die Plug-in-Lösungen.
3. Verwenden Sie das **Dashboard** auf der OfficeScan Webkonsole zur Verwaltung der Widgets für die Plug-in-Lösungen.

Verwaltung nativer OfficeScan Funktionen

Die nativen OfficeScan Funktionen werden zusammen mit OfficeScan installiert, und Administratoren aktivieren diese Funktionen über den Plug-in Manager. Einige Funktionen, wie etwa Trend Micro Virtual Desktop Support, werden über den Plug-in Manager verwaltet, während andere, wie etwa der OfficeScan Datenschutz, über die OfficeScan Webkonsole verwaltet werden.

Plug-in-Programme verwalten

Installieren und aktivieren Sie Plug-in-Programme unabhängig von OfficeScan. Jedes Plug-in bietet eine separate Konsole für das Produkt-Management. Diese Management-Konsolen sind über die OfficeScan Webkonsole zugänglich.

Plug-in-Programme-Installation

Plug-in-Programme werden auf der **Plug-in Manager**-Konsole angezeigt. Auf der Konsole können Sie die Programmme herunterladen, installieren und verwalten. Der Plug-in Manager lädt das Installationspaket für das Plug-in-Programm vom Trend Micro ActiveUpdate Server oder einer benutzerdefinierten Update-Quelle herunter, falls eine solche korrekt erstellt wurde. Zum Herunterladen des Pakets vom ActiveUpdate Server ist eine Internet-Verbindung erforderlich.

Wenn der Plug-in Manager ein Installationspaket herunterlädt oder die Installation startet, deaktiviert er vorübergehend andere Plug-in-Programmfunktionen wie Downloads, Installationen und Upgrades.

Der Plug-in Manager unterstützt keine Installation oder Verwaltung von Plug-in-Programmen über die Single-Sign-On-Funktion von Trend Micro Control Manager.

Installation von Plug-in-Programme

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
2. Navigieren Sie im Fenster **Plug-in Manager** zum Abschnitt für Plug-in-Programme und klicken Sie auf **Download**.

   Die Größe des Plug-in-Programmpakets wird neben der Schaltfläche **Download** angezeigt. Der Plug-in Manager speichert das heruntergeladene Paket unter `<Installationsordner des Servers>\PCCSRV\Download\Product`.

   Plug-in-Manager speichert das heruntergeladene Paket unter `<Installationsordner des Servers>\PCCSRV\Download\Product`.

Während des Downloads können Sie den Fortschritt überwachen oder zu anderen Fenstern navigieren.

Hinweis

Treten beim Herunterladen oder Installieren des Pakets in OfficeScan Probleme auf, überprüfen Sie die Server-Update-Protokolle auf der OfficeScan Webkonsole. Klicken Sie im Hauptmenü auf **Protokolle** > **Server-Update**.

3. Klicken Sie auf **Jetzt installieren** oder **Später installieren**.

   - Wenn Sie auf **Jetzt installieren** klicken, wird die Installation gestartet und ein Fenster für den Installationsfortschritt angezeigt.
   - Nach dem Klicken auf **Später installieren** wird das Fenster **Plug-in Manager** angezeigt.

     Installieren Sie das Plug-in-Programm, indem Sie auf die Schaltfläche **Installieren** im Plug-in-Programm-Abschnitt des Fensters **Plug-in Manager** klicken.

   Das Fenster **Trend Micro Endbenutzer-Lizenzvereinbarung** wird angezeigt.

   Hinweis

   Dieses Fenster ist nicht für alle Plug-in-Programme erforderlich. Falls dieses Fenster nicht angezeigt wird, wird die Installation des Plug-ins gestartet.

4. Klicken Sie auf **Stimme zu**, um das Plug-in-Programm zu installieren.

   Während der Installation können Sie den Fortschritt überwachen oder zu anderen Fenstern navigieren.

   Hinweis

   Treten beim Herunterladen oder Installieren des Pakets in OfficeScan Probleme auf, überprüfen Sie die Server-Update-Protokolle auf der OfficeScan Webkonsole. Klicken Sie im Hauptmenü auf **Protokolle** > **Server-Update**.

Nach der Installation wird die aktuelle Version des Plug-in-Programms im Fenster **Plug-in Manager** angezeigt.

Plug-in-Programme Lizenz aktivieren

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
2. Navigieren Sie im Fenster **Plug-in Manager** zum Abschnitt für Plug-in-Programme und klicken Sie auf **Programm verwalten**.

   Das Fenster **Produktlizenz – Neuer Aktivierungscode** wird angezeigt.
3. Geben Sie den Aktivierungscode in die Textfelder ein, oder kopieren Sie den Aktivierungscode und fügen ihn in die Textfelder ein.
4. Klicken Sie auf **Speichern**.

   Die Plug-in-Konsole wird angezeigt.

Lizenzdaten anzeigen und Lizenzen verlängern

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
2. Navigieren Sie im Fenster **Plug-in Manager** zum Abschnitt für Plug-in-Programme und klicken Sie auf **Programm verwalten**.
3. Navigieren Sie auf der Plug-in-Konsole zum Hyperlink **Lizenzdaten anzeigen**.

   Der Hyperlink **Lizenzdaten anzeigen** wird nicht für alle Plug-in-Programme an derselben Stelle angezeigt. Weitere Informationen finden Sie in der Benutzerdokumentation zu dem Plug-in-Programm.

4. Ein Fenster mit den folgenden Informationen zur Lizenz wird geöffnet.

Option	Bezeichnung
Status	Wird entweder als "Aktiviert", "Nicht aktiviert" oder "Abgelaufen" angezeigt
Version	Wird entweder als "Vollversion" oder "Testversion" angezeigt **Hinweis** Die Aktivierung sowohl der Vollversion als auch der Testversion wird als "Vollversion" angezeigt.
Arbeitsplätze	Zeigt an, wie viele Endpunkte vom Plug-in-Programm verwaltet werden können.
Lizenz läuft ab am	Wenn es für das Plug-in-Programm mehrere Lizenzen gibt, wird das am weitesten in der Zukunft liegende Ablaufdatum angezeigt. Laufen die Lizenzen beispielsweise am 31.12.2011 und am 30.06.2011 ab, wird das Datum 31.12.2011 angezeigt.
Aktivierungscode	Zeigt den Aktivierungscode an
Erinnerungen	In Abhängigkeit von der aktuellen Lizenzversion zeigt das Plug-in Erinnerungen zum Datum des Lizenzablaufs an, entweder während der Übergangsfrist (nur Vollversionen) oder wenn die Lizenz abläuft.

Hinweis

Die Dauer der Übergangsfrist ist regional verschieden. Überprüfen Sie die Übergangsfrist eines Plug-in-Programms mit einem Trend Micro Vertriebspartner.

Nach Ablauf der Lizenz für ein Plug-in-Programm ist das Plug-in weiterhin funktionsfähig, Updates und Support sind aber nicht mehr verfügbar.

5. Klicken Sie auf **Detailansicht der Lizenz online anzeigen**, um Informationen zur aktuellen Lizenz auf der Trend Micro Website anzuzeigen.

6. Um die aktuellsten Lizenzdaten anzuzeigen, klicken Sie auf **Informationen aktualisieren**.

7. Klicken Sie auf **Neuer Aktivierungscode**, um das Fenster **Produktlizenz – Neuer Aktivierungscode** zu öffnen.

   Weitere Informationen finden Sie unter *Plug-in-Programme Lizenz aktivieren auf Seite 3-4*.

Verwaltung der Plug-in-Programme

Konfigurieren Sie die Einstellungen und führen Sie programmbezogene Aufgaben über die Management-Konsole des Plug-in-Programms durch, auf die Sie über die OfficeScan Webkonsole zugreifen können. Diese Aufgaben umfassen die Aktivierung des Programms und möglicherweise die Verteilung des Plug-in-Programm-Agents auf die Endpunkte. Die Dokumentation enthält außerdem ausführliche Hinweise zur Konfiguration und Verwaltung des jeweiligen Plug-in-Programms.

Plug-in-Programme verwalten

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.

2. Navigieren Sie im Fenster **Plug-in Manager** zum Abschnitt für Plug-in-Programme und klicken Sie auf **Programm verwalten**.

ABBILDUNG 17-1. Schaltfläche "Programm verwalten"

   Wenn Sie das Plug-in-Programm zum ersten Mal verwalten, muss es möglicherweise erst aktiviert werden. Weitere Informationen finden Sie unter *Plug-in-Programme Lizenz aktivieren auf Seite 3-4*.

Plug-in-Programme Upgrades

Jede neue Version eines installierten Plug-in-Programms wird auf der Plug-in Manager-Konsole angezeigt. Laden Sie das Plug-in-Programm herunter, und upgraden Sie das Plug-in-Programm auf der Konsole. Plug-in Manager lädt das Paket vom Trend Micro ActiveUpdate Server oder einer definierten Update-Quelle herunter, falls eine solche ordnungsgemäß erstellt wurde. Zum Herunterladen des Pakets vom ActiveUpdate Server ist eine Internet-Verbindung erforderlich.

Wenn der Plug-in Manager ein Installationspaket herunterlädt oder ein Upgrade startet, deaktiviert er vorübergehend andere Plug-in-Programmfunktionen wie Downloads, Installationen und Upgrades.

Der Plug-in Manager unterstützt kein Upgrade des Plug-in-Programms über die Single-Sign-On-Funktion von Trend Micro Control Manager.

Plug-in-Programme upgraden

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
2. Navigieren Sie im Fenster **Plug-in Manager** zum Abschnitt für Plug-in-Programme und klicken Sie auf **Download**.

   Die Größe des Upgrade-Pakets erscheint neben der Schaltfläche **Download**.

   Während des Downloads können Sie den Fortschritt überwachen oder zu anderen Fenstern navigieren.

   Hinweis

   Treten beim Herunterladen oder Installieren des Pakets in OfficeScan Probleme auf, überprüfen Sie die Server-Update-Protokolle auf der OfficeScan Webkonsole. Klicken Sie im Hauptmenü auf **Protokolle** > **Server-Update**.

3. Nach dem Download des Pakets wird ein neues Fenster angezeigt:

4. Klicken Sie auf **Jetzt upgraden** oder **Später upgraden**.

   - Wenn Sie auf **Jetzt upgraden** klicken, wird das Upgrade gestartet und ein Fenster für den Upgrade-Fortschritt angezeigt.

   - Wenn Sie auf **Später upgraden** klicken, wird das Fenster **Plug-in Manager** angezeigt.

     Upgraden Sie das Plug-in-Programm, indem Sie auf die Schaltfläche **Upgrade** im Plug-in-Programm-Abschnitt des Fensters **Plug-in Manager** klicken.

Nach dem Upgrade muss der Plug-in Manager Dienst möglicherweise neu gestartet werden. Das Fenster **Plug-in Manager** ist dann vorübergehend nicht verfügbar. Sobald das Fenster wieder verfügbar ist, wird die aktuelle Version des Plug-in-Programms angezeigt.

Plug-in-Programme Deinstallation

Ein Plug-in-Programm kann mit Hilfe der folgenden Methoden deinstalliert werden:

- Deinstallieren Sie das Plug-in-Programm über die Plug-in Manager-Konsole.
- Deinstallieren Sie den OfficeScan Server. Dabei werden der Plug-in Manager und alle installierten Plug-in-Programme ebenfalls deinstalliert. Anweisungen zum Deinstallieren des OfficeScan-Servers finden Sie im *Installations- und Upgrade-Handbuch für OfficeScan*.

Bei Plug-in-Programmen mit Agents auf dem Endpunkt:

- In der Dokumentation des Plug-in-Programms finden Sie Hinweise darüber, ob bei der Deinstallation des Plug-in-Programms auch der Plug-in-Agent deinstalliert wird.
- Bei Plug-in-Agents, die auf demselben Endpunkt wie der OfficeScan Agent installiert sind, werden bei der Deinstallation des OfficeScan Agent auch die Plug-in-Agents und der OfficeScan Agent Plug-in Manager (`CNTAoSMgr.exe`) deinstalliert.

Plug-in-Programme über die Plug-In Manager-Konsole deinstallieren

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
2. Navigieren Sie im Fenster **Plug-in Manager** zum Abschnitt für Plug-in-Programme, und klicken Sie auf **Programm verwalten**.

3. Während der Deinstallation können Sie den Deinstallationsfortschritt überwachen oder zu anderen Fenstern navigieren.
4. Aktualisieren Sie das Fenster **Plug-in Manager** nach der Deinstallation.

   Das Plug-in-Programm steht wieder zur Installation zur Verfügung.

Plug-in Manager deinstallieren

Deinstallieren Sie den OfficeScan Server, um Plug-in Manager und alle installierten Plug-in-Programme zu deinstallieren. Anweisungen zum Deinstallieren des OfficeScan-Servers finden Sie im *Installations- und Upgrade-Handbuch für OfficeScan*.

Fehlersuche in Plug-in Manager

Überprüfen Sie die Debug-Protokolle von OfficeScan Server und OfficeScan Agent, um Informationen zur Fehlerbehebung für Plug-In Manager und Plug-in-Programme zu erhalten.

Das Plug-in-Programm wird nicht auf der Plug-in Manager-Konsole angezeigt.

Ein zum Download und zur Installation verfügbares Plug-in-Programm wird möglicherweise auf der Plug-in Manager-Konsole aus folgenden Gründen nicht angezeigt:

Prozedur

1. Der Plug-in Manager hat den Download des Plug-in-Programms noch nicht abgeschlossen, da dieser bei großen Programmpaketen länger dauert. Überprüfen Sie von Zeit zu Zeit das Fenster, um festzustellen, ob das Plug-in-Programm angezeigt wird.

   Hinweis

   Wenn Plug-in Manager das Plug-in-Programm nicht herunterladen kann, wiederholt er den Versuch automatisch nach 24 Stunden. Um den Download manuell zu starten, muss der OfficeScan Plug-in Manager Dienst neu gestartet werden.

2. Der Servercomputer kann keine Verbindung mit dem Internet herstellen. Verbindet sich der Server über einen Proxy-Server mit dem Internet, stellen Sie sicher, dass die Internet-Verbindung über die Proxy-Einstellungen hergestellt werden kann.

3. Die OfficeScan Update-Adresse ist nicht der ActiveUpdate Server. Navigieren Sie auf der OfficeScan Webkonsole zu **Updates** > **Server** > **Update-Adresse**, und überprüfen Sie die Update-Adresse. Ist die Update-Adresse nicht der ActiveUpdate Server, haben Sie folgende Möglichkeiten:

   - Wählen Sie den ActiveUpdate Server als Update-Adresse.

- Wenn Sie **Andere Update-Adresse** auswählen, wählen Sie den ersten Eintrag in der Liste **Andere Update-Adresse** als Update-Adresse aus, und überprüfen Sie, ob sich die Quelle mit dem ActiveUpdate Server erfolgreich verbinden kann. Der Plug-in Manager unterstützt nur den ersten Eintrag in der Liste.
- Wenn Sie **Intranet-Site, die eine Kopie der aktuellen Datei enthält** auswählen, stellen Sie sicher, dass der Endpunkt im Intranet ebenfalls eine Verbindung zum ActiveUpdate Server herstellen kann.

Probleme bei der Installation und Anzeige des Plug-in Agents auf den Endpunkte

Die Installation des Agents eines Plug-in-Programms auf dem Endpunkt könnte fehlschlagen oder der Agent könnte aus folgenden Gründen nicht auf der OfficeScan Agent-Konsole angezeigt werden:

Prozedur

1. Plug-in Manager (`CNTAosMgr.exe`) wird auf dem Endpunkt nicht ausgeführt. Öffnen Sie auf dem OfficeScan Agent Endpunkt den Windows Task-Manager, und führen Sie den Prozess `CNTAosMgr.exe` aus.
2. Das Installationspaket für den Plug-in-Agent wurde nicht in den Ordner des OfficeScan Agent Endpunkts unter `<Installationsordner des Agents>\AU_Data\AU_Temp\{xxx}AU_Down\Product` heruntergeladen. Überprüfen Sie die Datei `Tmudump.txt` unter `\AU_Data\AU_Log\` nach Ursachen für das Fehlschlagen des Downloads.

   Hinweis

   Wenn der Agent erfolgreich installiert wurde, befinden sich die Informationen über diesen Agent in der Datei `<Installationsordner des Agents>\AOSSvcInfo.xml`.
3. Die Installation des Agents ist fehlgeschlagen und erfordert eine weitere Aktion. Den Installationsstatus sehen Sie auf der Management-Konsole des Plug-in-

Programms. Dort können Sie verschiedene Aktionen durchführen, wie etwa den OfficeScan Agent-Endpunkt nach der Installation neu starten oder vor der Installation die für das Betriebssystem erforderlichen Patches installieren.

Agents auf den Endpunkte können nicht gestartet werden, wenn die Einstellung des automatischen Konfigurationsskripts im Internet Explorer auf einen Proxy-Server umgeleitet wird

Der OfficeScan Agent Plug-in Manager (`CNTAosMgr.exe`) kann Agents auf Endpunkte nicht starten, da der Befehl zum Start des Agents auf einen Proxy-Server umgeleitet wird. Dieses Problem tritt nur dann auf, wenn die Proxy-Einstellung den HTTP-Verkehr des Benutzers auf 127.0.0.1 umleitet.

Um dieses Problem zu beheben, verwenden Sie eine gültige Proxy-Serverrichtlinie. Leiten Sie beispielsweise den HTTP-Verkehr nicht auf 127.0.0.1 um.

Wenn Sie die Proxy-Konfiguration verwenden müssen, die die 127.0.0.1 HTTP-Anfragen steuert, führen Sie die folgenden Aufgaben durch.

Prozedur

1. Konfigurieren Sie die OfficeScan Firewall-Einstellungen auf der OfficeScan Webkonsole.

   Hinweis

   Führen Sie diesen Schritt nur dann aus, wenn Sie die OfficeScan Firewall auf den OfficeScan Agents aktivieren.

   a. Gehen Sie auf der Webkonsole zu **Agents** > **Firewall** > **-Richtlinien** und klicken Sie auf **Ausnahmevorlage bearbeiten**.

   b. Klicken Sie im Fenster Ausnahmevorlage bearbeiten auf **Hinzufügen**.

   c. Verwenden Sie die folgenden Informationen:

- **Name**: Ihr bevorzugter Name
- **Aktion**: Netzwerkdatenverkehr zulassen
- **Richtung**: Eingehend
- **Protokoll**: TCP
- **Port(s)**: Alle Portnummern zwischen 5000 und 49151

d. **IP-Adresse (n)**: Wählen Sie **Einzelne IP-Adresse**, und geben Sie die IP-Adresse Ihres Proxy-Servers ein (empfohlen), oder wählen Sie **Alle IP-Adressen**.

e. Klicken Sie auf **Speichern**.

f. Klicken Sie dann im Fenster Ausnahmevorlage bearbeiten auf **Speichern und für alle vorhandenen Richtlinien übernehmen**.

g. Navigieren Sie zu **Agents** > **Firewall** > **Profile** und klicken Sie auf **Den Agents ein Profil zuweisen**.

