

11.0

OfficeScan™

Service Pack 1

Administratorhandbuch

Für große und mittelständische Unternehmen



Endpoint Security



Protected Cloud



Web Security



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

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

Trend Micro, das Trend Micro T-Ball-Logo, OfficeScan, Control Manager, Damage Cleanup Services, eManager, InterScan, Network VirusWall, ScanMail, ServerProtect und TrendLabs sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Produkt- oder Firmennamen können Marken oder eingetragene Marken ihrer Eigentümer sein.

Copyright © 2015. Trend Micro Incorporated. Alle Rechte vorbehalten.

Dokument-Nr.: OSGM116958/150522

Release-Datum: Juni 2015

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	xii
Dokumentationskonventionen	xiii
Begriffe	xiv

Teil I: Einführung und erste Schritte

Kapitel 1: Einführung in OfficeScan

Info über OfficeScan	1-2
Was ist neu in dieser Version?	1-2
Wichtigste Funktionen und Vorteile	1-12
Der OfficeScan Server	1-15
Das OfficeScan Agent	1-16
Integration in Trend Micro Produkte und Services	1-17

Kapitel 2: Erste Schritte in OfficeScan

Die Webkonsole	2-2
Die Dashboard	2-5
Server-Migrationstool	2-34
Active Directory-Integration	2-38
Die OfficeScan Agent-Hierarchie	2-42
OfficeScan Domänen	2-56

Kapitel 3: Erste Schritte mit Datenschutz

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

Teil II: Schützen OfficeScan Agents

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	4-34

Kapitel 5: Den OfficeScan Agent installieren

OfficeScan Agent Erstinstallationen	5-2
Überlegungen zur Installation	5-2
Überlegungen zur Verteilung	5-11
Zu OfficeScan Agent migrieren	5-68
Nach der Installation	5-72
OfficeScan Agent deinstallieren	5-75

Kapitel 6: Schutzfunktionen aktuell halten

OfficeScan Komponenten und Programme	6-2
Update-Übersicht	6-14

OfficeScan Server-Updates	6-17
Updates für den integrierten Smart Protection Server	6-30
OfficeScan Agent Updates	6-30
Update-Agents	6-58
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	7-59
Allgemeine Sucheinstellungen	7-76
Benachrichtigungen bei Sicherheitsrisiken	7-87
Sicherheitsrisiko-Protokolle	7-98
Ausbrüche von Sicherheitsrisiken	7-114

Kapitel 8: Verhaltensüberwachung verwenden

Verhaltensüberwachung	8-2
Einstellungen der globalen Verhaltensüberwachung konfigurieren	8-10
Verhaltensüberwachungsberechtigungen	8-13
Benachrichtigungen der Verhaltensüberwachung für OfficeScan Agent-Benutzer	8-15
Verhaltensüberwachungsprotokolle	8-16

Kapitel 9: Die Gerätesteuerung verwenden

Gerätesteuerung	9-2
Berechtigungen für Speichergeräte	9-4

Berechtigungen für Nicht-Speichergeräte	9-11
Gerätesteuerungsbenachrichtigungen ändern	9-18
Protokolle der Gerätesteuerung	9-19

Kapitel 10: Prävention vor Datenverlust verwenden

Über Prävention vor Datenverlust (DLP)	10-2
Richtlinien für 'Prävention vor Datenverlust'	10-3
Datenbezeichnertypen	10-6
Vorlagen für 'Prävention vor Datenverlust'	10-22
DLP-Kanäle	10-27
Aktionen der Funktion "Prävention vor Datenverlust"	10-41
Ausnahmen für Prävention vor Datenverlust	10-44
Richtlinienkonfiguration der Funktion "Prävention vor Datenverlust"	10-50
Benachrichtigungen der Funktion "Prävention vor Datenverlust"	10-56
Protokolle für 'Prävention vor Datenverlust'	10-61

Kapitel 11: Computer vor Internet-Bedrohungen schützen

Info über Internet-Bedrohungen	11-2
Command & Control-Kontaktalarmdienste	11-2
Web Reputation	11-4
Web-Reputation-Richtlinien	11-5
Verdächtiger Verbindungsdienst	11-13
Benachrichtigungen über Internet-Bedrohungen für Agent-Benutzer	11-17
C&C-Callback-Benachrichtigungen für Administratoren konfigurieren	11-19
C&C-Kontaktalarmbenachrichtigungen für Agent-Benutzer	11-22
C & C-Callback-Ausbrüche	11-23
Protokolle für Internet-Bedrohungen	11-25

Kapitel 12: Die OfficeScan Firewall verwenden

Info über die OfficeScan Firewall	12-2
Die OfficeScan Firewall aktivieren oder deaktivieren	12-7
Firewall-Richtlinien und -Profile	12-9
Firewall-Berechtigungen	12-25
Allgemeine Firewall-Einstellungen	12-27
Benachrichtigungen bei Firewall-Verstößen für OfficeScan Agent-Benutzer	12-30
Firewall-Protokolle	12-31
Ausbrüche bei Firewall-Verstoß	12-33
Die OfficeScan Firewall testen	12-35

Teil III: OfficeScan Server und Agents verwalten

Kapitel 13: Den OfficeScan Server verwalten

Rollenbasierte Administration	13-3
Trend Micro Control Manager	13-25
Einstellungen für Liste der verdächtigen Objekte	13-32
Referenzserver	13-34
Einstellungen für die Administratorbenachrichtigungen	13-36
Systemereignisprotokolle	13-38
Protokollmanagement	13-40
Lizenzen	13-44
OfficeScan Datenbanksicherung	13-47
SQL Server Migration Tool	13-49
Einstellungen des OfficeScan Webservers/Agents	13-54

Kommunikation zwischen Server und Agents	13-55
Kennwort der Webkonsole	13-61
Einstellungen der Webkonsole	13-62
Quarantäne-Manager	13-62
Server Tuner	13-64
Smart Feedback	13-66

Kapitel 14: OfficeScan Agent verwalten

Endpunktspeicherort	14-2
OfficeScan Agent Programmverwaltung	14-6
Agent-Server-Verbindung	14-27
OfficeScan Agent Proxy-Einstellungen	14-52
OfficeScan Agent-Informationen anzeigen	14-57
Agent-Einstellungen importieren und exportieren	14-57
Einhaltung von Sicherheitsrichtlinien	14-59
Unterstützung für Trend Micro Virtual Desktop	14-79
Globale Agent-Einstellungen	14-94
Agent-Berechtigungen und weitere Einstellungen konfigurieren	14-96

Teil IV: Zusätzlichen Schutz bereitstellen

Kapitel 15: Plug-in Manager verwenden

Info über den Plug-in Manager	15-2
Plug-in Manager Installation	15-3
Verwaltung nativer OfficeScan Funktionen	15-4
Plug-in-Programme verwalten	15-4
Plug-in Manager deinstallieren	15-12

Fehlersuche in Plug-in Manager	15-12

Kapitel 16: Ressourcen zur Fehlerbehebung

Support-Informationssystem	16-2
Case Diagnostic Tool	16-2
Trend Micro Performance Tuning Tool	16-2
OfficeScan Serverprotokolle	16-3
OfficeScan Agent Protokolle	16-15

Kapitel 17: Technischer Support

Ressourcen zur Fehlerbehebung	17-2
Kontaktaufnahme mit Trend Micro	17-4
Verdächtige Inhalte an Trend Micro senden	17-5
Sonstige Ressourcen	17-6

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 2008/2012

Unterstützung für Windows Server Core 2008/2012	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 und Windows Server 2012

Informationen zu Windows 8/8.1 und Windows Server 2012	C-2
Internet Explorer 10/11	C-4

Anhang D: OfficeScan Rollback

Rollback des OfficeScan Servers und der OfficeScan Agents	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-3
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
SOCKS 4	E-13
SSL	E-13
SSL-Zertifikat	E-13
TCP	E-13
Telnet	E-14
Trojanerports	E-14

Vertrauenswürdiger Port	E-15
Zwei-Wege-Kommunikation	E-16
UDP	E-16
Dateien, die nicht gesäubert werden können	E-17

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 xii*
- *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 und zum Aktualisieren des Servers und der agents
Administratorhandbuch	Ein PDF-Dokument mit Informationen über die ersten Schritte, die Verfahren zur OfficeScan Agent-Installation und die Verwaltung von OfficeScan Server und agent
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 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.
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
Fettdruck	Menüs und Menübefehle, Schaltflächen, Registerkarten und Optionen
<i>Kursivdruck</i>	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

KONVENTION	BESCHREIBUNG
 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

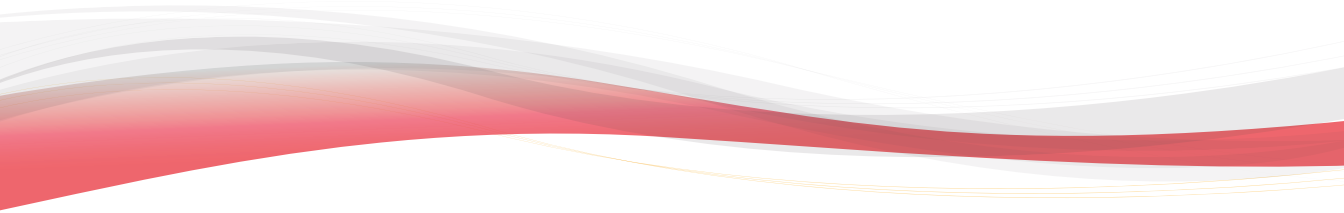
BEGRIFFE	BESCHREIBUNG
OfficeScan Agent	Das OfficeScan agent Programm
Agent Endpunkt	Der Endpunkt, auf dem OfficeScan Agent installiert ist
Agent-Benutzer (oder Benutzer)	Die Person, die den OfficeScan Agent auf dem agent-Endpunkt verwaltet
Server	Das OfficeScan Server-Programm.
Server-Computer	Der Endpunkt, auf dem 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 den agent. Die Konsole für das OfficeScan Server-Programm wird "Webkonsole" und die Konsole für das OfficeScan Agent-Programm wird "agent-Konsole" genannt.

BEGRIFFE	BESCHREIBUNG
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 Dienste	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.
Installationsordner des Agents	Der Ordner auf dem Endpunkt, in dem die OfficeScan Agent-Dateien enthalten sind. 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, in dem die OfficeScan Server-Dateien enthalten sind. 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.

BEGRIFFE	BESCHREIBUNG
agent der herkömmlichen Suche:	Ein OfficeScan Agent wurde so konfiguriert, dass die herkömmliche Suche verwendet wird.
Dual-stack	Elemente, die sowohl über IPv4- als auch IPv6-Adressen verfügen. Beispiel: • Endpunkte, die sowohl über IPv4- als auch IPv6-Adressen verfügen • OfficeScan Agents auf einem Dual-Stack installiert • Endpunkte • 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 dieser Version? auf Seite 1-2*
- *Wichtigste Funktionen und Vorteile auf Seite 1-12*
- *Der OfficeScan Server auf Seite 1-15*
- *Das OfficeScan Agent auf Seite 1-16*
- *Integration in Trend Micro Produkte und Services auf Seite 1-17*

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 dieser Version?

Trend Micro OfficeScan umfasst die folgenden neuen Funktionen und Erweiterungen:

Neu in OfficeScan 11.0 SP1

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

FUNKTION	BESCHREIBUNG
Ransomware-Schutz für Dokumente	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.
Verbesserte 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 Sicherheitsbestimmungen einzuhalten.
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.
Überwachung bei der Suche	OfficeScan bietet mehr Transparenz und Kontrolle über Suchfunktionen anhand: • Zur Wiederaufnahme von unterbrochenen zeitgesteuerten Suchvorgängen: Konfigurieren Sie OfficeScan, um unterbrochene zeitgesteuerten Suchvorgänge basierend auf einem konfigurierten Zeitplan wiederaufzunehmen • Protokolle zu Suchvorgängen: Überwachen Sie die Uhrzeit, den Status und die Ergebnisse der Suche unter Verwendung der Webkonsole
Verschlüsselung von vertraulichen Daten	Prävention vor Datenverlust lässt sich in Trend Micro™ Endpoint Encryption™ integrieren, wodurch die Verschlüsselung von vertraulichen Daten über Wechselspeicher- und Cloud-Speicherkanäle automatisiert wird.

FUNKTION	BESCHREIBUNG
Verbesserte OfficeScan Agent Eigenschutzfunktionen	• Dank verbesserter Überwachung der Dateiintegrität und dem Schutz vor DLL-Hijacking kann die Gültigkeit und Verfügbarkeit von OfficeScan Agent Programmdateien sichergestellt werden. • Schutz vor der Sperrung von OfficeScan Agent Prozessen
OfficeScan Agent Unterstützung für mehrere Sprachen	Administratoren können die OfficeScan Agent Programmsprache über die Webkonsole konfigurieren. Wählen Sie die Anzeige der OfficeScan Agent Konsole basierend auf den Spracheinstellungen oder den OfficeScan Server-Spracheinstellungen des angemeldeten Benutzers aus.
Erweiterte Richtlinienverwaltung über Control Manager™	• Mit der Control Manager™ Richtlinienverwaltung des OfficeScan Servers können Administratoren jetzt untergeordnete Richtlinien erstellen, die auf die globalen Control Manager-Einstellungen übertragen werden. Über die Control Manager-Konsole können lokale OfficeScan Administratoren diese untergeordneten Richtlinien ändern, um verbesserten Schutz für regionale, Abteilungs- oder Satellitenserver zu gewährleisten, für die spezifischere Einstellungen erforderlich sind. Neben den vom Control Manager-Administrator konfigurierten Sicherheitseinstellungen können lokale OfficeScan Administratoren Zeiten für die zeitgesteuerte Suche ändern und Ausnahmelisten durchsuchen, um ihre lokalen Umgebungen besser zu schützen. • Control Manager™ Administratoren können bestimmte OfficeScan Agent-Endpunkte aus dem Netzwerk unter Quarantäne stellen, um die Verbreitung von Sicherheitsbedrohungen zu verhindern. Einzelheiten zur OfficeScan Richtlinienkonfiguration unter Verwendung von Control Manager™ finden Sie im <i>Administratorhandbuch für Trend Micro Control Manager</i>.
Vertrauenswürdige Programme	Administratoren können OfficeScan konfigurieren, um von vertrauenswürdigen Unternehmen signierte Dateien und Prozesse von der Suche auszuschließen und um die konfigurierte Ausschlussliste auf die Echtzeitsuche und Verhaltensüberwachung anzuwenden bzw. um bestimmte Listen für jeden Suchtyp zu erstellen.