Wenn kein Firewall-Profil vorhanden ist, klicken Sie auf "Hinzufügen", und erstellen Sie ein Profil. Verwenden Sie dabei die folgenden Einstellungen:

- **Name**: Ihr bevorzugter Name
- **Beschreibung**: Ihre bevorzugte Beschreibung
- **Richtlinie**: Uneingeschränkter Zugriff

Klicken Sie nach dem Speichern des neuen Profils auf **Den Agents ein Profil zuweisen**.

2. Ändern Sie die Datei `ofcscan.ini`.

a. Öffnen Sie mit einem Texteditor die Datei `ofcscan.ini` im `Installationsordner des Servers`.

b. Suchen Sie nach dem Eintrag **`[Global Setting]`** und schreiben Sie `FWPortNum=21212` in die nächste Zeile. Ersetzen Sie den Wert "21212" mit der Portnummer, die Sie oben in Schritt c angegeben haben.

Beispiel:

```
[Global Setting]

FWPortNum=5000
```

c. Speichern Sie die Datei.

3. Navigieren Sie auf der Webkonsole zu **Agents** > **Globale Agent-Einstellungen** und klicken Sie auf **Speichern**.

Im System, Update-Modul oder Plug-in Manager Programm ist ein Fehler aufgetreten, und die Fehlermeldung enthält einen bestimmten Fehlercode.

In Plug-in Manager werden folgende Fehlercodes in einer Fehlermeldung angezeigt. Können Sie ein Problem trotz unserer Lösungsvorschläge in der unten stehenden Tabelle nicht beheben, wenden Sie sich an Ihren Support-Anbieter.

TABELLE 17-1. Plug-in Manager Fehlercodes

FEHLERCODE	MELDUNG, URSACHE UND LÖSUNG
001	Im Plug-in Manager Programm ist ein Fehler aufgetreten. Das Plug-in Manager Update-Modul antwortet nicht auf Abfragen über den Fortschritt eines Update-Tasks. Das Modul- oder Befehlssteuerprogramm wurde eventuell nicht initialisiert. Starten Sie den OfficeScan Plug-in Manager Dienst neu, und führen Sie den Task erneut aus.

FEHLERCODE	MELDUNG, URSACHE UND LÖSUNG
002	Es ist ein Systemfehler aufgetreten. Das Plug-in Manager Update-Modul kann den Registrierungsschlüssel `SOFTWARE\TrendMicro\OfficeScan\service\AoS` nicht öffnen, da er möglicherweise gelöscht wurde. Führen Sie folgende Schritte durch: 1. Öffnen Sie den Registrierungseditor, und navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service \AoS\OSCE_Addon_Service_CompList_Version`. Setzen Sie den Wert auf 1.0.1000 zurück. 2. Starten Sie den OfficeScan Plug-in Manager Dienst neu. 3. Laden Sie das Plug-in-Programm herunter oder deinstallieren Sie es.

FEHLERCODE	MELDUNG, URSACHE UND LÖSUNG
028	Es ist ein Update-Fehler aufgetreten. Mögliche Ursachen: • Das Update-Modul von Plug-in Manager konnte ein Plug-in-Programm nicht herunterladen. Überprüfen Sie die Netzwerkverbindung, und versuchen Sie es erneut. • Das Update-Modul von Plug-in Manager kann das Plug-in-Programm nicht installieren, weil der AU Patch-Agent einen Fehler zurückgegeben hat. Der AU Patch-Agent ist das Programm, das die Installation neuer Plug-in-Programme startet. Die genaue Ursache des Fehlers finden Sie im Debug-Protokoll des ActiveUpdate Moduls in der Datei "`TmuDump.txt`" unter `\PCCSRV\Web\Service\AU_Data\AU_Log`. Führen Sie folgende Schritte durch: 1. Öffnen Sie den Registrierungseditor, und navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`. Setzen Sie den Wert auf 1.0.1000 zurück. 2. Löschen Sie den Registrierungsschlüssel des Plug-in-Programms unter `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_xxxx`. 3. Starten Sie den OfficeScan Plug-in Manager Dienst neu. 4. Laden Sie das Plug-in-Programm herunter, und installieren Sie es.
170	Es ist ein Systemfehler aufgetreten. Das Update-Modul von Plug-in Manager kann einen eingehenden Vorgang nicht bearbeiten, da es zurzeit einen anderen Vorgang bearbeitet. Führen Sie die Aufgabe zu einem späteren Zeitpunkt durch.
202	Im Plug-in Manager Programm ist ein Fehler aufgetreten. Das Plug-in Manager-Programm kann die auf der Webkonsole ausgeführte Aufgabe nicht bearbeiten. Aktualisieren Sie die Webkonsole, oder führen Sie ein Upgrade von Plug-in Manager durch, falls ein Programm-Upgrade zur Verfügung steht.

Fehlercode	Meldung, Ursache und Lösung
203	Im Plug-in Manager Programm ist ein Fehler aufgetreten. Bei der Kommunikation des Plug-in Manager Programms mit den Backend-Services ist ein IPC- (Intercommunication Process Communication) Fehler aufgetreten. Starten Sie den OfficeScan Plug-in Manager Dienst neu, und führen Sie den Task erneut aus.
Andere Fehlercodes	Es ist ein Systemfehler aufgetreten. Beim Download eines neuen Plug-in-Programms überprüft Plug-in Manager die Plug-in-Programmliste auf dem ActiveUpdate Server. Plug-in Manager konnte die Liste nicht anfordern. Führen Sie folgende Schritte durch: 1. Öffnen Sie den Registrierungseditor, und navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`. Setzen Sie den Wert auf `1.0.1000` zurück. 2. Starten Sie den OfficeScan Plug-in Manager Dienst neu. 3. Laden Sie das Plug-in-Programm herunter, und installieren Sie es.

Kapitel 18

Ressourcen zur Fehlerbehebung

In diesem Kapitel finden Sie eine Liste mit Ressourcen, die Sie zur Fehlerbehebung bei Problemen mit dem OfficeScan Server und dem OfficeScan Agent heranziehen können.

Es werden folgende Themen behandelt:

- *Support-Informationssystem auf Seite 18-2*
- *Case Diagnostic Tool auf Seite 18-2*
- *Trend Micro Performance Tuning Tool auf Seite 18-2*
- *OfficeScan Serverprotokolle auf Seite 18-3*
- *OfficeScan Agent Protokolle auf Seite 18-15*

Support-Informationssystem

Beim Support-Informationssystem handelt es sich um eine Seite, über die Sie ohne großen Aufwand Dateien an Trend Micro zur Analyse senden können. Dieses System ermittelt die GUID von OfficeScan Server und überträgt Informationen zusammen mit der gesendeten Datei. Über die OfficeScan Server-GUID wird sichergestellt, dass Trend Micro ein Feedback zu den zur Bewertung eingereichten Dateien abgeben kann.

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.

Führen Sie das Tool auf allen Plattformen aus, die von OfficeScan unterstützt werden. Das Tool und die zugehörige Dokumentation können Sie von Ihrem Support-Anbieter beziehen.

Trend Micro Performance Tuning Tool

Trend Micro stellt ein eigenständiges Performance Tuning Tool bereit, das die Anwendungen identifiziert, die Leistungsprobleme verursachen könnten. Das Trend Micro Performance Tuning Tool, das in der Trend Micro Knowledge Base erhältlich ist, sollte während der Pilotphase auf einem herkömmlichen Workstation-Image und/oder einigen wenigen Ziel-Workstations ausgeführt werden, um Leistungsprobleme beim realen Einsatz der Verhaltensüberwachung und Gerätesteuerung zu vermeiden.

Weitere Informationen finden Sie auf der Website http://esupport.trendmicro.com/solution/en-us/1056425.aspx.

OfficeScan Serverprotokolle

Neben den Protokollen, die über die Webkonsole verfügbar sind, können Sie zur Fehlerbehebung auch andere Protokolle, wie z. B. Debug-Protokolle, verwenden.

Warnung!

Debug-Protokolle können die Serverleistung beeinträchtigen und viel Speicherplatz in Anspruch nehmen. Aktivieren Sie Debug-Protokolle nur, wenn nötig, und deaktivieren Sie sie danach sofort wieder. Entfernen Sie die Protokolldatei, wenn Sie Speicherplatz sparen müssen.

Server-Debug-Protokolle unter Verwendung von LogServer.exe

Mit Hilfe von `LogServer.exe` können Sie Debug-Protokolle für Folgendes erfassen:

- Allgemeine Protokolle für den OfficeScan Server
- Trend Micro Vulnerability Scanner
- Protokolle der Active Directory-Integration
- Agent -Gruppierungsprotokolle
- Protokolle zur Einhaltung der Sicherheitsrichtlinien
- Rollenbasierte Administration
- Intelligente Suche

Debug-Protokollierung aktivieren

Prozedur

1. Melden Sie sich an der Webkonsole an.
2. Klicken Sie auf dem Banner der Webkonsole auf das erste "O" in "OfficeScan".

3. Wählen Sie **Fehlerprotokoll aktivieren** aus.
4. Geben Sie die Debug-Protokolleinstellungen an.
5. Klicken Sie auf **Speichern**.
6. Überprüfen Sie die Protokolldatei (`ofcdebug.log`) am Standardspeicherort: <*Installationsordner des Servers*>`\PCCSRV\Log`.

Debug-Protokollierung deaktivieren

Prozedur

1. Melden Sie sich an der Webkonsole an.
2. Klicken Sie auf dem Banner der Webkonsole auf das erste "O" in "OfficeScan".
3. Deaktivieren Sie **Fehlerprotokoll aktivieren**.
4. Klicken Sie auf **Speichern**.

Debug-Protokollierung für die Installation und das Upgrade des Servers aktivieren

Sie können die Debug-Protokollierung aktivieren, bevor Sie folgende Aufgaben ausführen:

- Den Server deinstallieren und dann erneut installieren.
- OfficeScan 8.0 auf eine neue Version upgraden.
- Remote-Installation/-Upgrade durchführen (die Debug-Protokollierung ist auf dem Endpunkt aktiviert, auf dem das Setup ausgeführt wird, und nicht auf dem Remote-Endpunkt).

Prozedur

1. Kopieren Sie den Ordner `LogServer` im Ordner <*Installationsordner des Servers*>`\PCCSRV\Private` nach `C:\`.

2. Erstellen Sie eine Datei mit dem Namen `cdebug.ini` und dem folgenden Inhalt:

   ```
   [debug]

   debuglevel=9

   debuglog=c:\LogServer\ofcdebug.log

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1
   ```

3. Speichern Sie `ofcdebug.ini` unter `C:\LogServer`.

4. Führen Sie die entsprechende Aufgabe durch (d. h. den Server deinstallieren und installieren, auf eine neue Version upgraden oder eine Remote-Installation/ein Remote-Upgrade durchführen).

5. Überprüfen Sie `ofcdebug.log` unter `C:\LogServer`.

Installationsprotokolle

- Lokale Installations-/Upgrade-Protokolle

  Dateiname: `OFCMAS.LOG`

  Speicherort: `%windir%`

- Remote-Installations-/Upgrade-Protokolle

  - Auf dem Endpunkt, auf dem Sie Setup gestartet haben:

    Dateiname: `ofcmasr.log`

    Speicherort: `%windir%`

  - Auf dem Ziel-Endpunkt:

    Dateiname: `OFCMAS.LOG`

Speicherort: `%windir%`

Active Directory Protokolle

- Dateiname: `ofcdebug.log`
- Dateiname: `ofcserver.ini`

  Speicherort: <*Installationsordner des Servers*>`\PCCSRV\Private\`
- Dateinamen:
  - `dbADScope.cdx`
  - `dbADScope.dbf`
  - `dbADPredefinedScope.cdx`
  - `dbADPredefinedScope.dbf`
  - `dbCredential.cdx`
  - `dbCredential.dbf`

  Speicherort: `<Installationsordner des Servers>\PCCSRV\HTTPDB\`

Protokolle zur rollenbasierten Administration

Gehen Sie wie folgt vor, um detaillierte Informationen zur rollenbasierten Administration zu erhalten:

- Rufen Sie das Trend Micro Case Diagnostics Tool auf. Weitere Informationen finden Sie unter *Case Diagnostic Tool auf Seite 18-2*.
- Sammeln Sie die folgenden Protokolle:
  - Alle Dateien im Ordner <*Installationsordner des Servers*>`\PCCSRV\Private\AuthorStore`.
  - *OfficeScan Serverprotokolle auf Seite 18-3*

OfficeScan Agent -Gruppierungsprotokolle

- Dateiname: `ofcdebug.log`
- Dateiname: `ofcserver.ini`

  Speicherort: <*Installationsordner des Servers*>`\PCCSRV\Private\`
- Dateiname: `SortingRule.xml`

  Speicherort: `<Installationsordner des Servers>\PCCSRV\Private\SortingRuleStore\`
- Dateinamen:
  - `dbADScope.cdx`
  - `dbADScope.dbf`

  Speicherort: `<Installationsordner des Servers>\HTTPDB\`

Komponenten-Update-Protokolle

Dateiname: `TmuDump.txt`

Speicherort: <*Installationsordner des Servers*>`\PCCSRV\Web\Service\AU_Data\AU_Log`

Detaillierte Server-Update-Informationen abrufen

Prozedur

1. Erstellen Sie eine Datei mit dem Namen `aucfg.ini` und dem folgenden Inhalt:

   ```
   [Debug]

   level=-1

   [Downloader]

   ProxyCache=0
   ```

2. Speichern Sie die Datei unter <*Installationsordner des Servers*>\PCCSRV\Web\Service.

3. Starten Sie den OfficeScan Master Service neu.

Sammeln detaillierter Server-Update-Informationen beenden

Prozedur

1. Löschen Sie die Datei `aucfg.ini`.

2. Starten Sie den OfficeScan Master Service neu.

Agent Packager-Protokolle

Protokollierung bei der Erstellung von Agent Packager Paketen aktivieren

Prozedur

1. Ändern Sie `ClnExtor.ini` in <*Installationsordner des Servers*>\PCCSRV\Admin\Utility\ClientPackager wie folgt:

```
[Common]

DebugMode=1
```

2. Überprüfen Sie die Datei `ClnPack.log` auf `C:\`.

Protokollierung bei der Erstellung von Agent Packager Paketen deaktivieren

Prozedur

1. Öffnen Sie `ClnExtor.ini`.
2. Ändern Sie den Wert für "DebugMode" von 1 nach 0.

Protokolle zum Bericht zur Einhaltung der Sicherheitsrichtlinien

Sammeln Sie die folgenden Informationen, um ausführliche Informationen über die Einhaltung der Sicherheitsrichtlinien zu erhalten:

- Dateiname: `RBAUserProfile.ini`

  Speicherort: <*Installationsordner des Servers*>`\PCCSRV\Private\AuthorStore\`

- Alle Dateien im Ordner `<Installationsordner des Servers>\PCCSRV\Log\Bericht zur Einhaltung der Sicherheitsrichtlinien`.
- *OfficeScan Serverprotokolle auf Seite 18-3*

Protokolle zur ausgelagerten Serververwaltung

- Dateiname: `ofcdebug.log`
- Dateiname: `ofcserver.ini`

  Speicherort: <*Installationsordner des Servers*>`\PCCSRV\Private\`

- Alle Dateien im Ordner `<Installationsordner des Servers>\PCCSRV\Log\Outside Server Management Report\`.
- Dateinamen:

- `dbADScope.cdx`
- `dbADScope.dbf`
- `dbClientInfo.cdx`
- `dbclientInfo.dbf`

Speicherort: `<Installationsordner des Servers>\HTTPDB\`

Protokolle zu den Ausnahmen der Gerätesteuerung

Sammeln Sie die folgenden Informationen, um ausführliche Informationen über die Ausnahmen der Gerätesteuerung zu erhalten:

- Dateiname: `ofcscan.ini`

  Speicherort: <*Installationsordner des Servers*>\

- Dateiname: `dbClientExtra.dbf`

  Speicherort: `<Installationsordner des Servers>\HTTPDB\`

- Ausschlussliste der Gerätesteuerung von der OfficeScan Webkonsole.

Web-Reputation-Protokolle des integrierten Smart Protection Servers

Dateiname: `diagnostic.log`

Speicherort: <*Installationsordner des Servers*>`\PCCSRV\LWCS\`

Protokolle zum ServerProtect Normal Server Migration Tool

Debug-Protokollierung für das ServerProtect Normal Server Migration Tool aktivieren:

Prozedur

1. Erstellen Sie eine Datei mit dem Namen `ofcdebug.ini` und dem folgenden Inhalt:

   ```
   [Debug]

   DebugLog=C:\ofcdebug.log

   DebugLevel=9
   ```

2. Speichern Sie die Datei auf dem Laufwerk `C:\`.

3. Überprüfen Sie `ofcdebug.log` unter `C:\`.

Hinweis

Löschen Sie die Datei `ofcdebug.ini`, um die Debug-Protokollierung zu deaktivieren.

VSEncrypt-Protokolle

OfficeScan erstellt das Debug-Protokoll (`VSEncrypt.log`) automatisch im temporären Ordner des Benutzerkontos. Dies ist beispielsweise `C:\Dokumente und Einstellungen\<Benutzername>\Lokale Einstellungen\Temp`.

Protokolle zum Control Manager MCP Agent

Debug-Dateien im Ordner <*Installationsordner des Servers*>`\PCCSRV\CMAgent`

- `Agent.ini`
- `Product.ini`
- Ein Screenshot der Seite mit den Control Manager Einstellungen
- `ProductUI.zip`

Debug-Protokollierung für den MCP Agent aktivieren

Prozedur

1. Ändern Sie die Datei `product.ini` im Ordner <*Installationsordner des Servers*>`\PCCSRV\CmAgent` wie folgt:

   ```
   [Debug]

   debugmode = 3

   debuglevel= 3

   debugtype = 0

   debugsize = 10000

   debuglog = C:\CMAgent_debug.log
   ```

2. Starten Sie den OfficeScan Control Manager Agent Dienst über die Microsoft Management-Konsole.

3. Überprüfen Sie die Datei `CMAgent_debug.log` unter `C:\`.

Debug-Protokollierung für den MCP Agent deaktivieren

Prozedur

1. Öffnen Sie die Datei `product.ini`, und löschen Sie die folgenden Einträge:

   ```
   debugmode = 3

   debuglevel= 3

   debugtype = 0

   debugsize = 10000

   debuglog = C:\CMAgent_debug.log
   ```

2. Starten Sie den OfficeScan Control Manager Dienst neu.

Viren-/Malware-Protokolle

Dateiname:

- `dbVirusLog.dbf`
- `dbVirusLog.cdx`

Speicherort: <*Installationsordner des Servers*>`\PCCSRV\HTTPDB\`

Spyware-/Grayware-Protokolle

Dateiname:

- `dbSpywareLog.dbf`
- `dbSpywareLog.cdx`

Speicherort: <*Installationsordner des Servers*>`\PCCSRV\HTTPDB\`

Ausbruchsprotokolle

PROTOKOLLTYP	DATEI
Protokolle zu aktuellen Firewall-Verstoß-Ausbrüchen	Dateiname: `Cfw_Outbreak_Current.log` Speicherort: <*Installationsordner des Servers*>`\PCCSRV\Log\`
Protokolle zu den letzten Firewall-Verstoß-Ausbrüchen	Dateiname: `Cfw_Outbreak_Last.log` Speicherort: <*Installationsordner des Servers*>`\PCCSRV\Log\`

PROTOKOLLTYP	DATEI
Protokolle zu aktuellen Viren-/Malware-Ausbrüchen	Dateiname: `Outbreak_Current.log` Speicherort: <*Installationsordner des Servers*>`\PCCSRV\Log\`
Protokolle zu den letzten Viren-/Malware-Ausbrüchen	Dateiname: `Outbreak_Last.log` Speicherort: <*Installationsordner des Servers*>`\PCCSRV\Log\`
Protokolle zu aktuellen Spyware-/Grayware-Ausbrüchen	Dateiname: `Spyware_Outbreak_Current.log` Speicherort: <*Installationsordner des Servers*>`\PCCSRV\Log\`
Protokolle zu den letzten Spyware-/Grayware-Ausbrüchen	Dateiname: `Spyware_Outbreak_Last.log` Speicherort: <*Installationsordner des Servers*>`\PCCSRV\Log\`

Protokolle zur Unterstützung von Virtual Desktop

- Dateiname: `vdi_list.ini`

  Speicherort: <*Installationsordner des Servers*>`\PCCSRV\TEMP\`

- Dateiname: `vdi.ini`

  Speicherort: `<Installationsordner des Servers>\PCCSRV\Private\`

- Dateiname: `ofcdebug.txt`

  Speicherort: `<Installationsordner des Servers>\PCCSRV\`

Um die Datei `ofcdebug.txt` zu erstellen, aktivieren Sie die Debug-Protokollierung. Hinweise zur Aktivierung der Debug-Protokollierung finden Sie unter *Debug-Protokollierung aktivieren auf Seite 18-3*.

OfficeScan Agent Protokolle

Verwenden Sie OfficeScan Agent-Protokolle (wie z. B. Debug-Protokolle), um Probleme mit dem OfficeScan Agent zu beheben.

Warnung!

Debug-Protokolle können die agent-Leistung beeinträchtigen und viel Speicherplatz in Anspruch nehmen. Aktivieren Sie Debug-Protokolle nur, wenn nötig, und deaktivieren Sie sie danach sofort wieder. Löschen Sie die Protokolldatei, wenn sie zu groß wird.

OfficeScan Agent Debug-Protokolle unter Verwendung von LogServer.exe

Debug-Protokollierung für den OfficeScan Agent deaktivieren:

Prozedur

1. Erstellen Sie eine Datei mit dem Namen `ofcdebug.ini` und dem folgenden Inhalt:

```
[Debug]

Debuglog=C:\ofcdebug.log

debuglevel=9

debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

2. Senden Sie die Datei `ofcdebug.ini` an die Benutzer, und weisen Sie sie an, die Datei auf dem Laufwerk `C:\` zu speichern.

Hinweis

`LogServer.exe` wird automatisch beim Systemstart des OfficeScan Agent-Endpunkts ausgeführt. Weisen Sie die Benutzer an, das Befehlsfenster von LogServer.exe, das beim Systemstart des Endpunkts geöffnet wird, NICHT zu schließen, da OfficeScan in diesem Fall die Debug-Protokollierung beenden würde. Schließt der Benutzer das Befehlsfenster, kann die Debug-Protokollierung erneut gestartet werden, indem der Prozess `LogServer.exe` im Ordner <*Installationsordner des Agents*> ausgeführt wird.

3. Prüfen Sie auf jedem OfficeScan Agent-Endpunkt die Datei ofcdebug.log auf Laufwerk C:\.

Hinweis

Deaktivieren Sie die Debug-Protokollierung für den OfficeScan Agent, indem Sie `ofcdebug.ini` löschen.

Erstinstallations-Protokolle

Für MSI-Paketinstallationen:

- Dateiname: `OFCNT.LOG`
- Speicherort: <*Installationsordner des Agents*>

Für Web-Installationen:

- Dateiname: `WebInstall.log`
- Speicherort: `C:\`

Für Remote-Installationen:

- Dateiname: `OFCNT.LOG`
- Speicherort: `C:\`

Für Autopcc- und EXE-Paketinstallationen:

- Dateiname: `OFCNT.LOG`

- Speicherort: <*Installationsordner des Agents*>`%windir%\`

Upgrade-/Hotfix-Protokolle

Dateiname: `upgrade_yyyymmddhhmmss.log`

Speicherort: <*Installationsordner des Agents*>`\Temp`

Protokolle für Damage Cleanup Services

Debug-Protokollierung der Damage Cleanup Services aktivieren

Prozedur

1. Öffnen Sie die Datei `TSC.ini` im Ordner <*Installationsordner des Agents*>.
2. Ändern Sie die folgende Zeile:

   ```
   DebugInfoLevel=5
   ```

3. Überprüfen Sie die Datei `TSCDebug.log` im Ordner `Installationsordner des Agents>\debug`.

Debug-Protokollierung der Damage Cleanup Services deaktivieren

Öffnen Sie die Datei `TSC.ini`, und ändern Sie den Wert für "`DebugInfoLevel`" von 5 in 0.

Säuberungsprotokoll

Dateiname: `jjjjmmtt.log`

Speicherort: <*Installationsordner des Agents*>`\report\`

Mail Scan Protokolle

Dateiname: `SmolDbg.txt`

Speicherort: <*Installationsordner des Agents*>

OfficeScan Agent -Verbindungsprotokolle

Dateiname: `Conn_JJJJMMTT.log`

Speicherort: <*Installationsordner des Agents*>`\ConnLog`

OfficeScan Agent -Update-Protokolle

Dateiname: `Tmudump.txt`

Speicherort: <*Installationsordner des Agents*>`\AU_Data\AU_Log`

Detaillierte OfficeScan Agent-Update-Informationen abrufen

Prozedur

1. Erstellen Sie eine Datei mit dem Namen `aucfg.ini` und dem folgenden Inhalt:

   ```
   [Debug]

   level=-1

   [Downloader]

   ProxyCache=0
   ```

2. Speichern Sie die Datei unter <*Installationsordner des Agents*>.

3. Laden Sie den OfficeScan Agent neu.

Hinweis

Beenden Sie das Sammeln detaillierter agent-Update-Informationen, indem Sie die Datei `aucfg.ini` löschen und den OfficeScan Agent neu laden.

Protokolle zur Viren-Scan-Engine

Debug-Protokollierung der Viren-Scan-Engine aktivieren:

Prozedur

1. Öffnen Sie den Windows Registrierungseditor (`regedit.exe`).
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters`.
3. Ändern Sie den Wert von "`DebugLogFlags`" in "`00003eff`".
4. Führen Sie die Schritte, die zum Problem mit der Suche geführt haben, aus.
5. Überprüfen Sie die Datei `TMFilter.log` in `%windir%`.

Hinweis

Deaktivieren Sie die Debug-Protokollierung, indem Sie den Wert von "`DebugLogFlags`" auf "`00000000`" zurücksetzen.

Ausbruchspräventions-Protokolle

Dateiname: `OPPLogs.log`

Speicherort: <*Installationsordner des Agents*>`\OppLog`

Protokolle zur Wiederherstellung im Zusammenhang mit Ausbruchsprävention

Dateinamen:

- `TmOPP.ini`
- `TmOPPRestore.ini`

Speicherort: <*Installationsordner des Agents*>\

Debug-Protokolle für die Verhaltensüberwachung

So aktivieren Sie die Debug-Protokollierung für die Verhaltensüberwachung:

Prozedur

1. Öffnen Sie den Windows Registrierungseditor (`regedit.exe`).
2. Gehen Sie zu `HKLM\SOFTWARE\TrendMicro\Aegis`.
3. Ändern Sie den Wert von "`DebugLogFlags`" in "`dword:00000032`".
4. Führen Sie die Schritte durch, die das Problem ausgelöst haben.
5. Überprüfen Sie die folgenden Protokolle im Ordner `C:\Programme (x86)\Trend Micro\BM\log\`.
   - `TmCommengyyyymmdd_nn.log`
   - `TMPEMyyyymmdd_nn.log`

OfficeScan Firewall-Protokolle

Debug-Protokollierung für den allgemeinen Firewall-Treiber auf Computern unter Windows Server 2008/7/ Server 2012/8/8.1/10/Server 2016 aktivieren

Prozedur

1. Bearbeiten Sie die folgenden Registrierungsschlüsselwerte:

REGISTRIERUNGSSCHLÜSSEL	WERTE
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmwfp\Parameters	Typ: DWORD Wert (REG_DWORD) Name: DebugCtrl Wert: 0x00001111
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmlwf\Parameters	Typ: DWORD value (REG_DWORD) Name: DebugCtrl Wert: 0x00001111

2. Starten Sie den Endpunkt neu.
3. überprüfen Sie die Dateien `wfp_log.txt` und `lwf_log.txt` auf Laufwerk `C:\`.

Debug-Protokollierung für den Treiber für die allgemeine Firewall auf Computern mit Windows XP und Windows Server 2003 aktivieren

Prozedur

1. Fügen Sie die folgenden Daten unter `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmcfw\Parameters` hinzu:
   - Typ: `DWORD value (REG_DWORD)`
   - Name: `DebugCtrl`
   - Wert: `0x00001111`
2. Starten Sie den Endpunkt neu.
3. Überprüfen Sie `cfw_log.txt` auf Laufwerk `C:\`.

Debug-Protokollierung für den Treiber für die allgemeine Firewall (alle Betriebssysteme) deaktivieren

Prozedur

1. Löschen Sie den Eintrag "`DebugCtrl`" aus dem Registrierungsschlüssel.
2. Starten Sie den Endpunkt neu.

Debug-Protokollierung für den OfficeScan NT Firewall-Dienst aktivieren

Prozedur

1. Bearbeiten Sie `TmPfw.ini` im Ordner <*Installationsordner des Agents*> wie folgt:

   ```
   [ServiceSession]

   Enable=1
   ```

2. Laden Sie den agent neu.
3. Überprüfen Sie die Datei `ddmmyyyy_NSC_TmPfw.log` unter `C:\temp`.

Debug-Protokollierung für den OfficeScan NT Firewall-Dienst deaktivieren

Prozedur

1. Öffnen Sie die Datei `TmPfw.ini`, und ändern Sie den Wert "`Enable`" von 1 in 0.
2. Laden Sie den OfficeScan Agent neu.

Web-Reputation- und POP3 Mail Scan Protokolle

Debug-Protokollierung des Web-Reputation-Moduls und POP3 Mail Scan aktivieren

Prozedur

- Für Agents unter Windows Server 2008:

  a. Bearbeiten Sie die Datei `TmProxy.ini` im Ordner <*Installationsordner des Agents*> wie folgt:

  ```
  [InteractiveSession]

  Enable=1

  LogFolder=C:\temp

  [ServiceSession]

  Enable=1

  LogFolder=C:\temp
  ```

  b. Laden Sie den OfficeScan Agent neu.

  c. überprüfen Sie die Datei `ddmmyyyy_NSC_TmProxy.log` unter `C:\temp`.

- Für Agents, die unter anderen Windows-Versionen ausgeführt werden:

  a. Bearbeiten Sie die Datei `TmOsprey.ini` im Ordner <*Installationsordner des Agents*> wie folgt:

  ```
  [InteractiveSession]

  Enable=1

  LogFolder=C:\temp

  [ServiceSession]

  Enable=1
  ```

```
LogFolder=C:\temp
```

b. Laden Sie den OfficeScan Agent neu.

c. überprüfen Sie die Datei `ddmmyyyy_NSC_TmProxy.log` unter `C:\temp`.

Debug-Protokollierung des Web-Reputation-Moduls und POP3 Mail Scan deaktivieren

Prozedur

- Für Agents unter Windows Server 2008:

  a. Bearbeiten Sie die Datei `TmProxy.ini` im Ordner <*Installationsordner des Agents*> wie folgt:

  ```
  [InteractiveSession]

  Enable=0

  LogFolder=C:\temp

  [ServiceSession]

  Enable=0

  LogFolder=C:\temp
  ```

  b. Laden Sie den OfficeScan Agent neu.

- Für Agents, die unter anderen Windows-Versionen ausgeführt werden:

  a. Bearbeiten Sie die Datei `TmOsprey.ini` im Ordner <*Installationsordner des Agents*> wie folgt:

  ```
  [InteractiveSession]

  Enable=0

  LogFolder=C:\temp

  [ServiceSession]
  ```

```
Enable=0

LogFolder=C:\temp
```

b. Laden Sie den OfficeScan Agent neu.

Protokolle für die Ausschlussliste der Gerätesteuerung

Dateiname: `DAC_ELIST`

Speicherort: <*Installationsordner des Agents*>\

Datenschutz-Debug-Protokolle

Datenschutz-Debug-Protokolle aktivieren:

Prozedur

1. Beziehen Sie die Datei `logger.cfg` von Ihrem Support-Anbieter.
2. Fügen Sie die folgenden Daten zu `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite` hinzu:
   - Typ: `String`
   - Name: `debugcfg`
   - Wert: `C:\Log\logger.cfg`
3. Erstellen Sie einen Ordner mit dem Namen „Protokoll“ im Verzeichnis `C:\`.
4. Kopieren Sie `logger.cfg` in den Ordner `Protokoll`.
5. Verteilen Sie die Einstellungen für die Funktion "Prävention vor Datenverlust" und die Gerätesteuerung über die Webkonsole, um mit dem Sammeln der Protokolle zu beginnen.

Hinweis

Deaktivieren Sie die Debug-Protokollierung für das Datenschutzmodul, indem Sie `debugcfg` im Registrierungsschlüssel löschen und den Endpunkt neu starten.

Windows Ereignisprotokolle

In der Windows Ereignisanzeige werden erfolgreiche Anwendungsereignisse aufgezeichnet, wie beispielsweise Anmeldungen oder Änderungen an den Kontoeinstellungen.

Prozedur

1. Wählen Sie eine der folgenden Optionen:
   - Klicken Sie auf **Starten** > **Systemsteuerung** > **Leistung und Wartung** > **Administrator-Tools** > **Computerverwaltung**.
   - Öffnen Sie die MMC mit dem Snap-in für die Ereignisanzeige.
2. Klicken Sie auf **Ereignisanzeige**.

TDI-Debug-Protokolle (Transport Driver Interface)

TDI-Debug-Protokolle (Transport Driver Interface) aktivieren:

Prozedur

1. Fügen Sie die folgenden Daten zu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\Parameters` hinzu:

PARAMETER	WERTE
Schlüssel 1	Typ: `DWORD` value `(REG_DWORD)` Name: `Fehlerbehebung` Wert: `1111 (hexadezimal)`

PARAMETER	WERTE
Schlüssel 2	Typ: `String-Wert (REG_SZ)` Name: `LogFile` Wert: `C:\tmtdi.log`

2. Starten Sie den Endpunkt neu.
3. Überprüfen Sie die Datei `tmtdi.log` auf Laufwerk `C:\`.

Hinweis

Deaktivieren Sie die Debug-Protokollierung für TDI, indem Sie `Debug` und `LogFile` im Registrierungsschlüssel löschen und den Endpunkt neu starten.

Kapitel 19

Technischer Support

Erfahren Sie mehr über die folgenden Themen:

- *Ressourcen zur Fehlerbehebung auf Seite 19-2*
- *Kontaktaufnahme mit Trend Micro auf Seite 19-3*
- *Verdächtige Inhalte an Trend Micro senden auf Seite 19-4*
- *Sonstige Ressourcen auf Seite 19-6*

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 http://esupport.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:

   http://esupport.trendmicro.com/srf/srfmain.aspx

   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 http://about-threats.trendmicro.com/de/threatencyclopedia#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 unsere Trend Micro Vetriebspartner telefonisch oder per E-Mail:

Adresse	Trend Micro Deutschland GmbH Zeppelinstraße 1 85399 Hallbergmoos Deutschland
Telefon	+49 (0) 811 88990-700
Website	http://www.trendmicro.de
E-Mail-Adresse	sales_info@trendmicro.de

- Weltweite Support-Büros:

  http://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:

  http://docs.trendmicro.com/de-de/home.aspx

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.

E-Mail-Reputation-Dienste

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://ers.trendmicro.com/

Informationen zum Senden von Nachrichten an Trend Micro finden Sie im folgenden Knowledge Base-Artikel:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

File-Reputation-Dienste

Sammeln Sie Systeminformationen, und senden Sie verdächtige Dateiinhalte an Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

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:

http://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:

http://downloadcenter.trendmicro.com/index.php?regs=de

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:

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

Anhänge

Anhänge

Anhang A

IPv6-Unterstützung in OfficeScan

Benutzer, die die Verteilung von OfficeScan 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 OfficeScan.

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 OfficeScan Server und Agents

Die IPv6-Unterstützung für OfficeScan beginnt in Version 10.6. Frühere OfficeScan Versionen unterstützen keine IPv6-Adressierung. Die IPv6-Unterstützung wird nach der Installation bzw. dem Upgrade der IPv6-kompatiblen OfficeScan Server und OfficeScan Agents automatisch aktiviert.

Voraussetzungen für OfficeScan Server

Für den OfficeScan Server gelten folgende IPv6-Voraussetzungen:

- Der Server muss unter Windows Server 2008, Windows Server 2012 oder Windows Server 2016 installiert werden.
- Der Server muss einen IIS Webserver verwenden.
- Wenn der Server IPv4- und IPv6-OfficeScan Agents verwaltet, muss er eine IPv4- wie auch eine IPv6-Adresse haben und über seinen Host-Namen identifiziert werden. Wenn der Server über seine IPv4-Adresse identifiziert wird, können IPv6-OfficeScan Agents keine Verbindung zum Server herstellen. Dasselbe Problem tritt auf, wenn reine IPv4-Agents 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.

Hinweis

Der FQDN kann nur bei einer lokalen Installation des Servers angegeben werden. Dies wird nicht auf Remote-Installationen unterstützt.

OfficeScan Agent Voraussetzungen

Der OfficeScan Agent muss unter einem der folgenden Betriebssysteme installiert sein:

- Windows 7
- Windows Server 2008
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows 10
- Windows Server 2016

Der OfficeScan 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 von Einschränkungen von OfficeScan Servern, die nur über eine IPv6-Adresse verfügen.

TABELLE A-1. Einschränkungen bei reinen IPv6-Servern

VORGANG	EINSCHRÄNKUNG
Agent - Verwaltung	Ein reiner IPv6-Server kann nicht: • OfficeScan Agents auf reine IPv4-Endpunkte verteilen. • Reine IPv4-OfficeScan Agents verwalten.
Updates und zentrale Verwaltung	Ein reiner IPv6-Server kann sich nicht über reine IPv4-Update-Adressen aktualisieren, wie etwa: • Trend Micro ActiveUpdate Server • Jede reine, benutzerdefinierte IPv4-Update-Adresse

VORGANG	EINSCHRÄNKUNG
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.
Plug-in-Lösungen	Ein reiner IPv6-Server verfügt über Plug-in Manager, kann aber keine Plug-in-Lösung verteilen an: • Reine IPv4-OfficeScan Agents oder reine IPv4-Hosts (da keine direkte Verbindung besteht) • Reine IPv6-OfficeScan 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 OfficeScan Server und den Elementen, zu denen er sich verbindet, oder den Elementen, die er bedient.

Einschränkungen bei reinen IPv6-OfficeScan Agents

Die folgende Tabelle enthält eine Liste von Einschränkungen, wenn der OfficeScan Agent nur über eine IPv6-Adresse verfügt.

TABELLE A-2. Einschränkungen bei reinen IPv6-OfficeScan Agents

ELEMENT	EINSCHRÄNKUNG
Übergeordneter OfficeScan-Server	Reine IPv6-OfficeScan Agents können nicht über einen reinen IPv4-OfficeScan verwaltet werden.

ELEMENT	EINSCHRÄNKUNG
Updates	Ein reiner IPv6-OfficeScan Agent kann sich nicht über reine IPv4-Update-Quellen aktualisieren, wie etwa: • Trend Micro ActiveUpdate Server • Ein reiner IPv4-OfficeScan Server • Ein reiner IPv4-Update-Agent • Jede reine, benutzerdefinierte IPv4-Update-Quelle
Suchabfragen, Web-Reputation-Abfragen und Smart Feedback	Ein reiner IPv6-OfficeScan Agent kann keine Abfragen an Smart-Protection-Quellen senden, wie etwa: • Smart Protection Server 2.0 (integriert oder standalone) **Hinweis** IPv6-Unterstützung für Smart Protection Server ist ab Version 2.5 verfügbar. • Trend Micro Smart Protection Network (auch für Smart Feedback)
Software-Sicherheit	Reine IPv6-OfficeScan Agents können sich nicht mit dem von Trend Micro gehosteten Certified Safe Software Service verbinden.
Plug-in-Lösungen	Reine IPv6-OfficeScan Agents können keine Plug-in-Lösungen installieren, weil keine dieser Lösungen IPv6 unterstützt.
Proxy-Verbindung	Ein reiner IPv6-OfficeScan 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 OfficeScan 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.

- OfficeScan 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
  ```