Eine Liste der Systemanforderungen finden Sie im Dokument *OfficeScan Systemanforderungen* unter:

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

Neu in OfficeScan 11.0

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

TABELLE 1-1. Verbesserungen beim Server

FUNKTION	BESCHREIBUNG
SQL Database Migration Tool	Administratoren können die vorhandene CodeBase®-Serverdatenbank zu einer SQL Server-Datenbank migrieren. Weitere Informationen finden Sie unter SQL Server Migration Tool auf Seite 13-49 .
Verbesserungen bei Smart Protection Server	In dieser Version von OfficeScan wird die aktualisierte Version Smart Protection Server 3.0 unterstützt. Der aktualisierte Smart Protection Server weist Verbesserungen der Pattern-Dateien für die File-Reputation-Dienste auf. Die Pattern-Dateien wurden optimiert und bieten folgende Vorteile: • Geringerer Arbeitsspeicherbedarf • Inkrementelle Pattern-Updates und verbesserte Erkennung der Pattern für File-Reputation-Dienste, wodurch die Bandbreitenauslastung erheblich reduziert wird
Serverauthentifizierung	Optimierte Serverauthentifizierungsschlüssel sorgen dafür, dass die gesamte Kommunikation zum und vom Server sicher und vertrauenswürdig ist. Weitere Informationen finden Sie unter Authentifizierung der vom Server gestarteten Kommunikation auf Seite 13-55 .

FUNKTION	BESCHREIBUNG
Verbesserungen bei der rollenbasierten Administration	Die Verbesserungen bei der rollenbasierten Administration vereinfachen die Konfiguration von Rollen und Konten für Administratoren sowie die Integration in Trend Micro™ Control Manager™. Weitere Informationen finden Sie unter Rollenbasierte Administration auf Seite 13-3.
Anforderungen für den Webserver	Diese Version von OfficeScan kann in den Apache 2.2.25 Webserver integriert werden.
Umgestaltung der OfficeScan Server-Schnittstelle	Die OfficeScan-Schnittstelle wurde umgestaltet und ist nun einfacher, besser und moderner. Alle Funktionen aus der Vorgängerversion von OfficeScan Server sind in der aktualisierten Version weiterhin verfügbar. • Übergeordnete Menüelemente schaffen Platz auf dem Bildschirm • Das Menü "Favoriten" vereinfacht das Auffinden häufig verwendeter Bildschirme • Mit Hilfe einer Bildschirmpräsentation der Registerkarten im Fenster Dashboard können Sie Widget-Daten anzeigen, ohne dass Sie die Konsole manuell bedienen müssen
Webbasierte kontextsensitive Online-Hilfe	Auf Grund der webbasierten kontextsensitiven Online-Hilfe haben Administratoren stets Zugriff auf die aktuellsten Informationen im Hilfesystem. Falls keine Internet-Verbindung verfügbar ist, wechselt der OfficeScan automatisch zum lokalen Online-Hilfesystem, das im Lieferumfang des Produkts enthalten ist.
Plattform- und Browser-Unterstützung	OfficeScan unterstützt die folgenden Betriebssysteme: • Windows Server™ 2012 R2 (Server und Agent) • Windows 8.1 (nur Agent) OfficeScan unterstützt den folgenden Browser: • Internet Explorer™ 11.0

TABELLE 1-2. Verbesserungen bei Agents

FUNKTION	BESCHREIBUNG
Zentrale Quarantänewiederherstellung	OfficeScan bietet Administratoren die Möglichkeit, zuvor als "verdächtig" eingestufte Dateien wiederherzustellen und Dateien zu "Zugelassen"-Listen auf Domänenebene hinzuzufügen, um weitere Maßnahmen für die Dateien zu verhindern. Falls ein Programm oder eine Datei erkannt wurde und unter Quarantäne gestellt wurde, können Administratoren die Datei global oder individuell auf Agents wiederherstellen. Administratoren können mit Hilfe zusätzlicher SHA1-Überprüfungen sicherstellen, dass die wiederherzustellenden Dateien nicht auf irgendeine Weise geändert wurden. Nach der Wiederherstellung der Dateien kann OfficeScan die Dateien automatisch zu Ausschlusslisten auf Domänenebene hinzufügen, um sie von weiteren Suchen auszuschließen. Weitere Informationen finden Sie unter Dateien in der Quarantäne wiederherstellen auf Seite 7-47.
Erweiterter Schutzdienst	Der erweiterte Schutzdienst weist die folgenden neuen Suchfunktionen auf. - Die Verhinderung von Browser-Schwachstellen verwendet Sandbox-Technologie, um das Verhalten von Webseiten in Echtzeit zu testen und bösartige Skripts oder Programme zu erkennen, bevor der OfficeScan Agent Bedrohungen ausgesetzt wird. Weitere Informationen finden Sie unter Eine Web-Reputation-Richtlinie konfigurieren auf Seite 11-5. - Die verbesserte Arbeitsspeichersuche wird in Kombination mit der Verhaltensüberwachung verwendet, um Malware-Varianten während der Echtzeitsuche zu erkennen und Quarantänemaßnahmen gegen Bedrohungen zu ergreifen. Weitere Informationen finden Sie unter Sucheinstellungen auf Seite 7-30.

FUNKTION	BESCHREIBUNG
Verbesserungen bei OfficeScan Datenschutz	OfficeScan Datenschutz wurde optimiert und bietet folgende Vorteile: • Datenerkennung durch Integration in Control Manager™: Administratoren können Richtlinien für die Prävention vor Datenverlust in Control Manager konfigurieren, um Ordner auf OfficeScan Agents nach sensiblen Dateien zu durchsuchen. Wenn vertrauliche Daten in einer Datei gefunden wurden, kann Control Manager den Speicherort der Datei protokollieren oder aber über die Integration in Trend Micro Endpoint Encryption die Datei auf dem OfficeScan Agent automatisch verschlüsseln. • Unterstützung von Benutzerrechtfertigungen: Administratoren können Benutzern erlauben, Gründe für die Übertragung vertraulicher Daten anzugeben, oder die Übertragungen selbst sperren. OfficeScan protokolliert alle Übertragungsversuche und die vom Benutzer angegebenen Gründe. Weitere Informationen finden Sie unter Aktionen der Funktion "Prävention vor Datenverlust" auf Seite 10-41. • Unterstützung von Smartphones und Tablets: Die Prävention vor Datenverlust und die Gerätesteuerung können nun vertrauliche Daten, die an Smartphones und Tablets gesendet werden, überwachen und entsprechende Maßnahmen ergreifen oder aber den Zugriff auf solche Geräte vollständig sperren. Weitere Informationen finden Sie unter Gerätesteuerung auf Seite 9-2. • Aktualisierte Datenbezeichner- und Vorlagebibliotheken: Die Bibliotheken für die Prävention vor Datenverlust wurden um 2 neue Schlüsselwortlisten und 93 neue Vorlagen erweitert. • Integration der Gerätesteuerungsprotokolle in Control Manager™

FUNKTION	BESCHREIBUNG
Verbesserungen bei "Verdächtige Verbindungseinstellungen"	Command & Control (C&C)-Kontaktalarmdienste wurden aktualisiert und enthalten nun Folgendes: • Globale benutzerdefinierte Liste mit zulässigen und gesperrten IP-Adressen Weitere Informationen finden Sie unter Globale Einstellungen für die benutzerdefinierte IP-Liste konfigurieren auf Seite 11-14. • Malware-Fingerabdruck für Netzwerk zur Erkennung von C&C-Callbacks • Detaillierte Konfiguration von Aktionen, wenn verdächtige Verbindungen erkannt werden Weitere Informationen finden Sie unter Verdächtige Verbindungseinstellungen konfigurieren auf Seite 11-15. • C&C-Server- und agent-Protokolle zeichnen den für C&C-Callbacks verantwortlichen Prozess auf
Verbesserungen bei der Ausbruchsprävention	Die Ausbruchsprävention wurde aktualisiert und bietet nun Schutz vor Folgendem: • Ausführbare komprimierte Dateien Weitere Informationen finden Sie unter Zugriff auf ausführbare komprimierte Dateien verweigern auf Seite 7-125. • Mutex-Prozesse Weitere Informationen finden Sie unter Mutex-Behandlung von Malware-Prozessen/-Dateien auf Seite 7-124.

FUNKTION	BESCHREIBUNG
Verbesserungen bei der Eigenschutzfunktion	Die in dieser Version verfügbaren Eigenschutzfunktionen bieten sowohl eine schlanke Sicherheitslösung als auch eine leistungsfähige Sicherheitslösung, um Ihren Server und Ihre OfficeScan Agent-Programme zu schützen. • Schlanke Sicherheitslösung: Diese Lösung ist für Serverplattformen gedacht, um OfficeScan Agent-Prozesse und Registrierungsschlüssel standardmäßig zu schützen, ohne die Leistung des Servers zu beeinträchtigen • Leistungsfähige Sicherheitslösung: Diese Lösung erweitert die in Vorgängerversionen verfügbare Eigenschutzfunktion des Agents um Folgendes: • IPC-Befehlsauthentifizierung • Schutz und Überprüfung der Pattern-Dateien • Update-Schutz der Pattern-Dateien • Schutz des Verhaltensüberwachungsprozesses Weitere Informationen finden Sie unter OfficeScan Agent Eigenschutz auf Seite 14-13.

FUNKTION	BESCHREIBUNG
Verbesserungen bei der Suchleistung und der Erkennung	• Die Echtzeitsuche verwaltet einen permanenten Such-Zwischenspeicher, 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. • Diese Version von OfficeScan enthält allgemein zulässige Listen für Windows-Systemdateien, für digital signierte Dateien aus zuverlässigen Quellen und für mit Trend Micro getestete Dateien. Nachdem überprüft wurde, dass eine Datei sicher ist, führt OfficeScan keine Aktionen für die Datei aus. • Verbesserungen bei Damage Cleanup Services ermöglichen die verbesserte Erkennung von Rootkit-Bedrohungen und eine geringere Anzahl von Fehlalarmen durch die aktualisierte GeneriClean-Suchfunktion. • Die Einstellungen für komprimierte Dateien sind in die Echtzeitsuche und die On-Demand-Suche unterteilt, um die Leistung zu verbessern. Weitere Informationen finden Sie unter Sucheinstellungen für große, komprimierte Dateien konfigurieren auf Seite 7-79. • Zweischichtige Protokolle ermöglichen eine detailliertere Darstellung von Erkennungen, die Administratoren weiter analysieren möchten.
Umgestaltung der OfficeScan Agent-Schnittstelle	Die OfficeScan Agent-Schnittstelle wurde umgestaltet und ist nun einfacher, besser und moderner. Alle Funktionen aus der Vorgängerversion des OfficeScan Client-Programms sind in der aktualisierten Version weiterhin verfügbar. Mit der aktualisierten Schnittstelle können Administratoren außerdem administrative Funktionen direkt in der OfficeScan Agent-Konsole "entsperren", um Probleme schnell zu beheben, ohne die Webkonsole zu öffnen.

Wichtigste Funktionen und Vorteile

OfficeScan bietet die folgenden Funktionen und Vorteile.

TABELLE 1-3. Wichtigste Funktionen und Vorteile

FUNKTION	VORTEILE
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
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.

FUNKTION	VORTEILE
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.
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.

FUNKTION	VORTEILE
Web Reputation	Die Web-Reputation-Technologie schützt agent-Computer innerhalb oder außerhalb des Unternehmensnetzwerks proaktiv vor bössartigen und potenziell gefährlichen Websites. Web Reputation durchbricht die Infektionskette und verhindert den Download bössartigen Codes. 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.
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 Übertragungskkanäle 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 1-4. Produkte und Services, die mit OfficeScan integriert werden können

PRODUKT/ SERVICE	BESCHREIBUNG	VERSION
ActiveUpdate Server	Liefert alle Komponenten, die der OfficeScan Agent benötigt, um agents 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.	• 6.0 SP3 (empfohlen) • 6.0 SP2 • 6.0 SP1 • 6.0 • 5.5 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 Attacks 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*
- *Server-Migrationstool auf Seite 2-34*
- *Active Directory-Integration auf Seite 2-38*
- *Die OfficeScan Agent-Hierarchie auf Seite 2-42*
- *OfficeScan Domänen auf Seite 2-56*

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 auf Seite 13-62](#).

Über die Webkonsole können Sie folgende Aktionen ausführen:

- Die auf den Netzwerkcomputern installierten agents verwalten
- agents zur gleichzeitigen Konfiguration und Verwaltung in logische Domänen gruppieren
- Auf einem oder mehreren Netzwerkcomputern 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 oder Windows Server 2012 im Windows-Benutzeroberflächen-Modus wird von der Webkonsole nicht unterstützt.

Voraussetzungen für das Öffnen der Web-Konsole

Öffnen Sie die Webkonsole von einem Endpunkt im Netzwerk aus, 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 1024 x 768 bei 256 Farben oder mehr
- Microsoft Internet Explorer™ 8.0 (oder höher)



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://<OfficeScan Server FQDN oder IP-Adresse>/OfficeScan
Mit SSL am virtuellen Standort	https://<OfficeScan Server FQDN oder IP-Adresse:<HTTP-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 des Browsers und aller Proxy-Server zwischen dem OfficeScan Server und dem Endpunkt, 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 13-3*.

Das Banner der Webkonsole

Im Bannerbereich der Webkonsole sind die folgenden Optionen verfügbar:

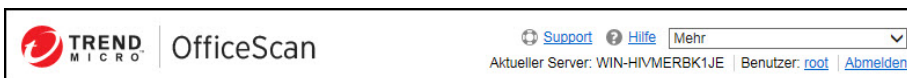


ABBILDUNG 2-1. Der Bannerbereich der Webkonsole

- **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.
- **Hilfe:** Zeigt die Webseite für die Online-Hilfe an.
- **Mehr**
 - **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 16-2](#).

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

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 13-3](#).

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.

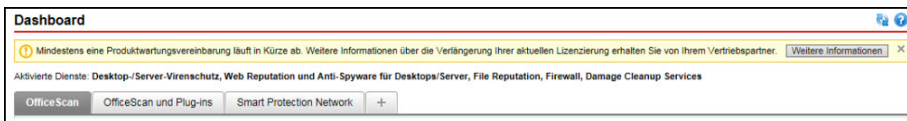


ABBILDUNG 2-2. Abschnitt Status der Produktlizenz

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 verwendete 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 13-66](#).

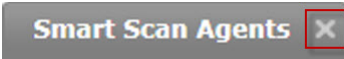
Registerkarten stellen einen Container für Widgets zur Verfügung. Die **Dashboard** unterstützt bis zu 30 Registerkarten.

Mit Registerkarten arbeiten

Verwalten Sie Registerkarten, indem Sie die folgenden Aufgaben ausführen:

TABELLE 2-2. Aufgaben zu Registerkarten

AUFGABE	SCHRITTE
Eine neue Registerkarte hinzufügen	- Klicken Sie auf das Symbol "Hinzufügen" oben auf dem Dashboard. Ein neues Fenster wird geöffnet.  - Geben Sie Folgendes ein: Titel: Der Name der Registerkarte Layout: Wählen Sie aus den verfügbaren Layouttypen aus Automatisch anpassen: Aktivieren Sie "Automatisch anpassen", wenn Sie ein Layout mit mehreren Kästchen ausgewählt haben (wie ) , und jedes Kästchen wird nur ein Widget enthalten. Beim automatischen Anpassen werden Widgets an die Größe eines Kästchens angepasst. - Klicken Sie auf Speichern.