- OfficeScan 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 OfficeScan diese Adresse akzeptieren kann. Zum Beispiel können OfficeScan 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 OfficeScan Agents verteilt, aber von OfficeScan 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-OfficeScan 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.

SPEICHERORT	BESCHREIBUNG
Agent-Hierarchie	Bei jedem Anzeigen der Agent-Hierarchie werden die IPv6-Adressen der reinen IPv6-OfficeScan Agents in der Spalte **IP-Adresse** angezeigt. Bei Dual-Stack-OfficeScan Agents werden die IPv6-Adressen angezeigt, wenn sie sich mit ihrer IPv6-Adresse am Server registriert haben. **Hinweis** Die IP-Adresse, die Dual-Stack-OfficeScan Agents zur Registrierung beim Server verwenden, kann über **Agents** > **Globale Agent-Einstellungen > Netzwerk** > **Bevorzugte IP-Adresse** gesteuert werden. Wenn Sie die Einstellungen der Agent-Hierarchie in eine Datei exportieren, erscheinen die IPv6-Adressen auch in der exportierten Datei.
Agent-Status	Ausführliche Informationen zu den Agents erhalten Sie unter **Agents** > **Agent-Verwaltung > Status**. In diesem Fenster sehen Sie die IPv6-Adressen reiner IPv6-OfficeScan Agents sowie von Dual-Stack-OfficeScan Agents, die sich mit ihrer IPv6-Adresse am Server registriert haben.

SPEICHERORT	BESCHREIBUNG
Protokolle	Die IPv6-Adressen von Dual-Stack- und reinen IPv6-OfficeScan Agents finden sich in den folgenden Protokollen: • Viren-/Malware-Protokolle • Spyware-/Grayware-Protokolle • Firewall-Protokolle • Verbindungsüberprüfungsprotokolle
Control Manager Konsole	Im Folgenden wird aufgeführt, welche der IP-Adressen des OfficeScan Servers und der OfficeScan Agents auf der Control Manager-Konsole angezeigt werden. • Dual-Stack-Server: IPv4 und IPv6 • Reiner IPv4-Server: IPv4 • Reiner IPv6-Server: IPv6 • Dual-stack OfficeScan Agent: Die IP-Adresse, mit der sich der OfficeScan Agent am OfficeScan Server registriert hat • Reines IPv4 OfficeScan Agent: IPv4 • Reines IPv6 OfficeScan Agent: IPv6

Anhang B

Unterstützung für Windows Server Core

Dieser Anhang behandelt den OfficeScan-Support für Windows Server Core.

Unterstützung für Windows Server Core

Windows Server Core ist eine Minimalinstallation einer Windows Server-Version. In einem Server Core:

- Viele der Optionen und Funktionen von Windows Server stehen nicht zur Verfügung.
- Auf dem Server läuft ein viel schlankerer Betriebssystemkern.
- Die meisten Aufgaben werden über die Eingabeaufforderung ausgeführt.
- Auf dem Betriebssystem werden weniger Dienste ausgeführt und zum Starten sind weniger Ressourcen erforderlich.

OfficeScan unterstützt OfficeScan Agent-Installationen in den folgenden Versionen von Windows Server Core:

- Windows Server Core 2008
- Windows Server Core 2008 R2
- Windows Server Core 2012
- Windows Server Core 2012 R2
- Windows Server Core 2016

Der OfficeScan Agent unterstützt Server Core. Dieser Abschnitt enthält Informationen über den Support-Umfang für Server Core.

Der OfficeScan Server unterstützt Server Core nicht.

Installationsmethoden für Windows Server Core

Die folgenden Installationsmethoden werden nicht oder nur teilweise unterstützt:

- Web-Installationsseite:Diese Methode wird nicht unterstützt, da Server Core keine Webbrowser unterstützt.

- Trend Micro Vulnerability Scanner:Vulnerability Scanner kann nicht lokal auf dem Server Core ausgeführt werden. Führen Sie das Tool über den OfficeScan Server oder einen anderen Endpunkt aus.

Die folgenden Installationsmethoden werden unterstützt:

- Remote-Installation. Weitere Informationen finden Sie unter *Remote-Installation über die OfficeScan Webkonsole auf Seite 5-19*.
- Anmeldeskript-Setup
- Agent Packager

OfficeScan Agent mit dem Anmeldeskript-Setup installieren

Prozedur

1. Öffnen Sie auf dem Zielendpunkt eine Eingabeaufforderung.
2. Ordnen Sie den Speicherort der Datei `AutoPcc.exe` auf dem OfficeScan Server zu, indem Sie den folgenden Befehl eingeben:

   ```
   net use <zugeordneter Laufwerksbuchstabe> \\<Hostname und IP-Adresse des OfficeScan Servers>\ofcscan
   ```

   Beispiel:

   ```
   net use P: \\10.1.1.1\ofcscan
   ```

3. Geben Sie den Benutzernamen und das Kennwort für den Zielserver ein.

   Eine Meldung wird angezeigt, die Sie darüber informiert, ob der Speicherort von `AutoPcc.exe` erfolgreich zugeordnet wurde.

4. Ändern Sie den Speicherort von `AutoPcc.exe`, indem Sie den zugeordneten Laufwerksbuchstaben und einen Doppelpunkt eingeben. Beispiel:

   ```
   P:
   ```

5. Geben Sie zum Starten der Installation Folgendes ein:

`AutoPcc.exe`

Im folgenden Bild werden die Befehle und Ergebnisse in der Eingabeaufforderung angezeigt.

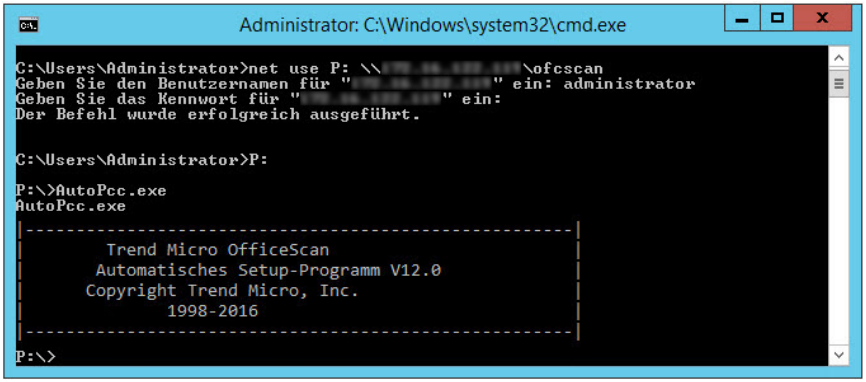


ABBILDUNG B-1. Eingabeaufforderung, die zeigt, wie der OfficeScan Agent mit Hilfe des Anmeldeskript-Setups installiert wird

Den OfficeScan Agent mit dem OfficeScan Agent-Paket installieren

Prozedur

1. Erstellen Sie das Paket.

   Weitere Informationen finden Sie unter *Installation mit Agent Packager auf Seite 5-25*.

2. Öffnen Sie ein Eingabeaufforderungsfenster.

3. Ordnen Sie den Speicherort des OfficeScan Agent-Pakets zu, indem Sie den folgenden Befehl eingeben:

   `net use <zugeordneter Laufwerksbuchstabe> \\<Speicherort des Agent-Pakets>`

   Beispiel:

```
net use P: \\10.1.1.1\Package
```

Eine Meldung wird angezeigt, die Sie darüber informiert, ob der Speicherort des OfficeScan Agent-Pakets erfolgreich zugeordnet wurde.

4. Ändern Sie den Speicherort des OfficeScan Agent-Pakets, indem Sie den zugeordneten Laufwerksbuchstaben und einen Doppelpunkt eingeben. Beispiel:

   ```
   P:
   ```

5. Kopieren Sie das OfficeScan Agent-Paket in ein lokales Verzeichnis auf dem Server Core-Endpunkt, indem Sie den folgenden Befehl eingeben:

   ```
   copy <Paketdateiname> <Verzeichnis auf dem Server Core-Endpunkt, in das Sie das Paket kopieren möchten>
   ```

   Beispiel:

   ```
   copy officescan.msi C:\Client0
   ```

   Eine Meldung wird angezeigt, die Sie darüber informiert, ob das OfficeScan Agent-Paket erfolgreich kopiert wurde.

6. Wechseln Sie zum lokalen Verzeichnis. Beispiel:

   ```
   C:
   ```

   ```
   cd C:\Client0
   ```

7. Geben Sie den Paketdateinamen ein, um die Installation zu starten. Beispiel:

   ```
   officescan.msi
   ```

Im folgenden Bild werden die Befehle und Ergebnisse in der Eingabeaufforderung angezeigt.

```
C:\Windows>net use P: \\172.16.8.73\package
Der Befehl wurde erfolgreich ausgeführt.

C:\Windows>P:

P:\>copy officescan.msi "C:\Client Package"
        1 Datei(en) kopiert.

P:\>C:

C:\Windows>cd "C:\Client Package"

C:\Client Package>officescan.msi
```

ABBILDUNG B-2. Eingabeaufforderung, die zeigt, wie der OfficeScan Agent mit Hilfe eines Agent-Pakets installiert wird

OfficeScan Agent-Funktionen unter Windows Server Core

Die meisten unter Windows Server 2008/2012/2016 verfügbaren OfficeScan Agent-Funktionen werden auch unter Server Core unterstützt. Der unabhängige Modus wird als einzige Funktion nicht unterstützt.

Eine Liste der unter Windows Server 2008/2012/2016 verfügbaren Funktionen finden Sie unter *OfficeScan Agent Funktionen auf Seite 5-3*.

Auf die OfficeScan Agent-Konsole kann nur über die Befehlszeilenschnittstelle zugegriffen werden.

Hinweis

In einigen Fenstern der OfficeScan Agent-Konsole befindet sich eine Hilfe-Schaltfläche, über die eine kontextsensitive HTML-Hilfe aufgerufen werden kann. Da Windows Server Core 2008/2012/2016 keinen Browser enthält, steht diese Hilfe dem Benutzer nicht zur Verfügung. Um die Hilfe anzuzeigen, muss der Benutzer einen Browser installieren.

Windows Server Core Befehle

Führen Sie OfficeScan Agent-Aufgaben durch, indem Sie Befehle über die Eingabeaufforderung ausführen.

Um die Befehle auszuführen, navigieren Sie zum Speicherort von `PccNTMon.exe`. Dieser Prozess ist verantwortlich für den Start der OfficeScan Agent-Konsole. Der Prozess befindet sich im <*Installationsordner des Agents*>.

Die folgende Tabelle enthält alle verfügbaren Befehle.

TABELLE B-1. Windows Server Core Befehle

BEFEHL	AKTION
`pccnt <Laufwerk oder Ordnerpfad>`	Durchsucht das angegebene Laufwerk oder den angegebenen Ordner nach Sicherheitsrisiken. Richtlinien: • Wenn der Ordnerpfad ein Leerzeichen enthält, setzen Sie den vollständigen Pfad in Anführungszeichen. • Das Durchsuchen einzelner Dateien wird nicht unterstützt. Korrekte Befehle: • `pccnt C:\` • `pccnt D:\Dateien` • `pccnt "C:\Dokumente und Einstellungen"` Falsche Befehle: • `pccnt C:\Dokumente und Einstellungen` • `pccnt D:\Dateien\Beispiel.doc`
`pccntmon -r`	Öffnet den Echtzeitmonitor
`pccntmon -v`	Führt die Agent-Komponenten und deren Versionen auf
`pccntmon -u`	Aktualisiert die OfficeScan Agent-Komponenten.
`pccntmon -n <unload_password>`	Entlädt den OfficeScan Agent. Geben Sie den folgenden Befehl ein, um den OfficeScan Agent erneut zu laden: `pccntmon`
`pccntmon -m <uninstall_password>`	Deinstalliert den OfficeScan Agent.

BEFEHL	AKTION

`pccntmon -c`	Zeigt die folgenden Informationen in der Befehlszeile:
	• Suchmethode
	  • Intelligente Suche
	  • Herkömmliche Suche
	• Pattern-Status
	  • Aktualisiert
	  • Nicht aktuell
	• Echtzeitsuchdienst
	  • Funktioniert
	  • Deaktiviert oder nicht funktionsfähig
	• Verbindungsstatus des Agents
	  • Online
	  • Unabhängig
	  • Offline
	• Web-Reputation-Dienste
	  • Verfügbar
	  • Die Verbindung wird wiederhergestellt
	• File-Reputation-Dienste
	  • Verfügbar
	  • Die Verbindung wird wiederhergestellt

`pccntmon -h`	Zeigt alle verfügbaren Befehle

Anhang C

Unterstützung für Windows 8/8.1/10 und Windows Server 2012/2016

In diesem Anhang wird die OfficeScan Unterstützung für Windows 8/8.1/10 und Windows Server 2012/2016 behandelt.

Informationen zu Windows 8/8.1/10 und Windows Server 2012/2016

Windows 8/8.1 und Windows Server 2012/2016 stellen Benutzern zwei verschiedene Betriebsmodi bereit: den Desktop-Modus und den Windows-Benutzeroberflächenmodus. Benutzer können Windows 10 entweder im Desktop-Modus oder im Tablet-Modus ausführen. Der Desktop-Modus gleicht dem klassischen Windows **Start**-Bildschirm.

Der Windows-Benutzeroberflächenmodus bietet Benutzern eine neue Benutzeroberfläche ähnlich derjenigen, die auf Windows-Handys verwendet wird. Neue Funktionen sind eine Touchscreen-Oberfläche zum Scrollen, Kacheln und Popupbenachrichtigungen.

TABELLE C-1. Kacheln und Popupbenachrichtigungen

STEUERELEMENT	BESCHREIBUNG
Kacheln	Kacheln ähneln den Desktopsymbolen in früheren Windows-Versionen. Benutzer klicken oder tippen auf eine Kachel, um die der Kachel zugeordnete Anwendung zu starten. Livekacheln stellen den Benutzern anwendungsspezifische Informationen bereit, die dynamisch aktualisiert werden. Anwendungen können Informationen auch dann an Kacheln senden, wenn die entsprechende Anwendung gerade nicht ausgeführt wird

STEUERELEMENT	BESCHREIBUNG
Popupbenachrichtigungen	Popupbenachrichtigungen gleichen anderen Popupmeldungen. Diese Benachrichtigungen stellen zeitkritischsten Informationen über Ereignisse bereit, die eintreten, während eine Anwendung ausgeführt wird. Popupbenachrichtigungen werden im Vordergrund angezeigt, ganz gleich of Windows sich gerade im Desktop-Modus befindet, ob der Sperrbildschirm angezeigt oder eine andere Anwendung ausgeführt wird. **Hinweis** Je nach Anwendung werden Popupbenachrichtigungen möglicherweise nicht auf allen Bildschirmen oder in jedem Modus angezeigt.

OfficeScan Unterstützung für Kacheln und Popupbenachrichtigungen

In der folgenden Tabelle wird beschrieben, wie OfficeScan Kacheln und Popupbenachrichtigungen im Windows-Benutzeroberflächenmodus unterstützt.

TABELLE C-2. OfficeScan Unterstützung für Kacheln und Popupbenachrichtigungen

STEUERELEMENT	OFFICESCAN UNTERSTÜTZUNG
Kacheln	OfficeScan stellt Benutzern eine Kachel bereit, die mit dem OfficeScan Agent-Programm verknüpft ist. Wenn Benutzer auf die Kachel klicken, wechselt Windows in den Desktop-Modus, und das OfficeScan Agent-Programm wird angezeigt. **Hinweis** OfficeScan unterstützt keine Livekacheln.

STEUERELEMENT	OFFICESCAN UNTERSTÜTZUNG
Popupbenachrichtigungen	OfficeScan sendet folgende Popupbenachrichtigungen: • Verdächtiges Programm erkannt • Zeitgesteuerte Suche • Bedrohung behoben • Neustart erforderlich • USB-Speichergerät entdeckt • Ausbruch entdeckt **Hinweis** OfficeScan zeigt Popupbenachrichtigungen nur im Windows-Benutzeroberflächenmodus an.

Aktivieren von Popupbenachrichtigungen in Windows 8/8.1 und Windows Server 2012 aktivieren

Benutzer können den Empfang von Popupbenachrichtigungen aktivieren, indem sie die **PC-Einstellungen** auf dem OfficeScan Agent-Endpunkt ändern. OfficeScan setzt voraus, dass Benutzer Popupbenachrichtigungen aktivieren.

Prozedur

1. Bewegen Sie den Mauszeiger in die untere rechte Ecke des Bildschirms um die **Charms**-Leiste anzuzeigen.
2. Klicken Sie auf **Einstellungen** > **PC-Einstellungen ändern**.

   Das Fenster **PC-Einstellungen** wird angezeigt.
3. Klicken Sie auf **Benachrichtigungen**.
4. Aktivieren Sie im Abschnitt **Benachrichtigungen** die folgenden Einstellungen:
   - **App-Benachrichtigungen anzeigen**

- **App-Benachrichtigungen auf dem Sperrbildschirm anzeigen** (optional)
- **Benachrichtigungstöne wiedergeben** (optional)

Aktivieren von Popupbenachrichtigungen in Windows 10 und Windows Server 2016

Benutzer können den Empfang von Popupbenachrichtigungen aktivieren, indem sie auf das **Active Center** auf dem OfficeScan Agent-Endpunkt zugreifen. OfficeScan setzt voraus, dass Benutzer Popupbenachrichtigungen aktivieren.

Prozedur

1. Klicken Sie in der Taskleiste auf das Benachrichtigungssymbol und anschließend auf **Alle Einstellungen**.
2. Klicken Sie im Fenster mit den Einstellungen auf **System** und **Benachrichtigungen & Aktionen**.
3. Setzen Sie im Abschnitt **Benachrichtigungen** die Einstellung **App-Benachrichtigungen anzeigen** auf **Ein**.

OfficeScan Funktionsunterstützung im Benutzeroberflächenmodus

Der Modus, in dem Benutzer Windows 8/8.1 oder Windows Server 2012/2016 verwenden, hat Einfluss auf Internet Explorer 10 oder höhere Versionen und somit darauf, in welchem Umfang die einzelnen OfficeScan Funktionen unterstützt werden. In der folgenden Tabelle ist der Umfang der Unterstützung für die verschiedenen OfficeScan Funktionen im Desktop-Modus und im Windows-Benutzeroberflächenmodus aufgeführt.

Hinweis

Nicht aufgeführte Funktionen bieten in beiden Windows-Betriebsmodi vollständige Unterstützung.

TABELLE C-3. OfficeScan Funktionsunterstützung im Benutzeroberflächenmodus

FUNKTION	DESKTOP-MODUS	WINDOWS-BENUTZEROBERFLÄCHEN MODUS
Webserverkonsole	Vollständige Unterstützung	Nicht unterstützt
Web reputation	Vollständige Unterstützung	Eingeschränkte Unterstützung • HTTPS-Suchfunktion deaktiviert
Firewall	Vollständige Unterstützung	Eingeschränkte Unterstützung • Anwendungsfilter deaktiviert

Internet Explorer 10/11 und Microsoft Edge

Internet Explorer (IE) 10 ist der Standardbrowser in Windows 8/8.1 und Windows Server 2012. Es gibt zwei verschiedene Versionen von Internet Explorer 10: eine für den Windows-Benutzeroberflächenmodus und einen für den Desktop-Modus.

Microsoft Edge wird in Windows 10 und Windows Server 2016 als Standardbrowser verwendet.

Hinweis

Die HTTPS-Suchfunktion ist in Microsoft Edge deaktiviert, da Microsoft Edge keine Plug-in-Erweiterungen unterstützt.

Internet Explorer 10 oder höher für den Windows-Benutzeroberflächenmodus bietet eine Plug-In-freie Browserumgebung. Plug-In-Programme für das Webbrowsing folgten

bisher keinen festgelegten Standards und demnach variiert die Qualität des Codes dieser Plug-In-Programme. Plug-Ins erfordern zudem mehr Systemressourcen und erhöhen das Risiko einer Malwareinfektion.

Microsoft hat Internet Explorer 10 oder höher für den Windows-Benutzeroberflächenmodus nach neuen standardbasierten Technologien entwickelt, um die zuvor verwendeten Plug-In-Lösungen zu ersetzen. In der folgenden Tabelle sind die Technologien aufgeführt, die Internet Explorer 10 oder höher statt der älteren Plug-In-Technologie einsetzt.

TABELLE C-4. Vergleich zwischen standardbasierten Technologien und Plug-In-Programmen

FUNKTION	STANDARDISIERTE WORLD WIDE WEB (W3C) TECHNOLOGIE	BEISPIELHAFTE PLUG-IN-ENTSPRECHUNGEN
Video und Audio	HTML5 Video und Audio	• Flash • Apple QuickTime • Silverlight
Grafiken	• HTML5 canvas • Scalable Vector Graphics (SVG) • Cascading Style Sheets, Level 3 (CSS3) Transitions und Animations • CSS-Transformationen	• Flash • Apple QuickTime • Silverlight • Java-Applets
Offline-Speicher	• Webspeicher • Datei-API • IndexedDB • Anwendungscache-API	• Flash • Java-Applets • Google Gears
Netwerkkommunikation, Ressourcenfreigabe, Dateiupload	• HTML Web Messaging • Cross-origin resource sharing (CORS)	• Flash • Java-Applets

Microsoft hat außerdem eine Plug-In-kompatible Internet Explorer 10-Version oder höher allein für den Desktop-Modus entwickelt. Wenn Benutzer im Windows-Benutzeroberflächenmodus auf eine Website treffen, die die Verwendung zusätzlicher Plug-In-Programme erfordert, wird in Internet Explorer 10 oder höher eine Benachrichtigung angezeigt, die die Benutzer auffordert, in den Desktop-Modus zu wechseln. Im Desktop-Modus können Benutzer Websites anzeigen, die die Verwendung oder Installation von Drittanbieter-Plug-Ins erfordern.

Anhang D

OfficeScan Rollback

In diesem Anhang werden der OfficeScan Server und die Unterstützung des agent-Rollbacks behandelt.

Durchführen eines Rollbacks des OfficeScan Servers und der OfficeScan Agenten mit dem Serversicherungspaket

Der Vorgang des OfficeScan Rollbacks umfasst das Rollback von OfficeScan Agents und anschließend das Rollback des OfficeScan Servers.

Wichtig

- Administratoren können das Rollback des OfficeScan Servers und der Agents nur durchführen, indem sie folgendermaßen vorgehen, wenn der Administrator den Server während des Installationsvorgangs sichern möchte. Wenn die Server-Sicherungsdateien nicht verfügbar sind, finden Sie im *Installations- und Upgrade-Handbuch* der zuvor installierten OfficeScan-Version weitere Informationen zum manuellen Rollback.
- Diese Version von OfficeScan unterstützt Rollbacks nur für die folgenden OfficeScan Versionen:
  - OfficeScan 11.0 Service Pack 1 mit kritischem Patch
  - OfficeScan 11.0 Service Pack 1
  - OfficeScan 11.0
  - OfficeScan 10.6 Service Pack 3

Durchführen eines Rollbacks des OfficeScan Agentens

OfficeScan kann für OfficeScan Agents nur ein Rollback auf die Version des wiederherzustellenden Servers durchführen. Ein Rollback von OfficeScan Agents auf eine ältere Version als die des Servers ist nicht möglich.

Wichtig

Stellen Sie sicher, dass Sie das Rollback zuerst für die OfficeScan Agents und erst dann für den OfficeScan Server durchführen.

Prozedur

1. Stellen Sie sicher, dass OfficeScan Agents das Agent-Programm nicht aktualisieren können.

   a. Navigieren Sie in der OfficeScan XG Service Pack 1 Webkonsole zu **Agents** > **Agent-Verwaltung**.

   b. Wählen Sie die OfficeScan Agents für das Rollback aus.

   c. Klicken Sie auf die Registerkarte **Einstellungen** > **Berechtigungen und andere Einstellungen** > **Andere Einstellungen**.

   d. Wählen Sie im Listenfeld **OfficeScan Agents aktualisieren nur die folgenden Komponenten** die Option **Pattern-Dateien, Engines, Treiber** aus.

2. Navigieren Sie in der OfficeScan XG Service Pack 1 Webkonsole zu **Updates** > **Agents** > **Update-Adresse**.

3. Wählen Sie **Benutzerdefinierte Update-Adresse** aus.

4. Klicken Sie in der **Liste der benutzerdefinierten Update-Adresse** auf **Hinzufügen**.

   Es öffnet sich ein neues Fenster.

5. Geben Sie die IP-Adressen der OfficeScan Agents ein, für die das Rollback ausgeführt werden soll.

6. Geben Sie die URL der Update-Adresse an.

   Geben Sie z. B. Folgendes ein:

   ```
   http://<IP-Adresse des OfficeScan Servers>:<port>/
   OfficeScan/download/Rollback
   ```

7. Klicken Sie auf **Speichern**.

8. Klicken Sie auf **Alle Agents benachrichtigen**.

   Wenn der OfficeScan Agent, für den ein Rollback ausgeführt werden soll, von der Update-Adresse aus aktualisiert wird, wird der OfficeScan Agent deinstalliert, und die vorherige Version des OfficeScan Agents wird installiert.

Tipp

Administratoren können den Rollback-Vorgang beschleunigen, indem sie ein manuelles Update auf OfficeScan Agents einleiten. Weitere Informationen finden Sie unter *OfficeScan Agenten manuell aktualisieren auf Seite 6-48*.

9. Fordern Sie den Benutzer nach der Installation der vorherigen Version des OfficeScan Agents auf, den Endpunkt neu zu starten.

   Nachdem der Rollback-Vorgang beendet wurde, berichtet der OfficeScan Agent weiterhin an denselben OfficeScan Server.

Hinweis

Nach dem Rollback des OfficeScan Agent wird ein Rollback aller Komponenten, einschließlich des Viren-Patterns, auf die Vorgängerversion durchgeführt. Wenn Administratoren das Rollback des OfficeScan Servers nicht durchführen, kann der OfficeScan Agent, für den ein Rollback durchgeführt wurde, keine Komponenten aktualisieren. Administratoren müssen die Update-Adresse des OfficeScan Agents, für den ein Rollback durchgeführt wurde, in die Standard-Update-Adresse ändern, um weitere Komponenten-Updates zu erhalten.

Wiederherstellen der Vorgängerversion des OfficeScan Servers

Für den Vorgang zur Wiederherstellung des OfficeScan Servers müssen die Administratoren den OfficeScan XG Service Pack 1 Server deinstallieren, die ältere Serverversion erneut installieren, die Windows-Dienste manuell beenden, die Systemregistrierung aktualisieren und die OfficeScan Server-Dateien im OfficeScan Installationsverzeichnis ersetzen.

Wichtig

Stellen Sie sicher, dass Sie zuerst das Rollback für die OfficeScan Agents durchführen, bevor Sie den OfficeScan Server wiederherstellen.

Prozedur

1. Deinstallieren Sie den OfficeScan XG Service Pack 1 Server.
2. Installieren Sie die Vorgängerversion des OfficeScan Servers.

Tipp

Trend Micro empfiehlt, den Host-Namen bzw. die IP-Adresse beim Wiederherstellen des Servers nicht zu ändern.

Sie können die Vorgängerversion des Servers wie folgt überprüfen: Öffnen Sie den <*Installationsordner des Servers*> und überprüfen Sie den Wiederherstellungsordner, der bei der Installation des OfficeScan XG Service Pack 1 Servers erstellt wurde. Der Ordner hat einen der folgenden Namen (als <Restore_folder_version> bezeichnet):

- OSCE11_SP1: OfficeScan 11.0 Service Pack 1
- OSCE11: OfficeScan 11.0
- OSCE106_SP3: OfficeScan 10.6 Service Pack 3

3. Beenden Sie die folgenden Dienste auf dem OfficeScan Server-Computer.
   - Intrusion Defense Firewall (wenn installiert)
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - OfficeScan Active Directory Integration Service
   - OfficeScan Control Manager Agent
   - OfficeScan Plug-in Manager
   - OfficeScan Master Service
   - World Wide Web Publishing Dienst
4. Kopieren Sie alle Dateien und Verzeichnisse aus dem Verzeichnis `<Server_installation_folder>\<Restore_folder_version>\` in das Verzeichnis `<Server_installation_folder>\PCCSRV\` und ersetzen Sie sie dort.

5. Stellen Sie die OfficeScan Registrierung wieder her.

   a. Öffnen Sie den **Registrierungseditor** (`regedit.exe`).

   b. Wählen Sie im linken Navigationsbereich einen der folgenden Registrierungsschlüssel aus:

      - Für 32-Bit-Systeme: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service`
      - Für 64-Bit-Systeme: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Officescan\service`

   c. Wechseln Sie zu **Datei** > **Importieren...**.

   d. Wählen Sie die allgemeine `.reg`-Datei für den OfficeScan Server aus, die sich im Verzeichnis `<Server_installation_folder>\<Restore_folder_version>\` befindet.

      Der Name der Registrierungsdatei hat das folgende Format:

      `RegBak_<Restore_folder_version>.reg`

   e. Klicken Sie auf **Ja**, um alle vorherigen Versionsschlüssel von OfficeScan wiederherzustellen.

6. Sie können optional den Zeitplan für die Datenbanksicherung wiederherstellen.

   a. Öffnen Sie den **Registrierungseditor** (`regedit.exe`).

   b. Wählen Sie im linken Navigationsbereich einen der folgenden Registrierungsschlüssel aus:

      - Für 32-Bit-Systeme: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Database Backup`
      - Für 64-Bit-Systeme: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Database Backup`

   c. Wechseln Sie zu **Datei** > **Importieren...**.

   d. Wählen Sie die `.reg`-Datei der Datenbank aus, die sich im Verzeichnis `<Server_installation_folder>\<Restore_folder_version>\` befindet.

Der Name der Registrierungsdatei hat das folgende Format:

```
RegBak_DBBak_<Restore_folder_version>.reg
```

e. Klicken Sie auf **Ja**, um alle vorherigen Versionsschlüssel von OfficeScan wiederherzustellen.

7. Öffnen Sie einen Befehlszeilen-Editor (`cmd.exe`) und geben Sie die folgenden Befehle ein, um den Leistungszähler des Local Web Classification Servers zurückzusetzen:

```
cd <Installationsordner des Servers>\PCCSRV\LWCS

regsvr32.exe /u /s perfLWCSPerfMonMgr.dll

regsvr32.exe /s perfLWCSPerfMonMgr.dll
```

8. Starten Sie die folgenden Dienste neu:

- Intrusion Defense Firewall (wenn installiert)
- Trend Micro Local Web Classification Server
- Trend Micro Smart Scan Server
- OfficeScan Active Directory Integration Service
- OfficeScan Control Manager Agent
- OfficeScan Plug-in Manager
- OfficeScan Master Service
- Apache 2 (bei Verwendung des Apache Webservers)
- World Wide Web Publishing Dienst (bei Verwendung des IIS-Webservers)

9. Säubern Sie den Zwischenspeicher des Internet Explorers und entfernen Sie manuell die ActiveX-Steuerelemente. Weitere Informationen zum Entfernen von ActiveX-Steuerelementen im Internet Explorer 9 finden Sie unter http://windows.microsoft.com/en-us/internet-explorer/manage-add-ons#ie=ie-9.

Die Einstellungen der Vorgängerversion des OfficeScan Servers wurden wiederhergestellt.

Tipp

Administratoren können einen erfolgreichen Rollback bestätigen, indem sie die OfficeScan Versionsnummer im **Info**-Fenster (**Hilfe** > **Info**) überprüfen.

10. Optional können Sie den OfficeScan Server mithilfe der Webkonsole beim Control Manager Server registrieren.

11. Optional können Sie den OfficeScan Server mithilfe der Webkonsole beim Deep Discovery Server registrieren.

Hinweis

Die Integration von Deep Discovery mit dem OfficeScan Server ist seit OfficeScan 10.6 Service Pack 2 möglich.

12. Nachdem Sie das erfolgreiche Rollback von OfficeScan bestätigt haben, löschen Sie alle Dateien im Verzeichnis `<Server_installation_folder>\<Restore_folder_version>\`.

Anhang E

Glossar

Die in diesem Glossar enthaltenen Begriffe bieten zusätzliche Informationen zu häufig verwendeten Endpunkt-Begriffen sowie zu Trend Micro Produkten und Technologien.

ActiveUpdate

Die ActiveUpdate Funktion ist Bestandteil vieler Trend Micro Produkte. Über die Verbindung zur Trend Micro Update-Website stellt ActiveUpdate aktuelle Downloads von Pattern-Dateien, Scan Engines, Programmen und anderen Trend Micro Komponentendateien über das Internet bereit.

Komprimierte Datei

Eine einzelne Datei, die eine oder mehrere andere Dateien sowie Informationen darüber enthält, wie diese von einem geeigneten Programm, wie z. B. WinZip, entpackt werden können.

Cookie

Ein Mechanismus zum Speichern von Informationen über einen Internet-Benutzer, wie z.B. Name, Vorlieben und Interessen, um später im Webbrowser wieder darauf zuzugreifen. Wenn Sie das nächste Mal auf eine Website zugreifen, für die vom Browser ein Cookie angelegt wurde, sendet der Browser das Cookie an den Webserver, das dann vom Webserver verwendet werden kann, um angepasste Webseiten darzustellen. Sie könnten zum Beispiel auf einer Website mit Ihrem Namen begrüßt werden.

Denial-of-Service-Angriff

Ein Denial-of-Service-Angriff (DoS) ist ein Angriff auf einen Endpunkt oder ein Netzwerk, der einen "Dienstausfall", nämlich die Unterbrechung der Netzwerkverbindung, zur Folge hat. In der Regel schränken DoS-Angriffe die Bandbreite ein oder überlasten die Endpunkt-Ressourcen (z. B. den Arbeitsspeicher).

DHCP

DHCP (Dynamic Host Control Protocol) ist ein Protokoll zur Zuweisung dynamischer IP-Adressen zu Geräten in einem Netzwerk. Bei der dynamischen Adressierung kann ein Gerät bei jeder Verbindung mit dem Netzwerk eine unterschiedliche IP-Adresse haben. In einigen System kann sich die IP-Adresse des Geräts sogar dann ändern, wenn das Gerät weiterhin verbunden ist. DHCP unterstützt darüber hinaus eine Mischung aus statischen und dynamischen IP-Adressen.

DNS

Bei DNS (Domain Name System) handelt es sich um einen allgemeinen Datenabfragedienst, der im Internet hauptsächlich zum Übersetzen von Host-Namen in IP-Adressen verwendet wird.