AUFGABE	SCHRITTE
Einstellungen von Registerkarten ändern	- Klicken Sie auf Einstellungen Registerkarte in der Ecke oben rechts der Registerkarte. Ein neues Fenster wird geöffnet.  - Ändern Sie den Namen der Registerkarte, das Layout und die Einstellungen für die automatische Anpassung. - Klicken Sie auf Speichern.
Eine Registerkarte verschieben	Verwenden Sie die Drag & Drop-Funktion, um die Position einer Registerkarte zu verändern.
Eine Registerkarte löschen	Klicken Sie auf das Symbol "Löschen" neben dem Registerkartentitel  Wird eine Registerkarte gelöscht, werden alle Widgets in der Registerkarte gelöscht.

Mit Widgets arbeiten

Verwalten Sie Widgets, indem Sie die folgenden Aufgaben ausführen:

TABELLE 2-3. Aufgaben zu Widgets

AUFGABE	SCHRITTE
Bildschirmpräsentation mit Registerkarte wiedergeben	Klicken Sie auf Bildschirmpräsentation mit Registerkarte wiedergeben , um automatisch zwischen Registerkartenansichten zu wechseln.

AUFGABE	SCHRITTE
Ein neues Widget hinzufügen	1. Klicken Sie auf eine Registerkarte. 2. Klicken Sie auf Widgets hinzufügen in der oberen rechten Ecke der Registerkarte. Ein neues Fenster wird geöffnet. 3. Wählen Sie die Widgets aus, die hinzugefügt werden sollen. Eine Liste verfügbarer Widgets finden Sie unter Verfügbare Widgets auf Seite 2-12. • Klicken Sie auf die Anzeigesymbole () im Bereich des Fensters oben rechts, um zwischen der Detailansicht und der Übersichtsansicht umzuschalten. • Links im Fenster befinden sich Widgetkategorien. Wählen Sie eine Kategorie aus, um die Auswahlmöglichkeiten einzugrenzen. • Verwenden Sie das Suchtextfeld im Fenster oben, um nach einem bestimmten Widget zu suchen. 4. Klicken Sie auf Hinzufügen.
Verschieben eines Widgets	Verwenden Sie die Drag & Drop-Funktion, um Widgets an eine andere Position innerhalb der Registerkarte zu verschieben.
Die Größe eines Widgets anpassen	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.

AUFGABE	SCHRITTE
Den Widgettitel bearbeiten	- Klicken Sie auf das Symbol "Bearbeiten" (). Ein neues Fenster wird angezeigt. - Geben Sie einen neuen Titel ein.  Hinweis Bei manchen Widgets, wie OfficeScan and Plug-ins Mashup, können widgetbezogene Elemente geändert werden. - Klicken Sie auf Speichern.
Widgetdaten aktualisieren	Klicken Sie auf das Symbol "Aktualisieren" ().
Ein Widget löschen	Klicken Sie auf das Symbol "Löschen" ().

Vordefinierte Registerkarten und Widgets

Die **Dashboard** verfügt über zahlreiche vordefinierte Registerkarten und Widgets. Sie können diese Registerkarten und Widgets umbenennen oder löschen.

TABELLE 2-4. Standardregisterkarten in der Dashboard

REGISTERKARTEN	BESCHREIBUNG	WIDGETS
OfficeScan	Diese Registerkarte enthält die gleichen Informationen wie das Fenster Dashboard früherer OfficeScan Versionen. Mit dieser Registerkarte können Sie den allgemeinen Schutz vor Sicherheitsrisiken im OfficeScan Netzwerk anzeigen. Sie können, wenn nötig, auch Sofortmaßnahmen ergreifen, beispielsweise bei Ausbrüchen oder abgelaufenen Komponenten.	• Antivirus-Agent-Konnektivität-Widget auf Seite 2-15 • Sicherheitsrisiko-Funde auf Seite 2-20 • Virenausbrüche auf Seite 2-20 • Agent-Updates-Widget auf Seite 2-23

REGISTERKARTEN	BESCHREIBUNG	WIDGETS
OfficeScan und Plug-ins	Diese Registerkarte zeigt, welche Agents die OfficeScan Agent- und Plug-in-Lösungen verwenden. Verwenden Sie diese Registerkarte, um den allgemeinen Sicherheitsstatus von Agents zu bewerten.	OfficeScan- und Plug-in-Mashup-Widget auf Seite 2-24
Smart Protection Network	Diese Registerkarte enthält Informationen des Trend Micro Smart Protection Network, das File-Reputation-Dienste und Web-Reputation-Dienste an OfficeScan Agents sendet.	• Web Reputation – häufigste Bedrohungsquellen auf Seite 2-31 • Web Reputation – am häufigsten bedrohte Benutzer auf Seite 2-32 • File Reputation – Bedrohungskarte-Widget auf Seite 2-33

Verfügbare Widgets

Folgende Widgets sind in dieser Version verfügbar:

TABELLE 2-5. Verfügbare Widgets

WIDGET-NAME	VERFÜGBARKEIT
Agent-Server-Konnektivität	Direkt verfügbar Weitere Informationen finden Sie unter Agent-Server-Konnektivität-Widget auf Seite 2-14 .
Antivirus-Agent-Konnektivität	Direkt verfügbar Weitere Informationen finden Sie unter Antivirus-Agent-Konnektivität-Widget auf Seite 2-15 .

WIDGET-NAME	VERFÜGBARKEIT
Sicherheitsrisiko-Funde	Direkt verfügbar Weitere Informationen finden Sie unter Sicherheitsrisiko-Funde auf Seite 2-20 .
Virenausbrüche	Direkt verfügbar Weitere Informationen finden Sie unter Virenausbrüche auf Seite 2-20 .
Agent-Updates	Direkt verfügbar Weitere Informationen finden Sie unter Agent-Updates-Widget auf Seite 2-23 .
OfficeScan- und Plug-in-Mashup	Direkt verfügbar, zeigt aber nur Daten von OfficeScan Agents an Daten der folgenden Plug-in-Lösungen sind verfügbar, sobald jede Lösung aktiviert ist: • Intrusion Defense Firewall • Unterstützung für Trend Micro Virtual Desktop Weitere Informationen finden Sie unter OfficeScan- und Plug-in-Mashup-Widget auf Seite 2-24 .
Häufigste Vorfälle bei "Prävention vor Datenverlust"	Nach der Aktivierung von OfficeScan Data Protection verfügbar Weitere Informationen finden Sie unter Häufigste Vorfälle bei "Prävention vor Datenverlust" auf Seite 2-25 .
Prävention vor Datenverlust - Vorfälle im Zeitverlauf	Nach der Aktivierung von OfficeScan Data Protection verfügbar Weitere Informationen finden Sie unter Prävention vor Datenverlust - Vorfälle im Zeitverlauf-Widget auf Seite 2-27 .
Web Reputation – häufigste Bedrohungsquellen	Direkt verfügbar Weitere Informationen finden Sie unter Web Reputation – häufigste Bedrohungsquellen auf Seite 2-31 .

WIDGET-NAME	VERFÜGBARKEIT
Web Reputation – am häufigsten bedrohte Benutzer	Direkt verfügbar Weitere Informationen finden Sie unter Web Reputation – am häufigsten bedrohte Benutzer auf Seite 2-32 .
File Reputation – Bedrohungskarte	Direkt verfügbar Weitere Informationen finden Sie unter File Reputation – Bedrohungskarte-Widget auf Seite 2-33 .
C&C-Callback-Ereignisse	Direkt verfügbar Weitere Informationen finden Sie unter C&C-Callback-Ereignisse-Widget auf Seite 2-29 .
IDF Alarmstatus	Nach der Aktivierung von Intrusion Defense Firewall verfügbar. Weitere Informationen über diese Widgets finden Sie in der IDF Dokumentation.
IDF Computerstatus	
IDF Netzwerk-Ereignisverlauf	
IDF System-Ereignisverlauf	

Agent-Server-Konnektivität-Widget

Das **Agent-Server-Konnektivität**-Widget zeigt den Verbindungsstatus der agents mit dem OfficeScan Server an. Daten werden in einer Tabelle und in einem

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

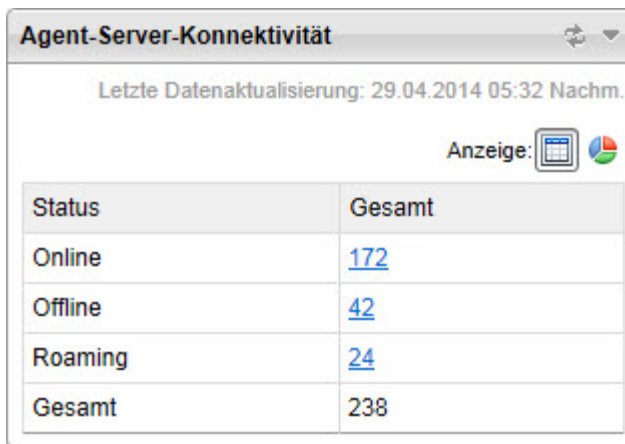


ABBILDUNG 2-3. Agent-Server-Konnektivität-Widget, das eine Tabelle anzeigt

Antivirus-Agent-Konnektivität-Widget

Das **Antivirus-Agent-Konnektivität**-Widget zeigt den Verbindungsstatus der Antivirus-agents mit dem OfficeScan Server an. Daten werden in einer Tabelle und in einem Tortendiagramm angezeigt. Sie können zwischen der Tabelle und dem

Kreisdiagramm umschalten, indem Sie auf das entsprechende Anzeigesymbol klicken ( ).

Antivirus-Agent-Konnektivität

Letzte Datenaktualisierung: 10.04.2014 12:15 Vorm.

Alle ▾ Anzeige:  

Status	Intelligente Suche	Herkömmliche Suche	Gesamt
Online	86	86	172
Offline	21	21	42
Roaming	12	12	24
Gesamt	119	119	238

ABBILDUNG 2-4. Antivirus-Agent-Konnektivität-Widget, das eine Tabelle anzeigt

Antivirus-Agent-Konnektivität-Widget als Tabelle dargestellt

Die Tabelle bricht agents nach der Suchmethode herunter.

Wenn die Anzahl der agents für einen bestimmten Status 1 oder mehr beträgt, können Sie auf die Zahl klicken, um die agents in der agent-Hierarchie anzuzeigen. Anschließend können Sie Tasks für diese agents starten oder ihre Einstellungen ändern.

Um nur agents anzuzeigen, die eine bestimmte Suchmethode verwenden, klicken Sie auf **Alle** und wählen Sie dann die Suchmethode aus.

Antivirus-Agent-Konnektivität	
Letzte Datenaktualisierung: 10.04.2014 12:43 Nachm.	
Herkömmliche Suche ▼	Anzeige:  
Status	Gesamt
Online	86
Offline	21
Roaming	12
Gesamt	119

ABBILDUNG 2-5. Verbindungsstatus von agents mit herkömmlicher Suche

Antivirus-Agent-Konnektivität	
Letzte Datenaktualisierung: 10.04.2014 01:02 Nachm.	
Intelligente Suche ▼	Anzeige:  
Status	Gesamt
[-] Online	86
  Mit einem Smart Protection-Server verbunden	86
 Nicht mit einem Smart Protection-Server verbunden	0
Offline	21
Roaming	12
Gesamt	119

ABBILDUNG 2-6. Verbindungsstatus von agents der intelligenten Suche

Wenn Sie **Intelligente Suche** ausgewählt haben:

- Die Tabelle schlüsselt die Online-agents der intelligenten Suche entsprechend dem Verbindungsstatus mit Smart Protection Servern auf.



Hinweis

Nur Online-agents können den Status ihrer Verbindung mit den Smart Protection Servern melden.

Wenn die Verbindung von agents zu einem Smart Protection Server unterbrochen wird, stellen Sie sie wieder her, indem Sie die Schritte unter [Lösungen für Probleme, die durch OfficeScan Agent-Symbole angezeigt werden auf Seite 14-42](#) durchführen.

- Jeder Smart Protection Server ist ein URL-Link. Die Konsole des Servers wird durch Klicken auf diesen Link gestartet.
- Wenn mehrere Smart Protection Server vorhanden sind, klicken Sie auf **MEHR**. Daraufhin öffnet sich ein neues Fenster, in dem alle Smart Protection Server angezeigt werden.

Smart Protection Server Hilfe

[Übersicht](#) > Smart Protection Server

Smart Protection Server	Verbundene Clients	Konsole
https://192.168.1.100:8443/agent/...	<u>1</u>	Konsole starten
https://192.168.1.101:8443/agent/...	<u>1</u>	Konsole starten
https://192.168.1.102:8443/agent/...	<u>1</u>	Konsole starten

[< Zurück](#)

ABBILDUNG 2-7. Liste der Smart Protection Server

In diesem Fenster können Sie:

- Alle Smart Protection Server anzeigen, mit denen agents eine Verbindung aufbauen, und die Anzahl der agents, die mit jedem Server verbunden sind. Wenn Sie auf die Anzahl klicken, wird die agent-Hierarchie geöffnet, in der Sie die agent-Einstellungen verwalten können.

- Die Serverkonsole aufrufen, indem Sie auf den Link für den Server klicken

Antivirus-Agent-Konnektivität-Widget als Kreisdiagramm dargestellt

Das Kreisdiagramm zeigt nur die Anzahl der agents für jeden Status an und bricht die agents nicht nach Suchmethoden herunter. Durch Anklicken eines Status wird dieser vom Rest des Diagramms ausgeschnitten oder wieder eingefügt.

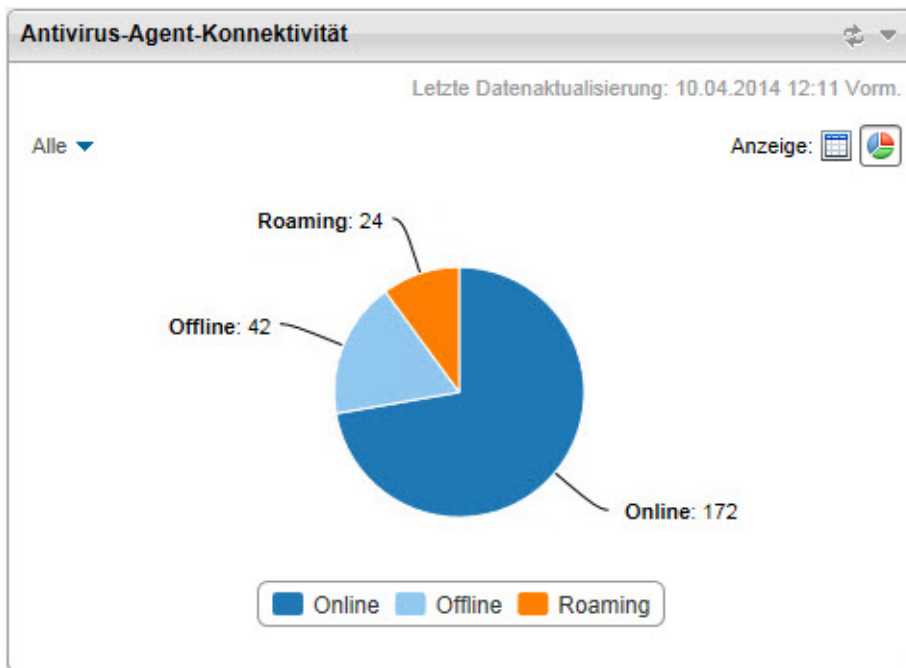


ABBILDUNG 2-8. Antivirus-Agent-Konnektivität-Widget, das ein Kreisdiagramm anzeigt

Sicherheitsrisiko-Funde

Das Widget **Sicherheitsrisiko-Funde** zeigt die Anzahl der Sicherheitsrisiken und der infizierten Endpunkte an.