Wenn ein DNS-agent Host-Name und Adressdaten von einem DNS-Server abfragt, wird dieser Vorgang als Auflösung bezeichnet. Bei der grundlegenden DNS-Konfiguration führt das Ergebnis zu einem Server, der eine Standardauflösung ausführt. Beispielsweise fragt ein Remote-Server einen anderen Server ab, um Daten zu ermitteln, die sich in einem Computer in der aktuellen Zone befinden. Die Agent-Software im Remote-Server stellt eine Abfrage an den Resolver, der die Anfrage auf Basis seiner Datenbankdateien beantwortet.

Domänenname

Der vollständige Name eines Systems, bestehend aus dem lokalen Host-Namen und dem Domänennamen, z. B. `tellsitall.com`. Ein Domänenname reicht normalerweise aus, um eine eindeutige Internetadresse für einen Host im Internet zu ermitteln. Bei dieser so genannten "Namensauflösung" wird das Domain Name System (DNS) verwendet.

Dynamische IP-Adresse

Eine dynamische IP-Adresse ist eine von einem DHCP-Server zugewiesene IP-Adresse. Die MAC-Adresse des Endpunkts bleibt unverändert, die IP-Adresse hingegen kann sich ändern, da der DHCP-Server dem Endpunkt je nach Verfügbarkeit eine neue IP-Adresse zuweist.

ESMTP

ESMTP (Enhanced Simple Mail Transport Protocol) umfasst Sicherheits-, Authentifizierungs- und weitere Vorrichtungen für die Einsparung von Bandbreite und den Schutz von Servern.

Endbenutzer-Lizenzvereinbarung

Eine Endbenutzer-Lizenzvereinbarung (oder auch EULA) ist ein rechtsgültiger Vertrag zwischen einem Software-Hersteller und dem Software-Benutzer. Der Vertrag legt in der Regel Einschränkungen für den Benutzer fest. Der Benutzer kann den Vertrag ablehnen, indem er während der Installation nicht auf "Ich akzeptiere" klickt. Klickt er auf "Ich akzeptiere die Bedingungen nicht", wird die Installation der Software unverzüglich abgebrochen.

Viele Benutzer stimmen versehentlich der Installation von Spyware und anderer Typen von Grayware zu, wenn sie bei der Installation bestimmter Arten kostenloser Software in der EULA-Eingabeaufforderung auf "Ich akzeptiere" klicken.

Fehlalarm

Ein Fehlalarm wird ausgelöst, wenn eine Datei von einer Sicherheitssoftware fälschlicherweise als infiziert eingestuft wird.

FTP

FTP (File Transfer Protocol) ist ein Standardprotokoll zum Übertragen von Dateien über das Internet vom Server zu einem Client. Weitere Informationen finden Sie in der Spezifikation RFC 959 der Network Working Group.

GeneriClean

GeneriClean, auch als referenzielle Säuberung bekannt, ist eine neue Technologie zum Entfernen von Viren/Malware, wenn keine Viren-Cleanup-Komponenten verfügbar sind. Mit Hilfe einer entdeckten Datei ermittelt GeneriClean, ob für diese Datei ein Prozess/Dienst im Speicher ausgeführt wird und ein Registrierungseintrag erstellt wurde; falls ja, werden diese Elemente entfernt.

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).

Standardmäßig können OfficeScan Agents Hotfixes installieren. Wenn die OfficeScan Agents keine Hotfixes installieren sollen, müssen Sie die agent-Einstellungen über die Webkonsole auf der Registerkarte unter **Agents** > **Agent-Verwaltung**, **Einstellungen** > **Berechtigungen und andere Einstellungen** > **Andere Einstellungen** ändern.

Wenn Sie erfolglos versuchen, einen Hotfix auf dem OfficeScan Server zu installieren, verwenden Sie das Touch Tool, um den Zeitstempel des Hotfixes zu ändern. Dadurch erkennt OfficeScan den Hotfix als neu, und der Server versucht automatisch, den Hotfix erneut zu verteilen. Detaillierte Hinweise zu diesem Tool finden Sie unter *Touch Tool für OfficeScan Agent Hot Fixes ausführen auf Seite 6-57*.

HTTP

Bei HTTP (Hypertext Transfer Protocol) handelt es sich um ein Standardprotokoll für die Übertragung von Websites (einschließlich Grafiken und Multimedia-Inhalten) von einem Server an einen Client über das Internet.

HTTPS

Hypertext Transfer Protocol mit SSL (Secure Socket Layer). HTTPS ist eine Variante von HTTP, die für sichere Transaktionen verwendet wird.

ICMP

Das ICMP-Protokoll (Internet Control Message Protocol) wird manchmal von einem Gateway oder Ziel-Host für die Kommunikation mit einem Quell-Host verwendet, um z. B. einen Fehler bei der Datagrammverarbeitung zu melden. Dabei verwendet ICMP die IP-Basisunterstützung, so als handle es sich um ein Protokoll einer höheren Ebene. Tatsächlich ist ICMP jedoch ein Bestandteil von IP und wird von jedem IP-Modul implementiert. ICMP-Nachrichten werden in verschiedenen Situationen gesendet, beispielsweise wenn ein Datagramm sein Ziel nicht erreichen kann, wenn das Gateway nicht über genügend Pufferkapazität verfügt, um ein Datagramm weiterzuleiten, und wenn das Gateway den Host anweisen kann, für den Datenverkehr eine kürzere Route zu wählen. Das Internet Protocol ist nicht absolut zuverlässig. Der Sinn und Zweck dieser Steuerungsnachrichten liegt darin, Rückmeldung über Probleme in der Kommunikationsumgebung zu geben, und nicht darin, die Zuverlässigkeit von IP zu erhöhen.

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

Virenschreiber versuchen häufig, durch die Verwendung von Methoden zur Echtzeitkomprimierung Virenfilter zu umgehen. IntelliTrap sperrt ausführbare, in Echtzeit komprimierte Dateien und überprüft sie auf andere Malware-Merkmale. Dadurch kann das Risiko einer Einschleusung solcher Viren in das Netzwerk reduziert werden. Da IntelliTrap derartige Dateien als Sicherheitsrisiko kennzeichnet und dadurch möglicherweise sichere Dateien sperrt, sollten Sie nach der Aktivierung von IntelliTrap Dateien in Quarantäne stellen (nicht löschen oder säubern). Tauschen die Benutzer im Netzwerk regelmäßig ausführbare, in Echtzeit komprimierte Dateien aus, deaktivieren Sie IntelliTrap.

IntelliTrap verwendet die folgenden Komponenten:

- Viren-Scan-Engine
- IntelliTrap Pattern
- IntelliTrap Ausnahme-Pattern

IP

"Das Internet Protocol (IP) ermöglicht die Übertragung von Datenblöcken, so genannten Datagrammen, von Quellen an Ziele. Bei diesen Quellen und Zielen handelt es sich um Hosts, die anhand von Adressen mit fester Länge identifiziert werden." (RFC 791)

Java-Datei

Java ist eine universelle Programmiersprache, die von Sun Microsystems entwickelt wurde. Eine Java-Datei enthält Java-Code. Java unterstützt die Programmierung für das Internet in Form von plattformunabhängigen Java-Applets. Bei einem Applet handelt es sich um ein in der Programmiersprache Java entwickeltes Programm, das auf einer HTML-Seite enthalten sein kann. Wenn Sie mit einem Java-fähigen Browser eine Seite anzeigen, die ein Applet enthält, wird der Code des Applets auf Ihren Endpunkt übertragen und von der Java Virtual Machine des Browsers ausgeführt.

LDAP

LDAP (Lightweight Directory Access Protocol) ist ein Anwendungsprotokoll, um Verzeichnisdienste über TCP/IP abzufragen und zu ändern.

Listening-Port

Ein Listening-Port wird für Verbindungsanfragen des agents zum Datenaustausch verwendet.

MCP Agent

Trend Micro Management Communication Protocol (MCP) ist der Agent der nächsten Generation von Trend Micro für verwaltete Produkte. MCP ersetzt die Trend Micro Management Infrastructure (TMI) für die Kommunikation zwischen dem Control Manager und OfficeScan. verfügt über mehrere neue Funktionen:

- Geringere Netzwerklast und Paketgröße
- Unterstützung für NAT- und Firewall-Traversal
- HTTPS-Unterstützung

- Unterstützung der Ein- und Zwei-Wege-Kommunikation
- SSO-Unterstützung (Single Sign-On)
- Cluster-Knoten-Unterstützung

Kombinierte Bedrohungen

Kombinierte Bedrohungen profitieren von mehreren Eintrittsstellen und Schwachstellen in den Unternehmensnetzwerken. Beispiele hierfür sind die Bedrohungen "Nimda" oder "Code Red".

NAT

NAT (Network Address Translation) ist ein Standard zur Übersetzung von sicheren IP-Adressen in temporäre, externe, registrierte IP-Adressen aus dem Adresspool. Auf diese Weise können vertrauenswürdige Netzwerke mit privat zugeordneten IP-Adressen auf das Internet zugreifen. Das bedeutet auch, dass Sie keine registrierte IP-Adresse für jeden Computer im Netzwerk benötigen.

NetBIOS

NetBIOS (Network Basic Input Output System) ist eine API (Application Program Interface), die das grundlegende Eingabe/Ausgabe-System (BIOS) des Betriebssystems (DOS) um weitere Funktionalität (beispielsweise Netzwerkfähigkeiten) ergänzt.

Ein-Wege-Kommunikation

Die Weiterleitung der übersetzten Netzwerkadresse (NAT-Traversal) ist in aktuellen, realen Netzwerkumgebungen ein immer wichtigeres Problem. Zur Lösung des Problems verwendet MCP die Ein-Wege-Kommunikation. Bei der Ein-Wege-Kommunikation stellt der MCP-Agent die Verbindung zum Server her und ruft die Befehle vom Server

ab. Jede Anfrage besteht aus einer CGI-ähnlichen Befehlsabfrage oder einer Protokollübertragung. Um das Netzwerk zu schonen, hält der MCP-Agent so viele Verbindungen wie möglich aufrecht und offen. Nachfolgende Anfragen verwenden eine vorhandene, offene Verbindung. Beim Abbruch der Verbindung können alle SSL-Verbindungen zum selben Host-Computer auf die zwischengespeicherte Sitzungskennung zugreifen und dadurch den erneuten Verbindungsaufbau erheblich beschleunigen.

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.

Phishing-Angriff

Phishen 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, 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.

Ping

Ping ist ein Dienstprogramm, das eine ICMP-Echoanfrage an eine IP-Adresse sendet und auf Antwort wartet. Das Ping-Dienstprogramm kann feststellen, ob der Endpunkt mit dieser IP-Adresse online ist oder nicht.

POP3

POP3 (Post Office Protocol 3) ist ein Standardprotokoll für das Speichern und Übertragen von E-Mail-Nachrichten von einem Server an einen E-Mail-Client.

Proxy-Server

Ein Proxy-Server ist ein WWW-Server, der URLs mit einem speziellen Präfix akzeptiert, mit dem Dokumente entweder von einem lokalen Zwischenspeicher oder einem Remote-Server abgerufen werden, und der dann den URL an die anfordernde Instanz zurücksendet.

RPC

RPC (Remote Procedure Call) ist ein Netzwerkprotokoll, das einem auf einem Host laufenden Programm ermöglicht, Code auf einem anderen Host auszuführen.

Sicherheits-Patch

Ein Sicherheits-Patch ist auf sicherheitsrelevante Probleme ausgerichtet und kann an alle Kunden verteilt werden. Sicherheits-Patches von Windows verfügen über ein Setup-

Programm, während andere Patches in der Regel über ein Setup-Skript ausgeführt werden.

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.

SMTP

SMTP (Simple Mail Transport Protocol) ist ein Standardprotokoll für die Übertragung von E-Mail-Nachrichten von Server zu Server und von agent zu Server über das Internet.

SNMP

SNMP (Simple Network Management Protocol) ist ein Protokoll, das die Überwachung von Geräten im Hinblick auf Zustände unterstützt, die die Aufmerksamkeit eines Administrators erfordern.

SNMP-Trap

Ein SNMP-Trap (Simple Network Management Protocol) ist eine Methode zum Versenden von Benachrichtigungen an Netzwerkadministratoren, deren Management-Konsolen dieses Protokoll unterstützen.

OfficeScan kann Benachrichtigungen in MIBs (Management Information Bases) speichern. Sie können den MIB-Browser verwenden, um SNMP-Trap-Benachrichtigungen anzuzeigen.

SSL

Secure Socket Layer (SSL) ist ein von Netscape entwickeltes Protokoll für die Datensicherheit, das im Schichtenmodell zwischen Anwendungsprotokollen (z. B. HTTP, Telnet oder FTP) und TCP/IP liegt. Dieses Sicherheitsprotokoll bietet Datenverschlüsselung, Serverauthentifizierung, Nachrichtenintegrität und optionale agent-Authentifizierung für eine TCP/IP-Verbindung.

SSL-Zertifikat

Dieses digitale Zertifikat baut eine sichere HTTPS-Kommunikation auf.

TCP

TCP (Transmission Control Protocol) ist ein verbindungsorientiertes, zuverlässiges End-to-End-Protokoll für eine aus Schichten bestehende Hierarchie von Protokollen zur Unterstützung von Multi-Netzwerk-Anwendungen. TCP verwendet IP-Datagramme für die Adressauflösung. Weitere Informationen finden Sie in der Spezifikation DARPA Internet Program RFC 793.

Telnet

Telnet stellt über TCP eine Standardschnittstelle zwischen Endgeräten bereit, indem ein so genanntes "Network Virtual Terminal" erstellt wird. Weitere Informationen finden Sie in der Spezifikation RFC 854 der Network Working Group.

Trojanerports

Trojaner-Ports werden häufig von Trojanern zum Verbindungsaufbau mit Endpunkte verwendet. Während eines Ausbruchs blockiert OfficeScan die folgenden Portnummern, die eventuell von Trojanern verwendet werden.

TABELLE E-1. 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
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

PORTNUMMER	TROJANER	PORTNUMMER	TROJANISCHES PFERD
7300	Net Spy	1234	Valvo line

Vertrauenswürdiger Port

Vertrauenswürdige Ports werden vom Server und vom OfficeScan Agent verwendet, um miteinander zu kommunizieren.

Wenn Sie nach einem Ausbruch die vertrauenswürdigen Ports gesperrt haben und die Netzwerkeinstellungen später wieder auf den Normalzustand zurücksetzen, nehmen die OfficeScan Agents nicht sofort wieder Verbindung zum Server auf. AgentDie Agent-Server-Kommunikation wird erst nach Ablauf der Anzahl von Stunden wiederhergestellt, die Sie im Fenster "Ausbruchsprävention – Einstellungen" festgelegt haben.

OfficeScan verwendet den HTTP-Port (standardmäßig 8080) als vertrauenswürdigen Port auf dem Server. Bei der Installation können Sie eine andere Portnummer eingeben. Um diesen und den vertrauenswürdigen Port auf dem OfficeScan Agent zu sperren, müssen Sie das Kontrollkästchen "Vertrauenswürdige Ports sperren" im Fenster "Ports sperren" aktivieren.

Bei der Installation generiert der Master Installer den vertrauenswürdigen OfficeScan Agent-Port nach dem Zufallsprinzip.

Ermitteln der vertrauenswürdigen Ports

Prozedur

1. Greifen Sie auf den Ordner <Installationsordner des Servers>\PCCSRV zu.
2. Öffnen Sie die Datei `ofcscan.ini` mit einem Texteditor, wie z. B. Notepad.
3. Um den vertrauenswürdigen Port auf dem Server zu ermitteln, suchen Sie die Zeichenfolge "Master_DomainPort", und überprüfen Sie den daneben stehenden Wert.

Wenn der Eintrag zum Beispiel `Master_DomainPort=80` lautet, wird Port 80 als vertrauenswürdiger Port auf dem Server verwendet.

4. Um den vertrauenswürdigen Port auf dem agent zu ermitteln, suchen Sie die Zeichenfolge "Client_LocalServer_Port" und überprüfen Sie den daneben stehenden Wert.

   Wenn der Eintrag zum Beispiel `Client_LocalServer_Port=41375` lautet, wird Port 41375 als vertrauenswürdiger Port auf dem agent verwendet.

Zwei-Wege-Kommunikation

Die Zwei-Wege-Kommunikation ist eine Alternative zur Ein-Wege-Kommunikation. Die Zwei-Wege-Kommunikation baut auf der Ein-Wege-Kommunikation auf, verfügt jedoch über einen zusätzlichen HTTP-basierten Kanal, der Server-Benachrichtigungen empfängt. Dadurch kann die Echtzeitverteilung und -verarbeitung von Serverbefehlen durch den MCP-Agent verbessert werden.

UDP

UDP (User Datagram Protocol) ist ein verbindungsloses Kommunikationsprotokoll, das zusammen mit dem IP-Übertragungsprotokoll für Anwendungsprogramme verwendet wird, um Nachrichten an andere Programme zu senden. Weitere Informationen finden Sie in der Spezifikation DARPA Internet Program RFC 768.

Dateien, die nicht gesäubert werden können

Die Viren-Scan-Engine ist nicht in der Lage, die folgende Dateien zu säubern:

TABELLE E-2. 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: Trojaner werden mit Hilfe der Damage Cleanup Engine und des Damage Cleanup Template entfernt.
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 Endpunkt-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 Endpunkt fehlerfrei funktioniert, können Sie die Kopie löschen.

Nicht zu säubernde Datei	Erklärung und Lösung
Infizierte Dateien im Papierkorb	Infizierte Dateien im Papierkorb des Systems können möglicherweise nicht entfernt werden, wenn das System aktiv ist.

	Lösung unter Windows XP oder Windows Server 2003 mit dem NTFS-Dateisystem:
	1. Melden Sie sich beim Endpunkt als Administrator an.
	2. Schließen Sie alle aktiven Anwendungen, damit die Datei nicht gesperrt wird. Windows könnte sie sonst nicht löschen.
	3. Öffnen Sie ein Eingabeaufforderungsfenster.
	4. Geben Sie zum Löschen der Dateien folgende Befehle ein:
	`cd \`
	`cd recycled`
	`del *.* /S`
	Mit dem letzten Befehl werden alle Dateien im Papierkorb gelöscht.
	5. Überprüfen Sie, ob die Dateien entfernt wurden.

	Bei Computern unter anderen Betriebssystemen (oder Plattformen ohne NTFS):
	1. Starten Sie den Endpunkt 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	Dateien in diesen Ordnern können möglicherweise nicht gesäubert werden, da sie vom Endpunkt verwendet werden. Möglicherweise handelt es sich bei den Dateien, die gesäubert

Nicht zu säubernde Datei	Erklärung und Lösung
Internet Explorer-Ordner "Temporary Internet Files"	werden sollen, um temporäre Dateien, die für den Betrieb von Windows benötigt werden.