Erkennung von Sicherheitsrisiken		
Letzte Datenaktualisierung: 10.04.2014 01:30 Vorm.		
Typ	Funde	Endpunkte
Viren/Malware	43	<u>26</u>
Spyware/Grayware	29	<u>17</u>

ABBILDUNG 2-9. Sicherheitsrisiko-Funde

Wenn die Anzahl der infizierten Endpunkte 1 oder mehr beträgt, können Sie auf die Zahl klicken, um die infizierten Endpunkte in der agent-Hierarchie anzuzeigen. Sie können für die OfficeScan Agents auf diesen Endpunkte Aufgaben ausführen oder ihre Einstellungen ändern.

Virenausbrüche

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

Ausbrüche			
Die 10 häufigsten Sicherheitsrisiken anzeigen		Letzte Datenaktualisierung: 10.04.2014 12:33 Vorm.	
Warnung	Typ	Aktueller Ausbruch	Letzter Ausbruch
	Viren/Malware	03/13/2014 22:46:51	01/12/2014 13:12:45
	Firewall-Verstoß	Keine	Keine
	Spyware/Grayware	Keine	Keine
			Zurücksetzen
			Zurücksetzen
			Zurücksetzen

ABBILDUNG 2-10. Virenausbrüche

In diesem Widget können Sie:

- Details zu Ausbrüchen können durch Klicken auf das Datum oder die Zeit der Warnmeldung angezeigt werden.
- Wenn OfficeScan einen Ausbruch erkennt, können Sie den Status der Informationen zu den Ausbruchswarnungen zurücksetzen und sofort Maßnahmen zur Ausbruchsprävention durchsetzen. Weitere Informationen über die Durchsetzung von Maßnahmen zur Ausbruchsprävention finden Sie unter [*Ausbruchpräventionsrichtlinien auf Seite 7-119*](#).
- Klicken Sie auf **Statistik der 10 häufigsten Sicherheitsrisiken anzeigen**, um die am häufigsten auftretenden Sicherheitsrisiken, die Computer mit der höchsten

Anzahl von Sicherheitsrisiken und die häufigsten Infektionsquellen anzuzeigen. Ein neues Fenster wird angezeigt.

Statistik der 10 häufigsten Sicherheitsrisiken für vernetzte Endpunkte



[Dashboard](#) > Statistik der 10 häufigsten Sicherheitsrisiken für vernetzte Endpunkte

Viren-/Malware-Statistik:

Virus/Malware		Infizierte Endpunkte			Infektionsquelle	
Name	Infektionen	Name	Funde	Protokoll	Name	Funde
WINCE_TEST_VIRUS	6	DEXP-PC	57	Anzeigen	10.64.39.115ADMIN	57
Q97M_TEST_VIRUS	6	DEWIN8-PC	27	Anzeigen		
CHM_Test_Virus	3					
P97M_TEST_VIRUS	3					
P2KM_TEST_VIRUS	3					
AM_TEST_VIRUS	3					
A97M_TEST_VIRUS	3					
JS_TEST_VIRUS	3					
HLP_TEST_VIRUS	2					
PALM_TEST_VIRUS	2					

Zuletzt zurückgesetzt am:

[Zähler zurücksetzen](#)

Zuletzt zurückgesetzt am:

[Zähler zurücksetzen](#)

Spyware-/Grayware-Statistik:

Spyware/Grayware		Infizierte Endpunkte		
Name	Infektionen	Name	Funde	Protokoll
SPYW_PKEYLOG.C	1	DEWIN8-PC	9	Anzeigen
Spyware_Test_File	1			
RAP_TEST_FILE	1			
JokePrograms_Test_File	1			
HKTL_TEST_FILE	1			
Dialer_Test_File	1			
CrackingApps_Test_File	1			
Adware_Test_File	1			
SPYCAR_TEST_FILE	1			

Zuletzt zurückgesetzt am:

[Zähler zurücksetzen](#)

Zuletzt zurückgesetzt am:

[Zähler zurücksetzen](#)

ABBILDUNG 2-11. Fenster Statistik der 10 häufigsten Sicherheitsrisiken für vernetzte Endpunkte

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 Namen des Endpunkts),

- die Statistiken in jeder Tabelle zurücksetzen (durch Klicken auf **Zähler zurücksetzen**)

Agent-Updates-Widget

Das **Agent-Updates**-Widget zeigt Komponenten und Programme an, die Netzwerk-Endpunkte vor Sicherheitsrisiken schützen.

Agent-Updates

Online-Agents: 1, Intelligente Suche: 1, Herkömmliche Suche: 0

Letzte Datenaktualisierung: 10.04.2014 12:15 Vorm.

☒ Alle einblenden

☐ Alle ausblenden

☐ Virenschutz	Aktuelle Version	Aktualisiert	Nicht aktuell	Update-Rate
Agent-Pattern der intelligenten Suche	10.597.00	56	5	91%
Viren-Pattern	10.599.00	44	4	91%
IntelliTrap-Pattern	0.172.49	119	0	100%
IntelliTrap Ausnahme-Pattern	0.953.00	119	0	100%
Pattern der Arbeitsspeicherprüfung	1.211.00	0	0	0%
Virus Scan Engine (32-bit)	9.768.1020	119	0	100%
Virus Scan Engine (64-bit)	9.768.1020	0	0	0%
☒ Anti-Spyware				
☐ Damage Cleanup Services	Aktuelle Version	Aktualisiert	Nicht aktuell	Update-Rate
Viren-Cleanup-Template	1356	86	33	72%
Virus Cleanup Engine (32-bit)	7.2.1018	86	33	72%
Virus Cleanup Engine (64-bit)	7.2.1018	0	0	0%
Early Boot Clean Driver (32 Bit)	1.5.1017	86	33	72%
Early Boot Clean Driver (64 Bit)	1.5.1017	86	33	72%
☒ Firewall				
☒ Komponenten der Verhaltensüberwachung				
☒ Lösung für Browser-Schwachstellen				
☒ Verdächtige Verbindungen				
☒ Programm				

ABBILDUNG 2-12. Agent-Updates-Widget

In diesem Widget können Sie:

- Für jede Komponente wird die aktuelle Version angezeigt.
- In der Spalte **Nicht aktuell** die Anzahl der agents mit nicht aktuellen Komponenten einsehen. Falls agents vorliegen, die aktualisiert werden müssen, starten Sie das Update, indem Sie auf die Anzahl klicken.
- Sie können die agents, für die noch kein Upgrade durchgeführt wurde, durch Klicken auf den Link mit der Anzahl des jeweiligen Programms anzeigen.

OfficeScan- und Plug-in-Mashup-Widget

Das **OfficeScan- und Plug-in-Mashup**-Widget verbindet Daten von OfficeScan Agents und installierten Plug-in-Lösungen und stellt diese Daten dann in der agent-Hierarchie dar. Dieses Widget unterstützt Sie dabei, den Schutzbereich der agents schnell zu bewerten und den erforderlichen Verwaltungsaufwand der individuellen Plug-in-Programme zu reduzieren.

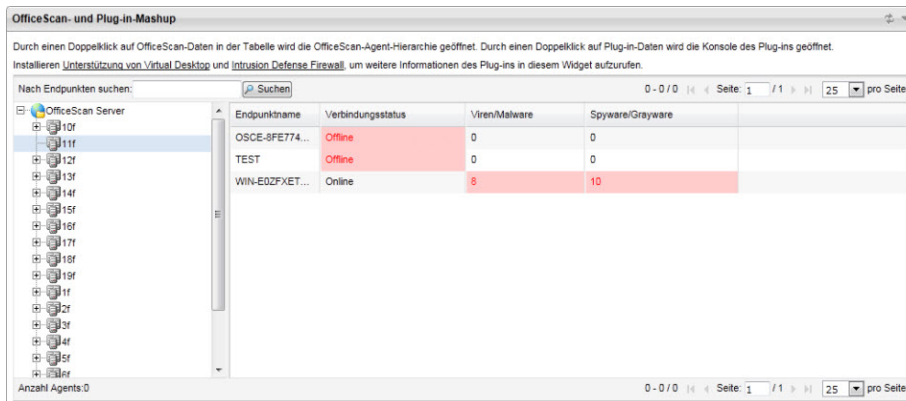


ABBILDUNG 2-13. OfficeScan- und Plug-in-Mashup-Widget

Dieses Widget zeigt jetzt die Daten der folgenden Plug-in-Programme an:

- Intrusion Defense Firewall
- Unterstützung für Trend Micro Virtual Desktop

Diese Plug-in-Programme müssen aktiviert sein, damit das Mashup-Widget Daten anzeigen kann. Aktualisieren Sie die Plug-in-Programme, wenn neuere Versionen verfügbar sind.

In diesem Widget können Sie:

- Die Spalten auswählen, die in der agent-Hierarchie angezeigt werden. Klicken Sie auf das Symbol "Bearbeiten" () in der rechten oberen Ecke des Widgets, und wählen Sie dann im angezeigten Fenster die Spalten aus.

TABELLE 2-6. OfficeScan- und Plug-in-Mashup-Spalten

NAME DER SPALTE	BESCHREIBUNG
Computername	Name des Endpunkts Diese Spalte ist immer verfügbar und kann nicht entfernt werden.
Domänenhierarchie	Die Domäne des Endpunkts in der OfficeScan-agent-Hierarchie
Verbindungsstatus	Die OfficeScan Agent-Verbindung zu seinem übergeordneten OfficeScan Server
Viren/Malware	Die Anzahl der vom OfficeScan Agent entdeckten Viren und Malware
Spyware/Grayware	Die Anzahl der vom OfficeScan Agent entdeckten Spyware und Grayware
VDI Support	Zeigt an, ob der Endpunkt eine virtuelle Maschine ist
IDF Sicherheitsprofil	Weitere Informationen über diese Spalten und die Daten, die sie anzeigen, finden Sie in der IDF Dokumentation.
IDF Firewall	
IDF Alarmstatus	
IDF DPI	

- Doppelklicken Sie auf die Daten in der Tabelle. Wenn Sie auf OfficeScan Daten doppelklicken, wird die OfficeScan-agent-Hierarchie angezeigt. Wenn Sie auf Daten für Plug-in-Programme doppelklicken (mit Ausnahme von Daten in der Spalte **VDI Support**), wird das Hauptfenster des Plug-in-Programms angezeigt.
- Verwenden Sie diese Suchfunktion, um individuelle Endpunkte zu finden. Sie können einen Hostnamen vollständig oder teilweise eingeben.

Häufigste Vorfälle bei "Prävention vor Datenverlust"

Dieses Widget ist nur verfügbar, wenn Sie OfficeScan Datenschutz aktivieren.

Dieses Widget zeigt die Anzahl der Übertragungen digitaler Assets an, unabhängig von der entsprechenden Aktion (sperrern oder übergehen).

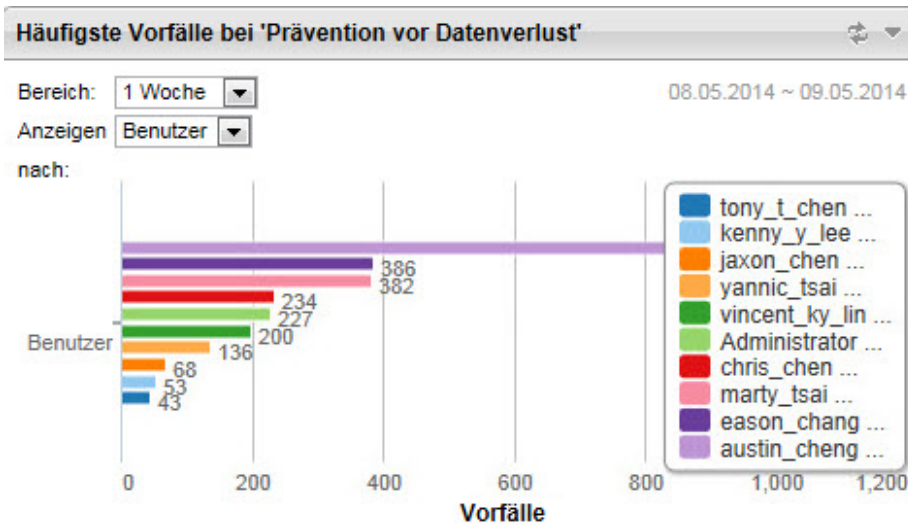


ABBILDUNG 2-14. Häufigste Vorfälle bei "Prävention vor Datenverlust"

Anzeigen von Daten:

- Wählen Sie einen Zeitraum für die Entdeckungen aus. Wählen Sie unter:
 - Heute:** Entdeckungen während der letzten 24 Stunden, einschließlich der aktuellen Stunde
 - 1 Woche:** Entdeckungen während der letzten 7 Tage, einschließlich des aktuellen Tages
 - 2 Wochen:** Entdeckungen während der letzten 14 Tage, einschließlich des aktuellen Tages
 - 1 Monat:** Entdeckungen während der letzten 30 Tage, einschließlich des aktuellen Tages
- Nachdem Sie einen Zeitraum ausgewählt haben, wählen Sie unter:

- **Benutzer:** Benutzer, die Übertragungen digitaler Assets am häufigsten durchführen
- **Kanal:** Kanäle, die am häufigsten für Übertragungen digitaler Assets benutzt werden
- **Vorlage:** Vorlagen für digitale Assets, die die häufigsten Entdeckungen auslösen
- **Computer:** Computer, die Übertragungen digitaler Assets am häufigsten durchführen

**Hinweis**

Dieses Widget zeigt maximal 10 Benutzer, Kanäle, Vorlagen oder Computer an.

Prävention vor Datenverlust - Vorfälle im Zeitverlauf-Widget

Dieses Widget ist nur verfügbar, wenn Sie OfficeScan Datenschutz aktivieren.

Dieses Widget zeichnet die Anzahl der Übertragungen digitaler Assets im Zeitverlauf auf. Die Übertragungen beinhalten auch jene, die gesperrt oder übergangen (zugelassen) wurden.