	Lösung unter Windows XP oder Windows Server 2003 mit dem NTFS-Dateisystem:
	1. Melden Sie sich beim Endpunkt als Administrator an.
	2. Schließen Sie alle aktiven Anwendungen, damit die Datei nicht gesperrt wird. Windows könnte sie sonst nicht löschen.
	3. Wenn sich die infizierte Datei im Windows Ordner "Temp" befindet:
	a. Öffnen Sie die Eingabeaufforderung und navigieren Sie zum Windows-Ordner "Temp" (standardmäßig unter `C:\Windows\Temp` für Windows XP oder Windows Server 2003-Endpunkte).
	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.
	4. Wenn sich die infizierte Datei im tempoären Ordner von Internet Explorer befindet:
	a. Öffnen Sie die Eingabeaufforderung, und navigieren Sie zum temporären Internet Explorer-Ordner (standardmäßig bei Endpunkte mit Windows XP oder Windows Server 2003 `C:\Dokumente und Einstellungen\<Ihr Benutzername>\Lokale Einstellungen\Temporary Internet Files`).
	b. Geben Sie zum Löschen der Dateien folgende Befehle ein:
	`cd tempor~1`

Nicht zu säubernde Datei	Erklärung und Lösung

	`attrib -h`
	
	`del *.* /S`
	
	Mit dem letzten Befehl werden alle Dateien im temporären Ordner des Internet Explorers gelöscht.
	
	c. Überprüfen Sie, ob die Dateien entfernt wurden.

	Bei Computern unter anderen Betriebssystemen (oder Plattformen ohne NTFS):
	
	1. Starten Sie den Endpunkt im MS-DOS Modus neu.
	
	2. Wenn sich die infizierte Datei im Windows Ordner "Temp" befindet:
	
	a. Öffnen Sie die Eingabeaufforderung und navigieren Sie zum Windows-Ordner "Temp" (standardmäßig unter `C:\Windows\Temp` für Windows XP oder Windows Server 2003-Endpunkte).
	
	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 Endpunkt im Normalmodus neu.
	
	3. Wenn sich die infizierte Datei im tempoären Ordner von Internet Explorer befindet:
	
	a. Öffnen Sie die Eingabeaufforderung, und navigieren Sie zum temporären Internet Explorer-Ordner (standardmäßig bei Endpunkte mit Windows XP oder Windows Server 2003 `C:\Dokumente und Einstellungen\<Ihr Benutzername>\Lokale Einstellungen\Temporary Internet Files`).

NICHT ZU SÄUBERNDE DATEI	ERKLÄRUNG UND LÖSUNG

	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 Endpunkt 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.

Mit Trojanern infizierte Dateien

Trojaner sind Programme, die unerwartete oder unberechtigte, in der Regel aber schädliche Aktionen ausführen. Es werden beispielsweise Meldungen angezeigt, Dateien gelöscht, oder Disketten und Festplatten werden formatiert. Da Trojaner keine Dateien infizieren, ist kein Säubern erforderlich.

Lösung: Der OfficeScan Agent entfernt Trojaner mit Hilfe der Damage Cleanup Engine und der Damage Cleanup Template.

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 Endpunkt-Systeme verteilen kann. Würmer verbreiten sich normalerweise über Netzwerkverbindungen oder E-Mail-Anhänge. Ein Wurm ist ein eigenständiges Programm, das nicht gesäubert werden kann.

Lösung: Trend Micro empfiehlt, Würmer zu löschen.

Infizierte, schreibgeschützte Dateien

Lösung: Heben Sie den Schreibschutz auf, damit der OfficeScan Agent die Datei säubern kann.

Kennwortgeschützte Dateien

Umfasst kennwortgeschützte komprimierte Dateien oder kennwortgeschützte Microsoft Office Dateien.

Lösung: Heben Sie den Kennwortschutz auf, damit OfficeScan Agent diese Dateien säubern kann.

Sicherungsdateien

Bei Dateien mit den Erweiterungen RB0~RB9 handelt es sich um Sicherungskopien infizierter Dateien. Der OfficeScan Agent erstellt eine Sicherungskopie der infizierten Datei, für den Fall, dass der Virus bzw. die Malware die Datei während des Säuberungsvorgangs beschädigt hat.

Lösung: Wenn die infizierte Datei von OfficeScan Agent gesäubert werden konnte, muss die Sicherungskopie nicht aufbewahrt werden. Wenn der Endpunkt fehlerfrei funktioniert, können Sie die Sicherungskopie löschen.

Stichwortverzeichnis

A

Abfragehandhabung für kontextbezogene Intelligenz, 6-6
ActiveAction, 7-43
Active Directory, 2-36–2-39, 2-55, 2-59, 5-14, 5-31
  Adressbereich und Abfrage, 15-79
  Agent-Gruppierung, 2-55
  Anmeldedaten, 2-38
  Ausgelagerte Serververwaltung, 2-37
  Benutzerdefinierte Agent-Gruppen, 2-37
  integration, 2-36
  Struktur duplizieren, 2-59
  Synchronisierung, 2-39
ActiveSync, 11-41
Agent deinstallieren, 5-74
Agent-Disk-Image, 5-15, 5-37
Agent-Gruppierung, 2-54–2-56, 2-58, 2-60–2-63
  Active Directory, 2-55, 2-58
  Agents verschieben, 2-63
  Aufgaben, 2-61
  Automatisch, 2-55, 2-56
  Benutzerdefinierte Gruppen, 2-55
  DNS, 2-55
  Domäne oder Agent löschen, 2-62
  Hinzufügen einer Domäne, 2-62
  IP-Adressen, 2-60
  Manuell, 2-55
  Methoden, 2-54
  NetBIOS, 2-55
  Umbenennen einer Domäne, 2-63
Agent-Hierarchie, 2-40, 2-43–2-46, 2-50–2-52
  Allgemeine Aufgaben, 2-43
  Ansichten, 2-43
  Erweiterte Suche, 2-43, 2-44
  Filter, 2-43
  Info über, 2-40
  Spezifische Aufgaben, 2-45, 2-46, 2-50–2-52
    Agent-Verwaltung, 2-46
    Ausbruchsprävention, 2-50
    Manuelle Komponenten-Updates, 2-51
    Rollback der Komponenten-Updates durchführen, 2-51
    Sicherheitsrisiko-Protokolle, 2-52
Agent-Installation, 5-2, 5-22
  Agent Packager, 5-25
  Anmeldeskript-Setup, 5-22
  E-Mail-Link, 5-17
  Nach der Installation, 5-71
  Per Agent-Disk-Image, 5-37
  Systemvoraussetzungen, 5-2
  über die Webkonsole, 5-19
  Verwenden der Sicherheitsrichtlinien, 5-65
  Vulnerability Scanner verwenden, 5-38
Agent-Konsole
  Zugriffsbeschränkung, 15-18
agent mover, 15-24
Agent Packager, 5-14, 5-25, 5-28, 5-31, 5-33
  Einstellungen, 5-28
  Verteilung, 5-25
Agent-Pattern der intelligenten Suche, 4-8
Agent-Protokolle
  Agent-Update-Protokolle, 18-18
  Agent-Verbindungsprotokolle, 18-18

Datenschutz-Debug-Protokolle, 11-69, 18-25
Debug-Protokolle, 18-15
Debug-Protokolle der Ausbruchsprävention, 18-19
Debug-Protokolle der OfficeScan Firewall, 18-20
Debug-Protokolle für die Verhaltensüberwachung, 18-20
Erstinstallations-Protokolle, 18-16
Mail Scan Protokolle, 18-18
Protokolle für Damage Cleanup Services, 18-17
TDI-Debug-Protokolle, 18-26
Upgrade-/Hotfix-Protokolle, 18-17
agents, 2-54, 2-62, 2-63, 4-32, 5-2
Gruppierung, 2-54
installation, 5-2
löschen, 2-62
Proxy-Einstellungen, 4-32
Standorte, 4-32
Verbindung, 4-32
verschieben, 2-63
Agents
Funktionen, 5-3
Agent-Update
Automatisch, 6-41
Benutzerdefinierte Adresse, 6-34
Berechtigungen, 6-49
Ereignisbedingt, 6-42
Manuell, 6-47
Standard-Adresse, 6-33
Über den ActiveUpdate Server, 6-50
Zeitgesteuertes Update, 6-43
Zeitgesteuertes Update mit NAT, 6-45
Agent-Upgrade
Deaktivieren, 6-50
Aktion bei überwachten Systemereignissen, 9-8
Aktionen
Prävention vor Datenverlust, 11-42
Allgemeine C&C-IP-Liste, 6-10
Allgemeiner Firewall-Treiber, 6-8
Angaben zum Webserver, 14-61
Anmeldeskript-Setup, 5-13, 5-14, 5-22, 5-23
Anregungen und Kritik, 19-6
ARP-Konflikt, 13-5
Aufgaben vor der Installation, 5-19, 5-65
Ausbruchpräventionsrichtlinie
Ausführbare komprimierte Dateien, 7-128
Gegenseitige Ausschlüsse, 7-127
Mutex-Behandlung, 7-127
Ports sperren, 7-124
Schreibzugriff verweigern, 7-126
Zugriff auf Freigabeordner einschränken/verweigern, 7-123
Zugriff auf komprimierte Dateien verweigern, 7-128
Ausbruchskriterien, 7-117, 12-20, 13-34
Ausbruchsprävention, 2-33
Deaktivieren, 7-129
Richtlinien, 7-123
Ausdrücke, 11-6
benutzerdefiniert, 11-7, 11-11
Kriterien, 11-8, 11-9
vordefiniert, 11-6, 11-7
Ausgelagerte Serververwaltung, 2-37, 15-78
Abfrageergebnisse, 15-82
Protokolle, 18-9
Zeitgesteuerte Abfrage, 15-83
Ausschlussliste, 9-10

Verhaltensüberwachung, 9-10
Automatische Agent-Gruppierung, 2-55, 2-56
AutoPcc.exe, 5-13, 5-14, 5-22, 5-23

B

Bedingungsanweisungen, 11-23
Begriffe, xiv
Benachrichtigungen
Agent-Benutzer, 7-97
Agent-Update, 6-54
C&C-Callback-Erkennungen, 12-19
Erkennung von Internet-Bedrohung, 12-14
Firewall-Verstöße, 13-31
Für Administratoren, 11-58, 14-43
für Agent-Benutzer, 11-62
Gerätesteuerung, 10-19
Neustart des Endpunkts, 6-55
Spyware-/Grayware-Fund, 7-56
Veraltetes Viren-Pattern, 6-55
Viren-/Malware-Fund, 7-49
Virenausbrüche, 7-117, 12-20, 13-34
Benutzerdefinierte Agent-Gruppen, 2-37, 2-55
Benutzerdefinierte Ausdrücke, 11-7–11-9, 11-11
Importieren, 11-11
Kriterien, 11-8, 11-9
Benutzerdefinierte Schlüsselwörter, 11-17
Importieren, 11-21
Kriterien, 11-17–11-19
Benutzerdefinierte Vorlagen, 11-23
erstellen, 11-24
Importieren, 11-26
Benutzerkonten, 2-5
dashboard, 2-5
Benutzerrolle
administrator, 14-16
Gastbenutzer, 14-17
Trend Hauptbenutzer, 14-17
Berechtigungen
Beenden, Berechtigung, 15-19
Berechtigungen für die zeitgesteuerte Suche, 7-65
Erweitert, 10-13
Firewall-Berechtigungen, 13-26, 13-28
Mail Scan Berechtigungen, 7-71
Nicht-Speichergeräte, 10-11
Programmpfad und -name, 10-9
Proxy-Konfiguration, Berechtigungen, 15-55
Speichergeräte, 10-4
Suchberechtigungen, 7-63
Unabhängiger Modus, Berechtigung, 15-20
Bericht zur Einhaltung von Richtlinien, 15-63
Bewertungsmodus, 7-86
Bootsektorvirus, 7-4
Bösartiger ActiveX-Code, 7-4
Bösartiger Java-Code, 7-4

C

C&C-Callbacks
Allgemeine Einstellungen
Benutzerdefinierte IPO-Listen, 8-7
widgets, 2-27
Cache-Einstellungen für die Suche, 7-73
Cache für die On-Demand-Suche, 7-75
Case Diagnostic Tool, 18-2
Certified Safe Software Liste, 13-3
Certified Safe Software Service, 7-80, 9-19, 13-29
COM-Dateiinfektor, 7-4
Command & Control-Kontaktalarmdienste, 12-2
Global Intelligence-Liste, 12-3

Smart Protection Server, 12-3
Virtual Analyzer, 12-3
Virtual Analyzer Liste, 12-3
Control Manager
Integration in OfficeScan, 14-25
MCP-Agent-Protokolle, 18-11
Cookies durchsuchen, 7-87
CPU-Auslastung, 7-33

D

Damage Cleanup Engine, 6-7
Damage Cleanup Services, 1-10, 5-4, 5-7
Damage Cleanup Template, 6-7
dashboard, 2-5
Benutzerkonten, 2-5
dashboards
Zusammenfassung, 2-6, 2-8
Dashboard Übersicht, 2-6, 2-8
Komponenten und Programme, 2-35
Registerkarten, 2-8
Status der Produktlizenz, 2-6
widgets, 2-8
Dateiattribute, 11-6, 11-11, 11-13, 11-14
erstellen, 11-13
Importieren, 11-14
Platzhalter, 11-13
vordefiniert, 11-12
Datenbank, Suche, 7-82
Datenbanksicherung, 14-54
Datenbezeichner, 11-6
Ausdrücke, 11-6
Dateiattribute, 11-6
Schlüsselwörter, 11-6
Datenschutz, 11-2
Deinstallation, 3-15
Installation, 3-2
Lizenz, 3-4
status, 3-8
Verteilung, 3-6
Debug-Protokolle
agents, 18-15
server, 18-3
Deinstallation, 5-74
Datenschutz, 3-15
Plug-in Manager, 17-12
Plug-in-Programm, 17-12
über die Webkonsole, 5-75
Verwenden des Deinstallationsprogramms, 5-76
Dekomprimierungsregeln, 11-47
Device List, 10-15
DHCP-Einstellungen, 5-48
Dienst neu starten, 15-12
digitaler Signatur-Cache, 7-74
Dokumentation, xii
Domänen, 2-54, 2-62, 2-63
Agent-Gruppierung, 2-54
hinzufügen, 2-62
löschen, 2-62
umbenennen, 2-63
DSP, 10-9

E

Early Boot Cleanup Driver, 6-7
Echtzeitsuchdienst, 15-43
Echtzeitsuche, 7-17
EICAR-Testskript, 5-73, 7-3
Eigenschutz des Agents, 15-13
eigenständiger Server, 4-7
Eigenständiger Smart Protection Server, 4-18
ptngrowth.ini, 4-18
Einhaltung von Sicherheitsrichtlinien, 15-62
Ausgelagerte Serververwaltung, 2-37, 15-78

Dienste, 15-64
durchsetzen, 15-79
Einstellungen, 15-71
installation, 5-64
Komponenten, 15-66
Protokolle, 18-9
Suche, 15-68
Update erzwingen, 6-56
Zeitgesteuerte Bewertungen, 15-77
Einheitliches Skriptanalysemuster, 6-10
Einstellungen exportieren, 15-60
Einstellungen importieren, 15-60
E-Mail-Domänen, 11-28
E-Mail-Link-Installation, 5-12
Endbenutzer-Lizenzvereinbarung (EULA), E-4
Ereignisüberwachung, 9-6
Erkennungs-Pattern der Verhaltensüberwachung, 6-8
Erweiterte Berechtigungen
konfigurieren, 10-13
Speichergeräte, 10-6–10-8
EXE-Dateiinfektor, 7-4
Externe Geräte
Zugriff verwalten, 10-11, 10-16
Externe Geräte, Schutz, 6-8

F

FakeAV, 7-49
Fehlerbehebung
Plug-in Manager, 17-13
file reputation, 4-3
File-Reputation-Dienste, 4-3
firewall, 5-4, 5-7, 13-2
Aufgaben, 13-9
Ausbruchsmonitor, 13-6
Ausnahmen der Standardrichtlinie, 13-15
Berechtigungen, 13-6, 13-26
Deaktivieren, 13-6
Profile, 13-4, 13-19
Richtlinien, 13-9
Richtlinienausnahmen, 13-14
Testen, 13-36
Firewall-Protokollzähler, 13-29
Fortgeschrittenes Bedrohungskorrelationsmuster, 6-6
Fortgeschrittenes Bedrohungssuchmaschine, 6-6
Fragmentiertes IGMP, 13-5
Fragment zu groß, 13-4
FTP, 11-30

G

Gateway-IP-Adresse, 15-3
Gerätesteuerung, 1-11, 10-2, 10-4, 10-6–10-11, 10-13, 10-14, 10-16
Benachrichtigungen, 10-19
Berechtigungen, 10-4, 10-6–10-9, 10-11
Programmpfad und -name, 10-9
Erweiterte Berechtigungen, 10-13
konfigurieren, 10-13
Externe Geräte, 10-11, 10-16
Liste 'Zulässig', 10-14
Nicht-Speichergeräte, 10-11
Platzhalter, 10-10
Protokolle, 10-19, 18-10
Provider der digitalen Signatur, 10-9
Speichergeräte, 10-4, 10-6–10-8
USB-Geräte, 10-14
Voraussetzungen, 10-2
Zugriff verwalten, 10-11, 10-16

Gerätesteuerung;Gerätesteuerungsliste;Gerätesteuerungsliste:Programme hinzufügen, 10-17

H

Herkömmliche Suche, 7-10
Hotfixes, 6-11
hot fixes, 6-57
HTML-Virus, 7-4
HTTP und HTTPS, 11-30

I

IDS, 13-4
IM-Anwendungen, 11-30
Import von Gateway-Einstellungen, 15-5
Inaktive Agents, 15-27
Inkrementelles Pattern, 6-22
installation, 5-2
    agent, 5-2
    Einhaltung von Sicherheitsrichtlinien, 5-64
    Plug-in Manager, 17-3
    Plug-in-Programm, 17-5
Installation
    Datenschutz, 3-2
Integrierter Server, 4-7
Integrierter Smart Protection Server, 4-18
    ptngrowth.ini, 4-18
    update, 4-19, 4-20
        Komponenten, 4-20
    Websperrliste, 4-21
Intelligente Suche, 7-10
IntelliScan, 7-30
IntelliTrap Ausnahme-Pattern, 6-4
IntelliTrap Pattern, 6-4
Internet-Bedrohungen, 12-2
intranet, 4-13
Intrusion Detection System, 13-4
IPv6, 4-23
    support, 4-23
IPv6-Unterstützung, A-2
    Einschränkungen, A-3, A-4
    IPv6-Adressen anzeigen, A-7
IpXfer.exe, 15-24