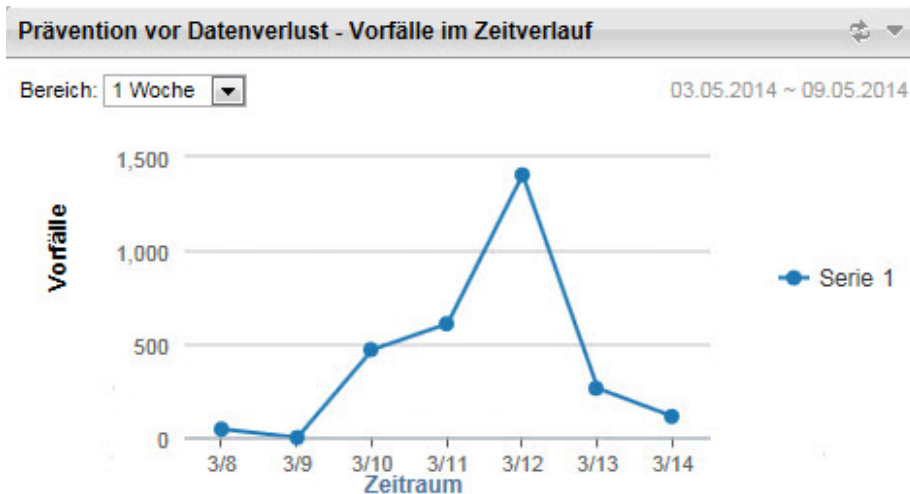


ABBILDUNG 2-15. Prävention vor Datenverlust - Vorfälle im Zeitverlauf-Widget

Wählen Sie einen Zeitraum für die Entdeckungen aus, um die Daten anzuzeigen.
Wählen Sie unter:

- **Heute:** Entdeckungen während der letzten 24 Stunden, einschließlich der aktuellen Stunde
- **1 Woche:** Entdeckungen während der letzten 7 Tage, einschließlich des aktuellen Tages
- **2 Wochen:** Entdeckungen während der letzten 14 Tage, einschließlich des aktuellen Tages
- **1 Monat:** Entdeckungen während der letzten 30 Tage, einschließlich des aktuellen Tages

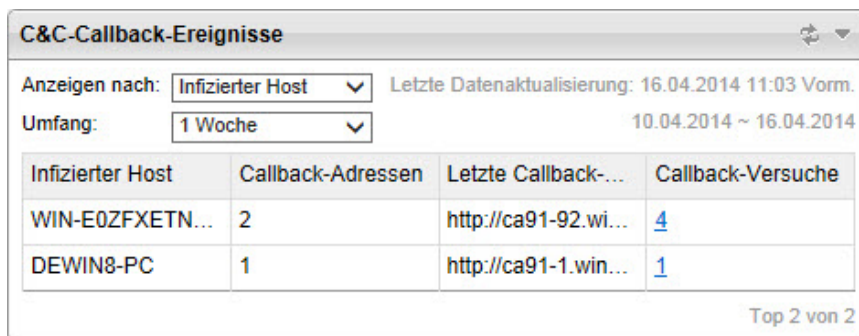
C&C-Callback-Ereignisse-Widget

Das **C&C-Callback-Ereignisse**-Widget zeigt sämtliche C&C-Callback-Ereignisinformationen einschließlich des Ziels eines Angriffs sowie der Callback-Adresse der Quelle an.

Administratoren können nach Bedarf C&C-Callback-Informationen aus einer bestimmten C&C-Serverliste einsehen. Klicken Sie zur Auswahl der Listenquelle (Global Intelligence, Virtual Analyzer) auf das Symbol "Bearbeiten" (⚙️) und wählen Sie die gewünschte Liste im Listenfeld **C&C-Listenquelle** aus.

Wählen Sie Folgendes zur Anzeige der C&C-Callback-Daten aus:

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



The screenshot shows the 'C&C-Callback-Ereignisse' widget. It has a title bar with a refresh icon and a dropdown arrow. Below the title bar, there are two dropdown menus: 'Anzeigen nach:' set to 'Infizierter Host' and 'Umfang:' set to '1 Woche'. To the right of these, it says 'Letzte Datenaktualisierung: 16.04.2014 11:03 Vorm.' and '10.04.2014 ~ 16.04.2014'. The main content is a table with four columns: 'Infizierter Host', 'Callback-Adressen', 'Letzte Callback-...', and 'Callback-Versuche'. The table contains two rows of data. The first row shows 'WIN-E0ZFXETN...' with 2 callback addresses, the last one being 'http://ca91-92.wi...', and 4 attempts. The second row shows 'DEWIN8-PC' with 1 callback address, the last one being 'http://ca91-1.win...', and 1 attempt. At the bottom right of the table, it says 'Top 2 von 2'.

Infizierter Host	Callback-Adressen	Letzte Callback-...	Callback-Versuche
WIN-E0ZFXETN...	2	http://ca91-92.wi...	4
DEWIN8-PC	1	http://ca91-1.win...	1

ABBILDUNG 2-16. C&C-Callback-Ereignisse-Widget mit Angaben zu Angriffszielen

TABELLE 2-7. 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

SPALTE	BESCHREIBUNG
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.

C&C-Callback-Ereignisse				
Anzeigen nach:	Callback-Adresse ▼	Letzte Datenaktualisierung: 16.04.2014 11:06 Vorm.		
Umfang:	1 Woche ▼	10.04.2014 ~ 16.04.2014		
Callback-Adr...	C&C-Risikos...	Infizierte Hosts	Letzter infizi...	Callback-Ver...
http://ca91-9...	Hoch	1	WIN-E0ZFX...	2
http://ca91-9...	Hoch	1	WIN-E0ZFX...	2
http://ca91-9...	Hoch	1	WIN-E0ZFX...	2
http://ca91-1...	Hoch	1	DEWIN8-PC	1
Top 4 von 4				

ABBILDUNG 2-17. C&C-Callback-Ereignisse-Widget mit Angaben zu Callback-Adressen

TABELLE 2-8. 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.

Web Reputation – häufigste Bedrohungsquellen

Dieses Widget zeigt die Anzahl aller Sicherheitsbedrohungen an, die Web-Reputation-Dienste entdeckt hat. Die geographische Lage der Entdeckungen wird auf einer

Weltkarte angezeigt. Um weitere Informationen zur Verwendung dieses Widgets zu erhalten, klicken Sie auf die Schaltfläche Hilfe (?) oben auf dem Widget.

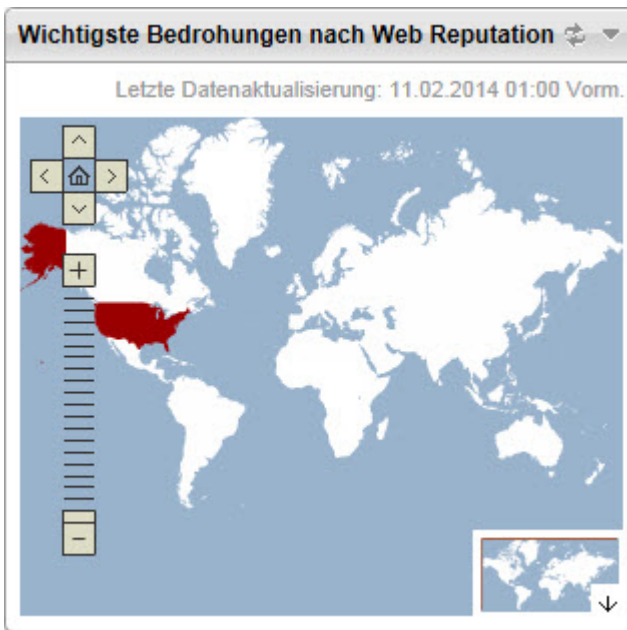


ABBILDUNG 2-18. Web Reputation – häufigste Bedrohungsquellen

Web Reputation – am häufigsten bedrohte Benutzer

Dieses Widget zeigt die von Web-Reputation-Dienste entdeckte Anzahl der Benutzer an, die durch bösartige URLs beeinträchtigt wurden. Die geographische Lage der Entdeckungen wird auf einer Weltkarte angezeigt. Um weitere Informationen zur

Verwendung dieses Widgets zu erhalten, klicken Sie auf die Schaltfläche Hilfe (?) oben auf dem Widget.

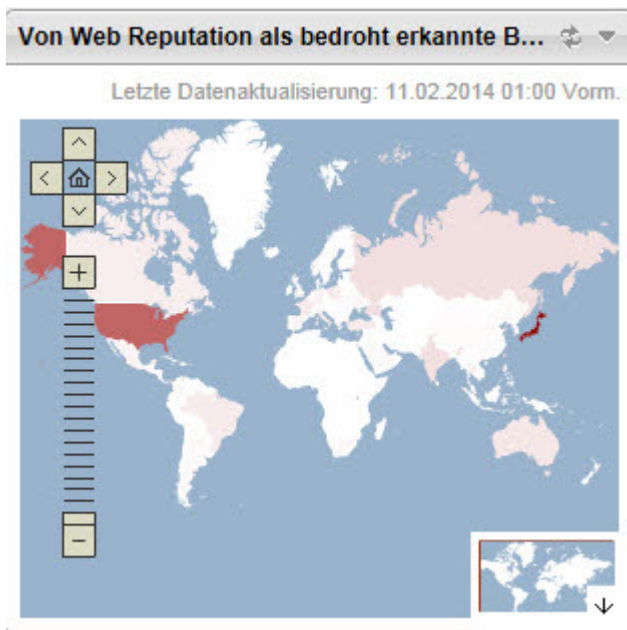


ABBILDUNG 2-19. Web Reputation – am häufigsten bedrohte Benutzer

File Reputation – Bedrohungskarte-Widget

Dieses Widget zeigt die Anzahl aller Sicherheitsbedrohungen an, die File-Reputation-Dienste entdeckt hat. Die geographische Lage der Entdeckungen wird auf einer

Weltkarte angezeigt. Um weitere Informationen zur Verwendung dieses Widgets zu erhalten, klicken Sie auf die Schaltfläche Hilfe (?) oben auf dem Widget.

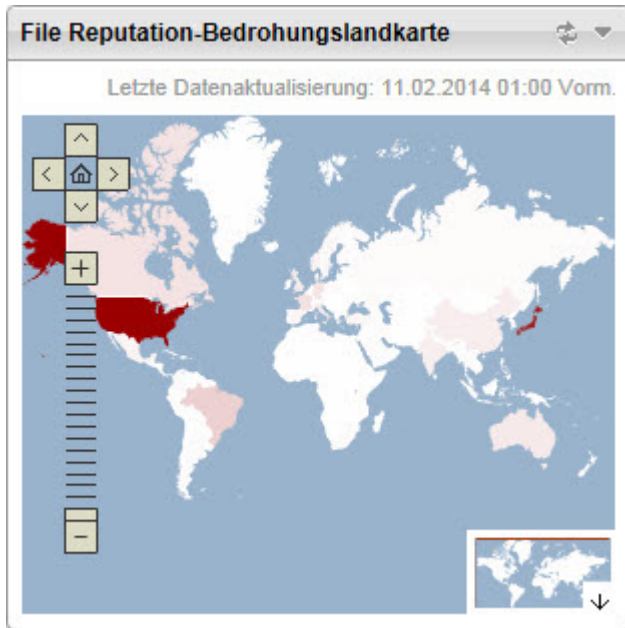


ABBILDUNG 2-20. File Reputation – Bedrohungskarte-Widget

Server-Migrationstool

OfficeScan beinhaltet das Server-Migrationstool, mit dem Administratoren OfficeScan Einstellungen aus früheren OfficeScan Versionen in die aktuelle Version übertragen können. Mit dem Server-Migrationstool werden folgende Einstellungen übertragen:

FUNKTION	MIGRIERTE EINSTELLUNGEN
Agent-Verwaltung	• Einstellungen für die manuelle Suche* • Einstellungen für die zeitgesteuerte Suche* • Einstellungen für die Echtzeitsuche* • Einstellungen für "Jetzt durchsuchen"* • Web-Reputation-Einstellungen* • Einstellungen der Verhaltensüberwachung* • Einstellungen der Gerätesteuerung* • Einstellungen für Prävention vor Datenverlust* • Berechtigungen und andere Einstellungen* • Zusätzliche Diensteinstellungen* • Liste der zulässigen Spyware/Grayware*  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.
Agent-Gruppierung	Alle Einstellungen  Hinweis Die Active-Directory-Domänenstrukturen werden nach dem ersten Synchronisieren mit Active Directory angezeigt.
Globale Agent-Einstellungen	Alle Einstellungen

FUNKTION	MIGRIERTE 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
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 Agent migriert 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.

Server-Migrationstool verwenden

**Hinweis**

Diese Version von OfficeScan unterstützt die Migration aus OfficeScan Version 10.0 oder höher.

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. Navigieren Sie auf dem OfficeScan 11.0 SP1 Server-Computer zu
<*Installationsordner des Servers*>\PCCSRV\Admin\Utility\ServerMigrationTool.
2. Kopieren Sie das Server Migration Tool auf den OfficeScan Server-Computer, der als Quelle fungiert.

**Wichtig**

Sie müssen das OfficeScan 11.0 SP1 Server Migration Tool auf der Version des OfficeScan Quellservers verwenden, um sicherzustellen, dass das Format aller Daten für den neuen Zielservers korrekt ist. OfficeScan 11.0 SP1 ist nicht mit älteren Versionen des Server Migration Tools kompatibel.

3. Doppelklicken Sie auf ServerMigrationTool.exe, um das Server-Migrationstool zu starten.

Das Server-Migrationstool wird geöffnet.

4. So exportieren Sie die Einstellungen aus dem ursprünglichen OfficeScan Server
 - a. Geben Sie über die Schaltfläche **Durchsuchen** den Zielordner an.



Hinweis

Der Standardname des Exportpakets lautet OsceMigrate.zip.

- b. Klicken Sie auf **Exportieren**.
Eine Bestätigungsmeldung wird angezeigt.
 - c. Kopieren Sie das Exportpaket auf den neuen OfficeScan Server.
5. So importieren Sie die Einstellungen in den neuen OfficeScan Server
 - a. Gehen Sie über die Schaltfläche **Durchsuchen** zum Exportpaket.
 - b. Klicken Sie auf **Importieren**.
Eine Warnmeldung wird angezeigt.
 - c. Klicken Sie zum Fortfahren auf **Ja**.
Eine Bestätigungsmeldung wird angezeigt.
6. Vergewissern Sie sich, dass der Server alle Einstellungen aus der früheren OfficeScan Version enthält.
7. Verschieben Sie die alten OfficeScan Agents auf den neuen Server.

Weitere Informationen zum Verschieben von OfficeScan Agents finden Sie unter *OfficeScan Agents in eine andere Domäne oder auf einen anderen OfficeScan Server verschieben auf Seite 2-65* oder *Agent Mover auf Seite 14-24*.

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:

- **Rollenbasierte Administration:** Sie können bestimmte administrative Verantwortlichkeiten Benutzern zuweisen, indem Sie ihnen Zugriff auf die Produktkonsole mit Hilfe ihrer Active Directory-Konten gewähren. Weitere Informationen finden Sie unter [Rollenbasierte Administration auf Seite 13-3](#).
- **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 2-58](#).
- **Nicht verwaltete Endpunkte:** Stellen Sie sicher, dass die Endpunkte im Netzwerk, die nicht vom OfficeScan Server verwaltet werden, die Sicherheitsrichtlinien Ihres Unternehmens einhalten. Weitere Informationen finden Sie unter [Einhaltung der Sicherheitsrichtlinien für nicht verwaltete Endpunkte auf Seite 14-74](#).

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 2-41](#).

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 synchronisieren.
8. Planen Sie regelmäßige Synchronisierungsdurchläufe. Weitere Informationen finden Sie unter [Daten mit Active Directory-Domänen synchronisieren auf Seite 2-41](#).

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 gegenwärtig vom Server verwaltet werden. Agents werden in Domänen

gruppiert, so dass Sie für alle Domänenmitglieder gleichzeitig dieselbe Konfiguration festlegen, verwalten und übernehmen können.

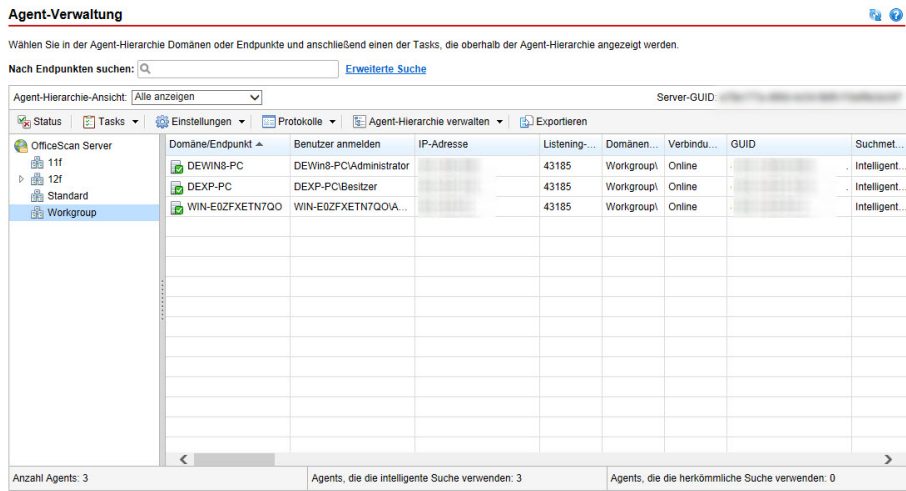


ABBILDUNG 2-21. OfficeScan agent -Hierarchie

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

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

Allgemeine Aufgaben in der Agent-Hierarchie

Die folgende Übersicht enthält die allgemeinen Aufgaben, die Sie in der agent-Hierarchie durchführen können:

Prozedur

- Um alle Domänen und agents auszuwählen, klicken Sie auf das Stammsymbol . Wenn Sie auf das Symbol der Root-Domäne klicken und anschließend eine Aufgabe über der agent-Hierarchie auswählen, wird ein Fenster angezeigt, in dem Sie die Einstellungen konfigurieren können. Wählen Sie aus dem Fenster eine der folgenden allgemeinen Optionen:
 - Auf alle Agents anwenden:** Wendet die Einstellungen auf alle vorhandenen agents und auf alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser

Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

- Mehrere benachbarte Domänen oder agents auswählen:
 - Wählen Sie aus dem rechten Fensterbereich die erste Domäne, halten Sie die UMSCHALT-TASTE gedrückt und klicken Sie anschließend auf die letzte Domäne oder den letzten agent in diesem Bereich.
- Um mehrere nicht unmittelbar aufeinander folgende Domänen oder agents auszuwählen, halten Sie im rechten Fensterbereich die STRG-Taste gedrückt und klicken Sie auf die gewünschten Domänen oder agents.
- Sie können nach einem bestimmten zu verwaltenden agent suchen, indem Sie den Namen des agents im 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

IPv6- oder IPv4-Adressen können nicht angegeben werden, wenn nach bestimmten agents gesucht wird. Verwenden Sie die erweiterte Suche, um nach IPv4- oder IPv6-Adressen zu suchen. Weitere Informationen finden Sie unter [Erweiterte Suchoptionen auf Seite 2-46](#).

- Nach Auswahl einer Domäne wird die agent-Hierarchie erweitert, sodass 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 (herkömmliche oder intelligente Suche), und die Smart Protection Komponenten an.
 - **Update-Agent-Ansicht:** Zeigt Informationen zu allen Update-Agents an, die vom OfficeScan Server verwaltet werden.
 - Sie können agents durch Klicken auf den Spaltennamen nach den Informationen in den Spalten sortieren.
 - Aktualisieren Sie die agent-Hierarchie, indem Sie auf das Symbol "Aktualisieren" () klicken.
 - Unterhalb der agent-Hierarchie werden die agent-Statistiken angezeigt, wie die Gesamtzahl der agents, die Anzahl der agents der intelligenten Suche und die Anzahl der agents der herkömmlichen Suche.
-

Erweiterte Suchoptionen

Suche nach agents basierend auf den folgenden Kriterien:

Prozedur

- **Grundlegende Kriterien:** Umfasst grundlegende Informationen über Endpunkte wie IP-Adresse, Betriebssystem, Domäne, MAC-Adresse, Suchmethode oder 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.

- **Komponentenversion:** 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:** Enthält agent-Einstellungen
- Klicken Sie nach Eingabe Ihrer Suchkriterien auf **Suchen**. In der agent-Hierarchie wird eine Liste der Endpunkt-Namen angezeigt, die die festgelegten Kriterien erfüllen.

Spezifische 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 2-47*
- *Ausbruchsprävention auf Seite 2-51*
- *Fenster Agent-Auswahl auf Seite 2-52*
- *Rollback auf Seite 2-53*
- *Sicherheitsrisiko-Protokolle auf Seite 2-54*

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**).

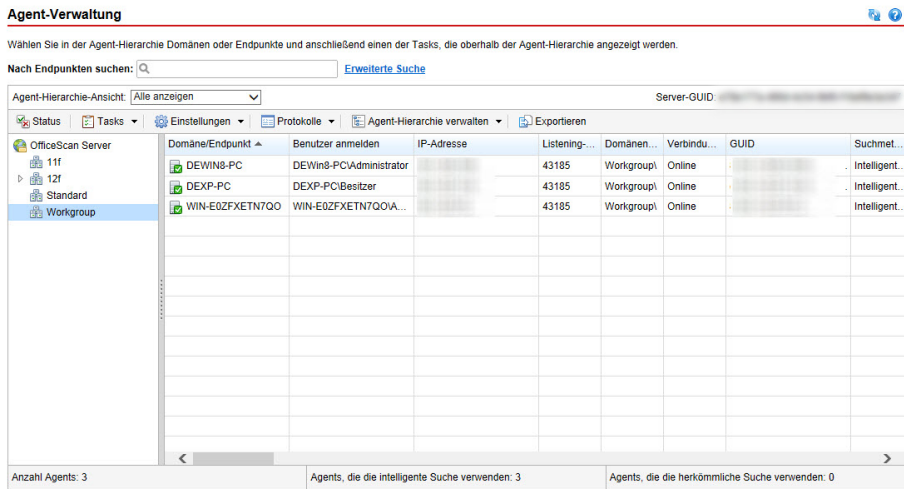


ABBILDUNG 2-22. Fenster Agent-Verwaltung

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 14-57 .
Aufgaben	"Jetzt durchsuchen" auf agent-Computern durchführen. Weitere Informationen finden Sie unter Jetzt durchsuchen starten auf Seite 7-27. - Den agent deinstallieren Weitere Informationen finden Sie unter Den OfficeScan Agent von der Webkonsole aus deinstallieren auf Seite 5-76.

MENÜSCHALTFLÄCHE	AUFGABE
	• Erkannte verdächtige Dateien wiederherstellen. Weitere Informationen finden Sie unter Dateien in der Quarantäne wiederherstellen auf Seite 7-47. • Spyware-/Grayware-Komponenten wiederherstellen. Weitere Informationen finden Sie unter Spyware/Grayware wiederherstellen auf Seite 7-56.
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 11-5. • Verdächtige Verbindungseinstellungen konfigurieren. Weitere Informationen finden Sie unter Verdächtige Verbindungseinstellungen konfigurieren auf Seite 11-15. • Konfigurieren Sie die Einstellungen der Verhaltensüberwachung. Weitere Informationen finden Sie unter Verhaltensüberwachung auf Seite 8-2. • Konfigurieren Sie die Einstellungen der Gerätesteuerung. Weitere Informationen finden Sie unter Gerätesteuerung auf Seite 9-2. • Konfigurieren Sie Richtlinien für die Prävention vor Datenverlust. Weitere Informationen finden Sie unter Richtlinienkonfiguration der Funktion "Prävention vor Datenverlust" auf Seite 10-50. • agents als Update-Agents zuweisen. Weitere Informationen finden Sie unter Konfiguration des Update-Agents auf Seite 6-59.

MENÜSCHALTFLÄCHE	AUFGABE
	• agent-Berechtigungen und andere Einstellungen konfigurieren. Weitere Informationen finden Sie unter Agent-Berechtigungen und weitere Einstellungen konfigurieren auf Seite 14-96. • OfficeScan Agent-Dienste aktivieren oder deaktivieren. Weitere Informationen finden Sie unter OfficeScan Agent Dienste auf Seite 14-7. • Die Liste der zulässigen Spyware/Grayware konfigurieren. Weitere Informationen finden Sie unter Liste der zulässigen Spyware/Grayware auf Seite 7-54. • Liste der vertrauenswürdigen Programme konfigurieren. Weitere Informationen finden Sie unter Liste der vertrauenswürdigen Programme konfigurieren auf Seite 7-58. • agent-Einstellungen importieren und exportieren. Weitere Informationen finden Sie unter Agent-Einstellungen importieren und exportieren auf Seite 14-57.
Protokolle	Die folgenden Protokolle anzeigen: • Viren/Malware-Protokolle (weitere Informationen hierzu finden Sie unter Viren-/Malware-Protokolle anzeigen auf Seite 7-98) • Spyware/Grayware-Protokolle (weitere Informationen hierzu finden Sie unter Spyware/Grayware-Protokolle anzeigen auf Seite 7-107) • Firewall-Protokolle (weitere Informationen hierzu finden Sie unter Firewall-Protokolle auf Seite 12-31) • Web-Reputation-Protokolle (weitere Informationen hierzu finden Sie unter Protokolle für Internet-Bedrohungen auf Seite 11-25) • Protokolle zu verdächtigen Verbindungen (weitere Informationen hierzu finden Sie unter Protokolle zu verdächtigen Verbindungen anzeigen auf Seite 11-29) • Protokolle zu verdächtigen Dateien (weitere Informationen hierzu finden Sie unter Protokolle zu verdächtigen Dateien anzeigen auf Seite 7-111) • C&C-Callback-Protokolle (weitere Informationen hierzu finden Sie unter C&C Callback-Protokolle anzeigen auf Seite 11-27)

MENÜSCHALTFLÄCHE	AUFGABE
	• Verhaltensüberwachungsprotokolle (weitere Informationen hierzu finden Sie unter Verhaltensüberwachungsprotokolle auf Seite 8-16) • Protokolle der Gerätesteuerung (weitere Informationen hierzu finden Sie unter Protokolle der Gerätesteuerung auf Seite 9-19) • DLP-Protokolle (weitere Informationen hierzu finden Sie unter Protokolle für 'Prävention vor Datenverlust' auf Seite 10-61) • Protokolle zu Suchvorgängen (weitere Informationen hierzu finden Sie unter Protokolle zu Suchvorgängen anzeigen auf Seite 7-113) Protokolle löschen. Weitere Informationen finden Sie unter Protokollmanagement auf Seite 13-40.
Agent-Hierarchie verwalten	Die agent-Hierarchie verwalten Weitere Informationen finden Sie unter Aufgaben zur Agent-Gruppierung auf Seite 2-63 .
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 7-118*.

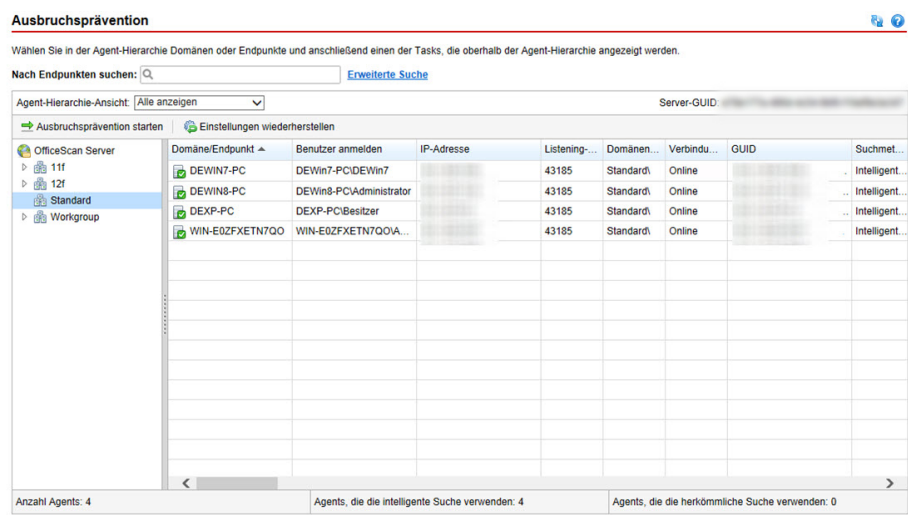


ABBILDUNG 2-23. Ausbruchsprävention

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*.

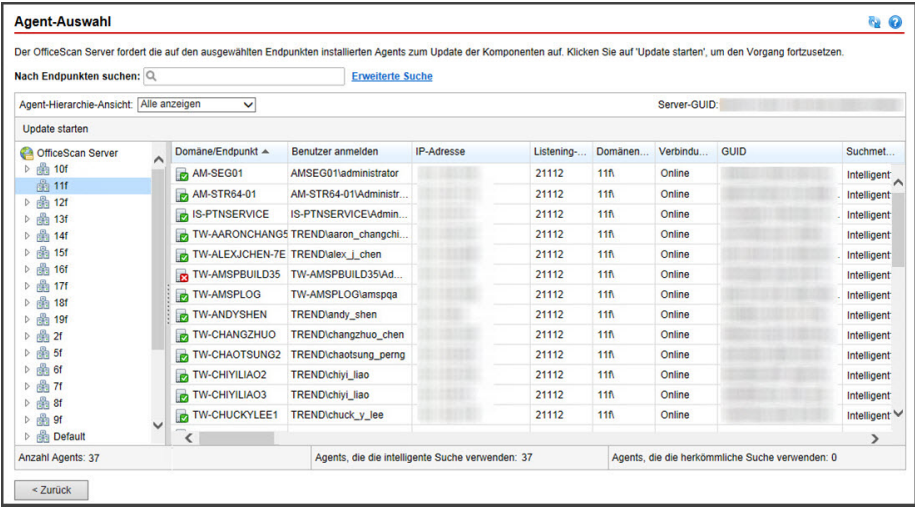


ABBILDUNG 2-24. Fenster Agent-Auswahl

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 *[Rollback der Komponenten durchführen für OfficeScan Agents auf Seite 6-56](#)*.