J

JavaScript-Virus, 7-4
Jetzt aktualisieren, 6-51
Jetzt durchsuchen, 7-25

K

Kennwort, 14-68
Kerndienst der Verhaltensüberwachung, 6-8
Komponenten, 2-35, 5-73, 6-2
    Aktualisieren der Übersicht, 6-68
    auf dem Agent, 6-29
    Auf dem OfficeScan Server, 6-16
    Auf dem Update-Agent, 6-59
    Update-Berechtigungen und -Einstellungen, 6-49
Komponentenduplizierung, 6-22, 6-65
Komprimierte Dateien, 7-31, 7-84
    Dekomprimierungsregeln, 11-47
Kontinuität des Schutzes, 4-11
Kriterien
    Benutzerdefinierte Ausdrücke, 11-8, 11-9
    Schlüsselwörter, 11-17–11-19

L

LAND Attack, 13-6
Liste 'Zulässig', 7-57
Liste der gesperrten Programme, 9-10
Liste der zulässigen Programme, 9-10
Lizenzen, 14-51

Datenschutz, 3-4
status, 2-6
location awareness, 15-2
logische Operatoren, 11-23
LogServer.exe, 18-3, 18-15

M

MAC-Adresse, 15-3
mail scan, 7-71
Makrovirus, 7-4
Manuelle Agent-Gruppierung, 2-55
Manuelle Suche, 7-20
Verknüpfung, 7-81
Maschine für Kontextbezogene Intelligenz, 6-5
Microsoft Exchange Server, Suche, 7-82
Microsoft SMS, 5-14, 5-33
migration
Von Antiviren-Programmen anderer Hersteller, 5-67
Von ServerProtect Normal Servern, 5-68
MSI-Paket, 5-14, 5-31, 5-33
Muster der Programmsinspektionsüberwachung, 6-9
Muster für kontextbezogene Intelligenz, 6-5

N

NetBIOS, 2-55
Network VirusWall Enforcer, 4-32
Netzwerkkanäle, 11-27, 11-28, 11-30–11-32, 11-34, 11-35, 11-45
E-Mail-Clients, 11-28
FTP, 11-30
HTTP und HTTPS, 11-30
IM-Anwendungen, 11-30
Nicht überwachte Ziele, 11-35, 11-45
SMB-Protokoll, 11-31
übertragungsumfang
alle übertragungen, 11-32
externe übertragungen, 11-34
Übertragungsumfang, 11-35
Konflikte, 11-35
übertragungsumfang und Ziele, 11-32
Überwachte Ziele, 11-35, 11-45
webmail, 11-32
Netzwerkvirus, 7-4, 13-3
Nicht erreichbare Agents, 15-49
Nicht-Speichergeräte
Berechtigungen, 10-11
nicht überwachte E-Mail-Domänen, 11-28
nicht überwachte Ziele, 11-32, 11-34

O

OfficeScan
agent, 1-13
Agent-Dienste, 15-12
Datenbank, Suche, 7-82
Datenbanksicherung, 14-54
Dokumentation, xii
Info über, 1-2
Komponenten, 2-35, 6-2
Komponenten-Update, 5-73
Lizenzen, 14-51
Programme, 2-35
Protokolle, 14-47
Webkonsole, 2-2
webserver, 14-61
Wichtigste Funktionen und Vorteile, 1-7
OfficeScan agent
Verbindung mit OfficeScan Server, 15-29
OfficeScan Agent
Dateien durchsuchen, 15-15

Deinstallation, 5-74
Detaillierte Agent-Informationen, 15-60
Einstellungen importieren und exportieren, 15-60
Inaktive Agents, 15-27
Installationsmethoden, 5-12
Prozesse, 15-17
Registrierungsschlüssel, 15-16
Reservierter Festplattenspeicher, 6-52
Verbindung mit OfficeScan Server, 15-44
Verbindung mit Smart Protection Server, 15-45
OfficeScan server, 1-11
Funktionen, 1-11
OfficeScan update, 6-13

P

packer, 7-2
Patches, 6-11
Pattern-Dateien
Agent-Pattern der intelligenten Suche, 4-8
Pattern der intelligenten Suche, 4-9
smart protection, 4-8
Websperrliste, 4-9
Pattern der allgemeinen Firewall, 6-8
Pattern der intelligenten Suche, 4-9
Pattern der Richtliniendurchsetzung, 6-9
Pattern für die Prävention von Angriffen auf Browser, 6-10
Pattern für digitale Signaturen, 6-9, 7-74
Pattern-Relevanzregeln, 6-10
Pattern zum Auslösen der Arbeitsspeichersuche, 6-9
Pattern zur Konfiguration der Verhaltensüberwachung, 6-8
PCRE, 11-8
performance control, 7-33
Performance Tuning Tool, 18-2
Perl Compatible Regular Expressions, 11-8
phishing, E-10
Ping-of-Death, 13-4
Platzhalter, 11-13
Dateiattribute, 11-13
Gerätesteuerung, 10-10
Plug-in Manager, 1-8, 5-6, 5-8, 17-2
Deinstallation, 17-12
Fehlerbehebung, 17-13
installation, 17-3
native Produktfunktionen verwalten, 17-4
Plug-in-Programm
Aktivieren, 3-4, 17-7
deinstallieren, 17-12
installation, 17-5
Ports sperren, 7-124
Prävention gegen Datenverlust
System- und Anwendungskanäle, 11-35, 11-40
Prävention vor Datenverlust, 11-2, 11-3, 11-6
Aktionen, 11-42
Ausdrücke, 11-6–11-9, 11-11
Dateiattribute, 11-11–11-14
Datenbezeichner, 11-6
Dekomprimierungsregeln, 11-47
Kanäle, 11-27
Netzwerkkanäle, 11-27, 11-28, 11-30–11-32, 11-34, 11-35, 11-45
Richtlinien, 11-3, 11-51
Schlüsselwörter, 11-15–11-19, 11-21
System- und Anwendungskanäle, 11-35, 11-36, 11-39, 11-41, 11-42

Vorlagen, 11-22–11-24, 11-26
widgets, 2-23, 2-24
Programme, 2-35, 6-2
Protokolle, 14-47
Agent-Update-Protokolle, 6-55
Firewall-Protokolle, 13-27, 13-28, 13-32, 13-33
Protokolle der Gerätesteuerung, 10-19
Protokolle der zentralen Quarantänewiederherstellung, 7-109
Protokolle zu verdächtigen Dateien, 7-115
Sicherheitsrisiko-Protokolle, 7-101
Spyware-/Grayware-Protokolle, 7-110
Spyware-/Grayware-Wiederherstellungsprotokolle, 7-114
Suchprotokolle, 7-116
Systemereignisprotokolle, 14-45
über, 14-47
Unbekannte Bedrohungen, 8-12
Verbindungsüberprüfungsprotokolle, 15-48
Verhaltensüberwachung, 9-24
Viren-/Malware-Protokolle, 7-80, 7-101
Web-Reputation-Protokolle, 12-23
Provider der digitalen Signatur, 10-9
Angeben, 10-9
Proxy-Einstellungen, 4-32
agents, 4-32
Berechtigungen, 15-55
Für das Update von Server-Komponenten, 6-20
ptngrowth.ini, 4-18

Q

Quarantäne-Manager, 14-70
Quarantäne-Ordner, 7-45, 7-52

R

Ransomware, 7-3
Referenzserver, 14-40
Registerkarten, 2-8
Remote-Installation, 5-13
Ressourcen zur Fehlerbehebung, 18-1
Richtlinien, 11-3
firewall, 13-4, 13-9
Prävention vor Datenverlust, 11-51
web reputation, 12-5
Rollenbasierte Administration, 14-3
Benutzerkonten, 14-3
Benutzerrollen, 14-14
rootkit, 7-3
Rootkit-Erkennung, 6-8

S

Schadensbehebungsmuster, 6-9
Scherzprogramm, 7-2
Schlüsselwörter, 11-6, 11-15
benutzerdefiniert, 11-17–11-19, 11-21
vordefiniert, 11-15, 11-16
ServerProtect, 5-68
Serverprotokolle
Active Directory Protokolle, 18-6
Agent-Gruppierungsprotokolle, 18-7
Agent Packager-Protokolle, 18-8
Debug-Protokoll der Viren-Scan-Engine, 18-19
Debug-Protokolle, 18-3
Debug-Protokolle des ServerProtect Migration Tools, 18-11
Debug-Protokolle von VSEncrypt, 18-11
Komponenten-Update-Protokolle, 18-7
Lokale Installations-/Upgrade-Protokolle, 18-5

Protokolle der Gerätesteuerung, 18-10
Protokolle zum Control Manager MCP Agent, 18-11
Protokolle zur ausgelagerten Serververwaltung, 18-9
Protokolle zur Einhaltung der Sicherheitsrichtlinien, 18-9
Protokolle zur rollenbasierten Administration, 18-6
Protokolle zur Unterstützung von Virtual Desktop, 18-14
Remote-Installations-/Upgrade-Protokolle, 18-5
Web-Reputation-Protokolle, 18-10
Server Tuner, 14-71
Server-Update
Komponentenduplizierung, 6-22
Manuelles Update, 6-27
Protokolle, 6-28
Proxy-Einstellungen, 6-20
Update-Methoden, 6-27
Zeitgesteuertes Update, 6-28
Sicherheits-Patches, 6-11
Sicherheitsrisiken, 7-2, 7-5, 7-6, 7-8
Phishing-Angriffe, E-10
Schutz vor, 1-9
Spyware/Grayware, 7-5, 7-6, 7-8
Sicherheits-Software anderer Anbieter, 5-66
Smart Feedback, 4-3
smart protection, 4-3, 4-6–4-10, 4-23, 4-24
Adresse, 4-7, 4-8
File-Reputation-Dienste, 4-3
Pattern-Dateien, 4-8–4-10
Agent-Pattern der intelligenten Suche, 4-8
Pattern der intelligenten Suche, 4-9
Update-Vorgang, 4-10
Websperrliste, 4-9
Quellen, 4-23, 4-24
IPv6-Unterstützung, 4-23
Protokolle, 4-8
Standorte, 4-24
Vergleich, 4-7
Smart Protection Network, 4-6
Smart Protection Server, 4-7
Umgebung, 4-13
Zahl der Bedrohungen, 4-3
Smart Protection, 4-4, 4-13
File-Reputation-Dienste, 4-3
Web-Reputation-Dienste, 4-3, 4-4
Smart Protection Network, 1-2, 4-6
Smart Protection Server, 4-7, 4-14, 4-17–4-21
Bewährte Methoden, 4-17
Eigenständig, 4-7, 4-18
installation, 4-14
integriert, 4-7, 4-18–4-21
update, 6-15, 6-29
SMB-Protokoll, 11-31
Speichergeräte
Berechtigungen, 10-4
Erweiterte Berechtigungen, 10-6–10-8
Sperren des Malware-Verhaltens, 9-2
spyware/grayware
Mögliche Bedrohungen, 7-7
spyware, 7-5
Wiederherstellen, 7-59
Spyware/Grayware, 7-5, 7-6, 7-8
adware, 7-6
Anwendungen zum Entschlüsseln von Kennwörtern, 7-6
Dialer, 7-6
Hacker-Tools, 7-6

Scherzprogramme, 7-6
Schutz vor, 7-8
Tools für den Remote-Zugriff, 7-6
Spyware/Grayware-Pattern, 6-7
Spyware/Grayware Scan Engine, 6-7
Spyware-Aktivmonitor-Pattern, 6-7
SQL Server Migration Tool, 14-56, 14-60
Konfigurieren, 14-57
Warnmeldung, 14-60
Standorte, 4-32
awareness, 4-32
Statistik der 10 häufigsten Sicherheitsrisiken für vernetzte Endpunkte, 2-34
Suchaktionen, 7-41
spyware/grayware, 7-55
Viren/Malware, 7-84
Suchausschlüsse, 7-34, 7-35
Dateien, 7-39
Dateierweiterungen, 7-40
Verzeichnisse, 7-36
Suchberechtigungen, 7-62
Suche nach Spyware/Grayware
Aktionen, 7-55
Ergebnisse, 7-112
Liste 'Zulässig', 7-57
Suche nach Viren/Malware
Allgemeine Einstellungen, 7-79
Ergebnisse, 7-103
Suchkriterien
Benutzerdefinierte Aktionen für Dateien, 7-30
CPU-Auslastung, 7-33
Dateikomprimierung, 7-31
Zeitplan, 7-34
Zu durchsuchende Dateien, 7-30
Suchmethode, 5-26
Standardeinstellung, 7-9
Suchmethoden
Herkömmliche Suche, 7-11
Intelligente Suche, 7-11
Suchmethoden wechseln, 7-11
Suchtypen, 5-3, 5-6, 7-16
Such-Zwischenspeicher, 7-73
support
Probleme schneller beheben, 19-4
Support-Informationssystem, 2-5, 18-2
SYN-Flooding, 13-5
System- und Anwendungskanäle, 11-27, 11-35, 11-36, 11-39–11-42
CD/DVD, 11-36
Cloud Storage Service, 11-35
Drucker, 11-39
peer-to-peer (P2P), 11-39
PGP-Verschlüsselung, 11-39
Synchronisierungs-Software, 11-41
Wechseldatenträger, 11-40
Windows-Zwischenablage, 11-42
Systemvoraussetzungen
Update-Agent, 6-59

T

Teardrop, 13-5
Testsuche, 5-73
Testversion, 14-51
test virus, 7-3
Tiny Fragment Attack, 13-5
TMPerftool, 18-2
TMTouch.exe, 6-57
touch tool, 6-57
Treiber der Verhaltensüberwachung, 6-8
Treiber für die allgemeine Firewall, 18-20, 18-21
Trojaner, 1-10, 7-3

Trojanisches Pferd, 6-7

U

Überlappendes Fragment, 13-5
überwachte E-Mail-Subdomänen, 11-28
Überwachte Systemereignisse, 9-6
überwachte Ziele, 11-33, 11-34
Unabhängige Agents, 5-6, 5-8
Unbekannte Bedrohungen, 8-12
    Protokolle, 8-12
Unterstützung von Virtual Desktop, 15-84
update
    Smart Protection Server, 6-15, 6-29
Update-Adresse
    agents, 6-32
    OfficeScan server, 6-19
    Update-Agents, 6-61
Update-Agent, 5-4, 5-7, 6-59
    Analysebericht, 6-67
    Komponentenduplizierung, 6-65
    Standard-Update-Adresse, 6-62
    Systemvoraussetzungen, 6-59
    Update-Methoden, 6-66
    Zuweisen, 6-59
Update-Methoden
    agents, 6-40
    OfficeScan server, 6-27
    Update-Agent, 6-66
updates, 4-19, 4-20
    agents, 6-29
    durchsetzen, 6-56
    Integrierter Smart Protection Server, 4-19, 4-20
    OfficeScan Server, 6-16
    Update-Agent, 6-59
URL-Filter-Engine, 6-12
USB-Geräte
    Liste 'Zulässig', 10-14
        konfigurieren, 10-14

V

VBScript-Virus, 7-4
VDI, 15-84
    Protokolle, 18-14
VDI Tool zur Generierung von Prescan-Vorlagen, 15-95
Verbindungsüberprüfung, 15-47
Verhaltensüberwachung, 9-24
    Aktion bei Systemereignissen, 9-8
    Ausschlussliste, 9-10
    Protokolle, 9-24
Verschlüsselte Dateien, 7-51
Viren-Enzyklopädie, 7-5
Viren-Pattern, 6-3, 6-55, 6-56
Viren-Scan-Engine, 6-3
Virensuchtreiber, 6-3
virus/malware, 7-2–7-5
    Bootsektorvirus, 7-4
    Bösartiger ActiveX-Code, 7-4
    Bösartiger Java-Code, 7-4
    COM- und EXE-Dateien-Infektor, 7-4
    Makrovirus, 7-4
    packer, 7-2
    Ransomware, 7-3
    rootkit, 7-3
    Scherzprogramm, 7-2
    test virus, 7-3
    Trojaner, 7-3
    Typen, 7-2–7-5
    VBScript-, JavaScript- oder HTML-Virus, 7-4
    Wahrscheinlich Virus/Malware, 7-5
    Wurm, 7-4
vordefinierte Ausdrücke, 11-6

anzeigen, 11-7
Vordefinierte Schlüsselwörter
Abstand, 11-16
Anzahl der Schlüsselwörter, 11-16
Vordefinierte Vorlagen, 11-22
Vorlagen, 11-22–11-24, 11-26
Bedingungsanweisungen, 11-23
benutzerdefiniert, 11-23, 11-24, 11-26
logische Operatoren, 11-23
vordefiniert, 11-22
Vulnerability Scanner, 5-15, 5-38
DHCP-Einstellungen, 5-48
Effektivität, 5-39
Endpunktbeschreibung abrufen, 5-59
Ping-Einstellungen, 5-62
Produktabfrage, 5-55
Unterstützte Protokolle, 5-57

W

Wahrscheinlich Virus/Malware, 7-5, 7-104
Web-Installationsseite, 5-12
Webkonsole, 1-9, 2-2–2-4
Anmeldekonto, 2-4
banner, 2-4
Info über, 2-2
Kennwort, 2-4
URL, 2-3
Voraussetzungen, 2-3
webmail, 11-32
web reputation, 5-4, 5-7
Protokolle, 18-10
Richtlinien, 12-5
Web Reputation, 1-10, 12-4
Web-Reputation-Dienste, 4-3, 4-4
Websperrliste, 4-9, 4-21
widgets, 2-8, 2-28, 2-29, 2-33, 2-35, 2-36, 17-3
Ausbrüche, 2-33
Widgets, 2-23, 2-24, 2-27, 2-30, 2-32
Agent-Server-Konnektivität, 2-36
Agent-Updates, 2-35
Antivirus-Agent-Konnektivität, 2-30
C &C-Callback-Ereignisse, 2-27
Mit dem Edge-Relais-Server verbundene Agents, 2-32
OfficeScan- und Plug-in-Mashup, 2-29
Prävention vor Datenverlust – Erkennungen im Zeitverlauf, 2-23
Prävention vor Datenverlust – Häufigste Entdeckungen, 2-24
Sicherheitsrisiko-Funde, 2-28
Windows Server Core, B-2
Befehle, B-7
unterstützte Installationsmethoden, B-2
verfügbare Agent-Funktionen, B-6
Windows-Zwischenablage, 11-42
Wurm, 7-4

Z

Zeitgesteuerte Bewertungen, 15-77
Zeitgesteuerte Suche, 7-22
Automatisch beenden, 7-89
Erinnerung, 7-88
Fortsetzen, 7-89
Überspringen und beenden, 7-66, 7-89
Verschieben, 7-88
Zusammenfassung
dashboard, 2-6, 2-8
updates, 6-68
Zusätzliche Diensteinstellungen, 15-6, 15-7

TREND MICRO INCORPORATED

Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland
Tel.: +49 (0) 811 88990-700 Fax: +4981188990799
sales@trendmicro.de marketing@trendmicro.de

www.trendmicro.com

Item Code: OSGMXG8027/170922