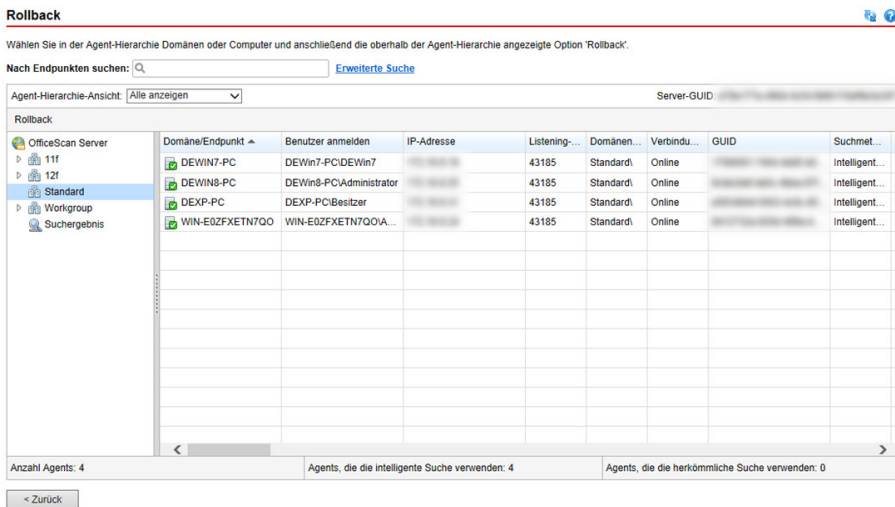


ABBILDUNG 2-25. Rollback

Sicherheitsrisiko-Protokolle

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

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

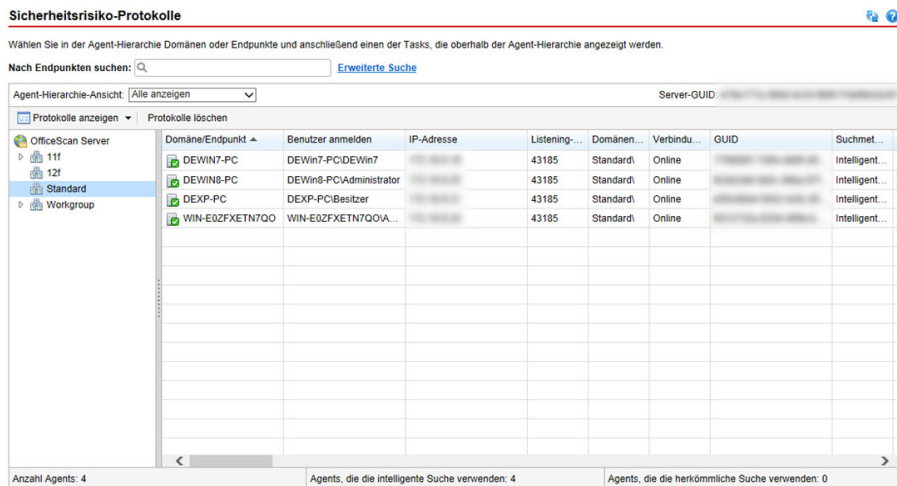


ABBILDUNG 2-26. Sicherheitsrisiko-Protokolle

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 7-98*
 - *Spyware/Grayware-Protokolle anzeigen auf Seite 7-107*
 - *Firewall-Protokolle anzeigen auf Seite 12-32*
 - *Web-Reputation-Protokolle anzeigen auf Seite 11-26*
 - *Protokolle zu verdächtigen Verbindungen anzeigen auf Seite 11-29*
 - *C&C Callback-Protokolle anzeigen auf Seite 11-27*
 - *Verhaltensüberwachungsprotokolle anzeigen auf Seite 8-16*
 - *Protokolle der Gerätesteuerng anzeigen auf Seite 9-19*

- *Protokolle der Funktion "Prävention vor Datenverlust" anzeigen auf Seite 10-61*
2. Protokolle löschen. Weitere Informationen finden Sie unter *Protokollmanagement auf Seite 13-40*.

OfficeScan Domänen

Eine Domäne in OfficeScan umfasst eine Gruppe von agents mit derselben Konfiguration, die dieselben Tasks 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 2-56*.

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 <i>Manuelle Agent-Gruppierung auf Seite 2-57</i>.

METHODE	AGENT-GRUPPIERUNG	BESCHREIBUNGEN
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 2-58.

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 2-63](#).

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** 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 2-60*.
 - Wenn Sie **IP-Adresse** ausgewählt haben, finden Sie die Konfigurationsanweisungen unter *Agent-Gruppierungsregeln nach IP-Adressen festlegen auf Seite 2-61*.
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 sortiert 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 2-61*, Schritt 7, oder in *Agent-Gruppierungsregeln nach Active Directory-Domänen festlegen auf Seite 2-60*, 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 2-38*.

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. (Optional) Wählen Sie **Active Directory-Struktur in der OfficeScan Agent-Hierarchie nachbilden** aus. 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.

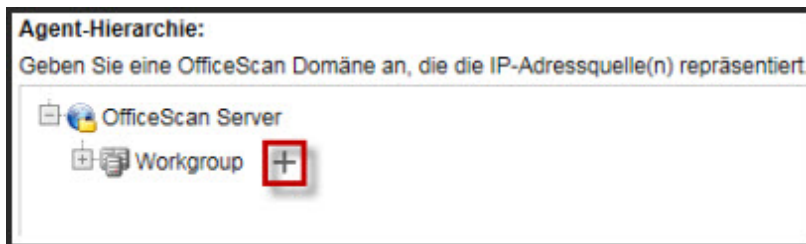


ABBILDUNG 2-27. Symbol "Domäne hinzufügen"

- 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 2-63](#)*.
- Domäne oder agent löschen. Weitere Informationen finden Sie unter *[Domäne oder Agent löschen auf Seite 2-64](#)*.
- Domäne umbenennen. Weitere Informationen finden Sie unter *[Umbenennen einer Domäne auf Seite 2-65](#)*.
- Einen einzelnen agent in eine andere Domäne oder auf einen anderen OfficeScan Server verschieben. Weitere Informationen finden Sie unter *[OfficeScan Agents in eine andere Domäne oder auf einen anderen OfficeScan Server verschieben auf Seite 2-65](#)*.

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 Agents 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. agents in eine andere Domäne verschieben:
 - 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 ausgewählte agents.



Tipp

Sie können agents auch per Drag & Drop in eine andere Domäne innerhalb der agent-Hierarchie verschieben.

5. agents in einen anderen OfficeScan Server verschieben:
 - Wählen Sie **Ausgewählte(n) Agent(s) auf einen anderen OfficeScan Server verschieben** aus.
 - Geben Sie den Servernamen oder die IPv4-/IPv6-Adresse und die HTTP-Portnummer ein.
 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 Agents 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 9-2](#).

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 15-12* 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 Agents 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 14-7](#).

- 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. Auf Offline- und Roaming-agents wird das Modul installiert, wenn sie wieder online sind.
- 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 10-67](#).

Das Datenschutzmodul an OfficeScan Agents 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** aus.
 - 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 Ziel-Endpunkt 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 sich dafür entschieden haben, das Modul nicht auf den agent zu verteilen, oder wenn sich der agent während der Verteilung im Offline- oder Roaming-Status befunden hat.
-

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 Patch 2* oder höher.
-

Einstellungen für Ordner der forensischen Daten und forensische Datenbank ändern

Administratoren können den Speicherort und den Löschrhythmus 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 Bereinigungsrückführung für forensische Datendateien konfigurieren	[INI_IDLP_SECTION] <code>ForensicDataPurgeCheckFrequency</code>  Hinweis - Die Einstellung <code>ForensicDataPurgeEnable</code> muss aktiviert sein, damit diese Einstellung in OfficeScan wirksam werden kann. - OfficeScan löscht nur Datendateien, die das in der Einstellung <code>ForensicDataExpiredPeriodInDays</code> 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] <code>ForensicDataExpiredPeriodInDays</code>	Standardwert (in Tagen): 180 Mindestwert: 1 Höchstwert: 3650
Zeitintervall der Speicherplatzrückführung für forensische Datendateien konfigurieren	[INI_SERVER_DISK_THRESHOLD] <code>MonitorFrequencyInSecond</code>  Hinweis Wenn der verfügbare Festplattenspeicher im Ordner der forensischen Daten unter den in der Einstellung <code>InformUploadOnDiskFreeSpaceInGb</code> 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	ForensicDataDelayUploadFrequencyInMinutes  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 *Benutzerdefinierter 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 Aktivierungscode.

Den Datenschutz über den Plug-in Manager deinstallieren

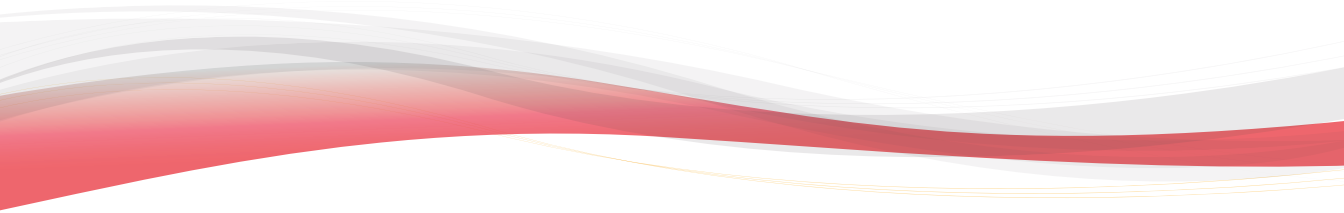
Prozedur

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 Agents



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 4-34*

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 auftkommender 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.

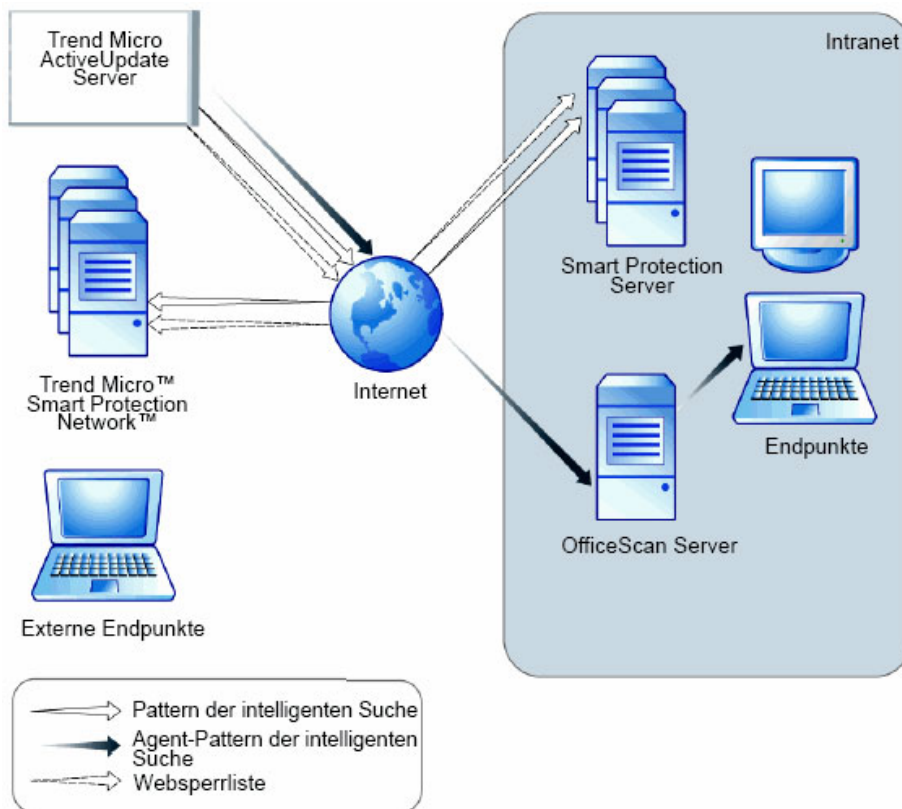


ABBILDUNG 4-1. Pattern-Update-Prozess

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 Websperreliste, 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 Websperreliste 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.

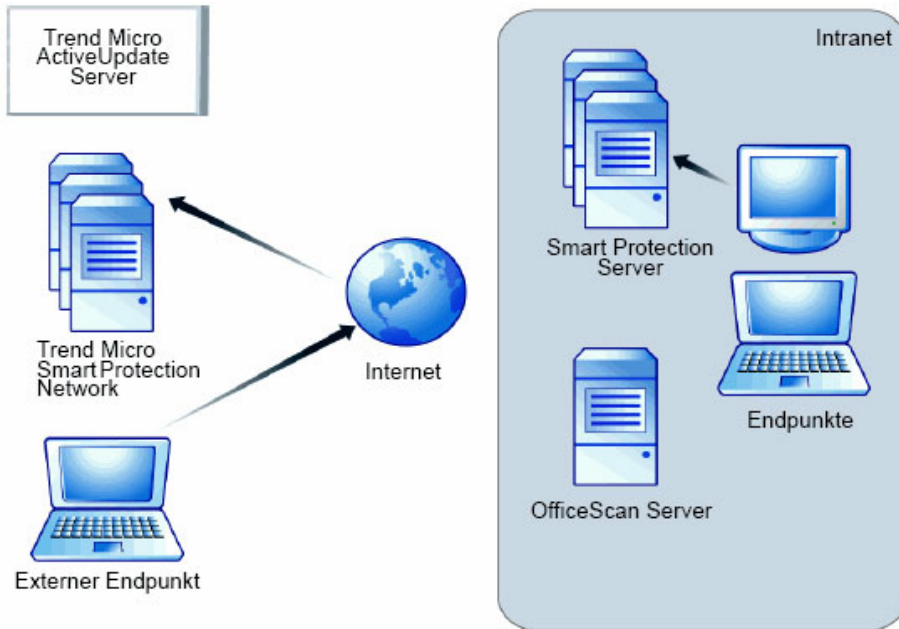


ABBILDUNG 4-2. Abfrageprozess

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 Schutzzumfang 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 4-20*
- *Liste der Smart Protection Quellen auf Seite 4-24*
- *Proxy-Einstellungen für Agent-Verbindungen auf Seite 4-33*
- *Trend Micro Network VirusWall Installationen auf Seite 4-33*

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 Servers 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 Servers:

- Aktivieren Sie den integrierten Server und konfigurieren Sie die Servereinstellungen. Weitere Informationen finden Sie unter *Verwaltung des integrierten Smart Protection Servers auf Seite 4-20*.

- 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 12-7](#).

**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 OfficeScan Tool für einen integrierten Smart Protection Server hilft Administratoren, einen integrierten Smart Protection Server zu installieren bzw. zu deinstallieren, nachdem die Installation des OfficeScan Servers abgeschlossen wurde. 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.

Bevor Sie den integrierten Smart Protection Server installieren, importieren Sie Folgendes auf Ihren aktualisierten OfficeScan 11.0 SP1 Server:

- Domänenstrukturen
- Die folgenden Einstellungen auf Root- und Domänenebene:
 - Suchkonfigurationen für alle Suchmethoden (manuelle Suche, Echtzeitsuche, zeitgesteuerte Suche und "Jetzt durchsuchen").
 - Web-Reputation-Einstellungen
 - Einstellungen der Verhaltensüberwachung

- Einstellungen der Gerätesteuerung
- Einstellungen für 'Prävention vor Datenverlust'
- Berechtigungen und andere Einstellungen
- Zusätzliche Diensteinstellungen
- Liste der zulässigen Spyware/Grayware
- Globale Agent-Einstellungen
- Endpunktspeicherort
- Firewall-Richtlinien und -Profile
- Smart Protection Quellen
- Zeitplan der Server-Updates
- Update-Adresse und Zeitplan des Agents
- Benachrichtigungen
- Proxy-Einstellungen

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.

BEFEHL	BESCHREIBUNG
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 Webserver 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)	
Apache Webserver mit aktiviertem SSL	8082	4345 (not configurable)	5274 (not configurable)
Apache Webserver mit deaktiviertem SSL	8082	4345 (not configurable)	5274 (not configurable)

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 iCRCSservice.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/Gespernte URLs des integrierten Servers

Weitere Informationen finden Sie unter *[Einstellungen eines integrierten Smart Protection Servers konfigurieren auf Seite 4-23](#)*.

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 4-23](#).

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 4-24](#).

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.



Tip

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 4-23](#).

Update der Komponenten des integrierten Servers

Der integrierte Server führt ein Update der folgenden Komponenten durch:

- **Pattern der intelligenten Suche:** OfficeScan Agents überprüfen potenzielle Bedrohungen mit Hilfe des Patterns der intelligente Suche, indem sie Suchabfragen an den integrierten Server senden.
- **Websperrierliste:** OfficeScan 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 4-23](#)*.

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 11-5](#)*). 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 4-23*.

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 6-21*.
 - 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 14-2](#).

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 sendet Suchabfragen mit dem HTTP-Protokoll oder mit dem HTTPS-Protokoll. HTTPS ermöglicht eine sicherere Verbindung, während HTTP weniger Bandbreite benötigt.
- 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.
 - 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 sendet Web-Reputation-Abfragen mit dem HTTP-Protokoll. HTTPS wird nicht unterstützt.
- Geben Sie den Server-Listening-Port für HTTP-Anfragen ein.
 - 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 die Endpunkt-Leistung bei sehr großem Datenverkehrsvolumen für die beiden 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.
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 Dual-Stack Smart Protection Servern verbinden. Agents mit einer IPv6-Adresse können sich mit reinen IPv6- oder Dual-Stack Smart Protection Servern verbinden. Agents, die sowohl eine IPv4- als auch eine IPv6-Adresse besitzen, können sich mit jedem beliebigen 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 sendet Suchabfragen mit dem HTTP- oder HTTPS-Protokoll. 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 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 sendet Web-Reputation-Abfragen mit dem 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 können, kann die Computerleistung bei sehr hohem Datenaufkommen für die beiden 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.

- 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** ( **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. Weitere Informationen finden Sie unter [Externer Proxy für OfficeScan Agents auf Seite 14-53](#).

Konfigurieren Sie interne Proxy-Einstellungen, die agents für Verbindungen mit einem Smart Protection Server verwenden. Weitere Informationen finden Sie unter [Interner Proxy für OfficeScan Agents auf Seite 14-52](#).

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 14-2](#).

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 11-5*.



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 13-66*.

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 5-11*
- *Zu OfficeScan Agent migrieren auf Seite 5-68*
- *Nach der Installation auf Seite 5-72*
- *OfficeScan Agent deinstallieren auf Seite 5-75*

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 agents folgende Hinweise:

TABELLE 5-1. Überlegungen zur 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-agents 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 agents mit sowohl IPv4- als auch IPv6-Adressen können Sie wählen, welche IP-Adresse verwendet wird, wenn sich der agent am Server anmeldet.

ÜBERLEGUNG	BESCHREIBUNG
Ausschlusslisten	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 8-7. • 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 11-5.

OfficeScan Agent Funktionen

Welche der OfficeScan Agent-Funktionen auf dem Endpunkt verfügbar sind, hängt vom Betriebssystem des Endpunkts ab.

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

FUNKTION	WINDOWS BETRIEBSSYSTEM		
	SERVER 2003	SERVER 2008/ SERVER CORE 2008	SERVER 2012/ SERVER CORE 2012
Manuelle Suche, Echtzeitsuche und zeitgesteuerte Suche	Ja	Ja	Ja
Komponenten-Update (manuelles und zeitgesteuertes Update)	Ja	Ja	Ja
Update-Agent	Ja	Ja	Ja

FUNKTION	WINDOWS BETRIEBSSYSTEM		
	SERVER 2003	SERVER 2008/ SERVER CORE 2008	SERVER 2012/ SERVER CORE 2012
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; eingeschränkte Unterstützung des Windows-Benutzeroberflächenmodus
Damage Cleanup Services	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; Anwendungsfilter nicht unterstützt
Verhaltensüberwachung	Ja (32 Bit), aber standardmäßig deaktiviert	Ja (32 Bit), aber standardmäßig deaktiviert	Ja (64 Bit), aber standardmäßig deaktiviert
	Nein (64 Bit)	Ja (64 Bit), aber standardmäßig deaktiviert	
Agent Selbstschutz für: - Registrierungsschlüssel - Prozesse	Ja (32 Bit), aber standardmäßig deaktiviert	Ja (32 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
Agent Selbstschutz für: - Dienste - Dateischutz	Ja	Ja	Ja
Geräteststeuerung (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
	Nein (64 Bit)	Ja (64 Bit), aber standardmäßig deaktiviert	
Datenschutz (einschließlich Datenschutz für die Geräteststeuerung)	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	
POP3 mail scan	Ja	Ja	Ja
Agent Plug-in Manager	Ja	Ja	Ja
Roaming-Modus	Ja	Ja (Server) Nein (Server-Kern)	Ja
Smart Feedback	Ja	Ja	Ja

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

FUNKTION	WINDOWS BETRIEBSSYSTEM			
	XP	VISTA	WINDOWS 7	WINDOWS 8/8.1
Manuelle Suche, Echtzeitsuche und zeitgesteuerte Suche	Ja	Ja	Ja	Ja
Komponenten-Update (manuelles und zeitgesteuertes Update)	Ja	Ja	Ja	Ja
Update-Agent	Ja	Ja	Ja	Ja
Web reputation	Ja	Ja	Ja	Ja, aber nur eingeschränkte Unterstützung des Windows-Benutzeroberflächenmodus
Damage Cleanup Services	Ja	Ja	Ja	Ja
OfficeScan firewall	Ja	Ja	Ja	Ja, aber Anwendungsfilter nicht unterstützt
Verhaltensüberwachung	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit)
	Nein (64 Bit)	Ja (64 Bit) Vista 64-Bit-Unterstützung erfordert SP1 oder SP2	Ja (64 Bit)	Ja (64 Bit)

FUNKTION	WINDOWS BETRIEBSSYSTEM			
	XP	VISTA	WINDOWS 7	WINDOWS 8/8.1
Agent Selbstschutz für: • Registrierungsschlüssel • Prozesse	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit)
	Nein (64 Bit)	Ja (64 Bit) Vista 64-Bit-Unterstützung erfordert SP1 oder SP2	Ja (64 Bit)	Ja (64 Bit)
Agent Selbstschutz für: • Dienste • Dateischutz	Ja	Ja	Ja	Ja
Geräteststeuerung (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) Vista 64-Bit-Unterstützung erfordert SP1 oder SP2	Ja (64 Bit)	Ja (64 Bit)
Datenschutz (einschließlich Datenschutz für die Gerätesteuerung)	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit)	Ja (32 Bit), im Desktop-Modus
	Ja (64 Bit)	Ja (64 Bit)	Ja (64 Bit)	Ja (64 Bit), im Desktop-Modus
POP3 mail scan	Ja	Ja	Ja	Ja
Agent Plug-in Manager	Ja	Ja	Ja	Ja
Roaming-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 einem Dual-Stack- oder reinen IPv6-agents.

Betriebssystem

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

- Windows Vista™ (alle Editionen)
- Windows Server 2008 (alle Editionen)
- Windows 7 (alle Editionen)
- Windows Server 2012 (alle Editionen)
- Windows 8/8.1 (alle Editionen)

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

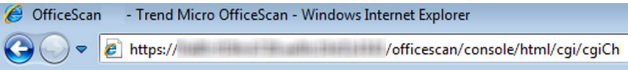
<http://docs.trendmicro.com/de-de/enterprise/officescan.aspx>

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 von Agents > Globale Agent-Einstellungen 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. Gehen Sie zum Abschnitt **Bevorzugte IP-Adresse**.
 3. 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.
 4. 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 5-8](#).

TABELLE 5-5. Überlegungen zur Verteilung für die Installation

INSTALLATIONSMETHODE/ BETRIEBSSYSTEMUNTERSTÜTZUNG	ÜBERLEGUNGEN ZUR VERTEILUNG					
	WAN- VERTEILUNG	ZENTRALE VERWALTUNG	ERFORDERT EINGREIFEN DURCH DEN BENUTZER	ERFORDERT IT- RESSOURCE	VERTEILUNG IN HOHER ANZAHL	VERBRAUCHTE BANDBREITE
Web- Installationsseite Unterstützt auf allen Betriebssystemen außer Windows Server Core 2008 und Windows 8/8.1/ Server 2012/ Server Core 2012 im Windows- Benutzeroberfläche modus	Nein	Nein	Ja	Nein	Nein	Hoch

INSTALLATIONSMETHODE/ BETRIEBSSYSTEMUNTERSTÜTZUNG	ÜBERLEGUNGEN ZUR VERTEILUNG					
	WAN- VERTEILUNG	ZENTRALE VERWALTUNG	ERFORDER- T EINGREIF- EN DURCH DEN BENUTZER	ERFORDER- T IT- RESSOURCE	VERTEILUNG IN HOHER ANZAHL	VERBRAUCHTE BANDBREITE
Browserbasierte Installationen Wird unter allen Betriebssystemen unterstützt  Hinweis Nicht unterstützt unter Windows 8, 8.1 und Windows Server 2012 im Windows-Benutzeroberflächen-Modus.	Nein	Nein	Ja	Ja	Nein	Hoch, wenn die Installationen gleichzeitig gestartet werden
UNC-basierte Installationen Wird unter allen Betriebssystemen unterstützt	Nein	Nein	Ja	Ja	Nein	Hoch, wenn die Installationen gleichzeitig gestartet werden

INSTALLATIONSMETHODE/ BETRIEBSSYSTEMUNTERSTÜTZUNG	ÜBERLEGUNGEN ZUR VERTEILUNG					
	WAN- VERTEILUNG	ZENTRALE VERWALTUNG	ERFORDERTE EINGREIFEN DURCH DEN BENUTZER	ERFORDERTE IT- RESSOURCE	VERTEILUNG IN HOHER ANZAHL	VERBRAUCHTE BANDBREITE
Remote-Installationen Wird auf allen Betriebssystemen unterstützt, außer: • Windows Vista Home Basic und Home Premium • Windows XP Home • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 (Basic-Versionen)	Nein	Ja	Nein	Ja	Nein	Hoch
Anmeldeskript-Setup Wird unter allen Betriebssystemen unterstützt	Nein	Nein	Ja	Ja	Nein	Hoch, wenn die Installationen gleichzeitig gestartet werden

INSTALLATIONSMETHODE/ BETRIEBSSYSTEMUNTERSTÜTZUNG	ÜBERLEGUNGEN ZUR VERTEILUNG					
	WAN- VERTEILUNG	ZENTRALE VERWALTUNG	ERFORDER- T EINGREIF- EN DURCH DEN BENUTZER	ERFORDER- T IT- RESSOURCE	VERTEILUNG IN HOHER ANZAHL	VERBRAUCHTE BANDBREITE
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
Agent-Disk-Image Wird unter allen Betriebssystemen unterstützt	Nein	Nein	Nein	Ja	Nein	Niedrig

INSTALLATIONSMETHODE/ BETRIEBSSYSTEMUNTERSTÜTZUNG	ÜBERLEGUNGEN ZUR VERTEILUNG					
	WAN- VERTEILUNG	ZENTRALE VERWALTUNG	ERFORDER- T EINGREIF- EN DURCH DEN BENUTZER	ERFORDER- T IT- RESSOURCE	VERTEILUNG IN HOHER ANZAHL	VERBRAUCHTE BANDBREITE
Trend Micro Vulnerability Scanner (TMVS) Wird auf allen Betriebssystemen unterstützt, außer: • Windows Vista Home Basic und Home Premium • Windows XP Home • Windows 8/8.1 (Basic- Versionen)	Nein	Ja	Nein	Ja	Nein	Hoch

INSTALLATIONSMETHODE/ BETRIEBSSYSTEMUNTERSTÜTZUNG	ÜBERLEGUNGEN ZUR VERTEILUNG					
	WAN- VERTEILUNG	ZENTRALE VERWALTUNG	ERFORDER- T EINGREIF- EN DURCH DEN BENUTZER	ERFORDER- T IT- RESSOURCE	VERTEILUNG IN HOHER ANZAHL	VERBRAUCHTE BANDBREITE
Installationen für die Einhaltung von Sicherheitsrichtlinien Wird auf allen Betriebssystemen unterstützt, außer: • Windows Vista Home Basic und Home Premium • Windows XP Home • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 (Basic-Versionen)	Nein	Ja	Nein	Ja	Nein	Hoch

Installationen über eine Web-Installationsseite

Sie können das OfficeScan Agent-Programm über die Web-Installationsseite installieren, wenn Sie den OfficeScan Server auf Endpunkte installiert haben, auf denen die folgenden Plattformen ausgeführt werden:

- Windows Server 2003 mit Internet Information Server (IIS) 6.0 oder Apache 2.0.x

- Windows Server 2008 mit Internet Information Server (IIS) 7.0
- Windows Server 2008 R2 mit Internet Information Server (IIS) 7.5
- Windows Server 2012 mit Internet Information Server (IIS) 8.0

Um eine Installation von der Web-Installationsseite durchzuführen, gelten folgende Voraussetzungen:

- Internet Explorer, wobei für die Sicherheitsstufe festgelegt ist, dass ActiveXTM-Steuerelemente verwendet werden dürfen. Die folgenden Versionen sind erforderlich:
 - 6.0 unter Windows XP und Windows Server 2003
 - 7.0 unter Windows Vista und Windows Server 2008
 - 8.0 unter Windows 7
 - 10.0 unter Windows 8/8.1 und Windows Server 2012
- Administratorberechtigungen auf dem Endpunkt

Senden Sie die folgenden Anweisungen zur Installation des OfficeScan Agents von der Web-Installationsseite an die Benutzer. Informationen zum Versenden einer Installationsbenachrichtigung per E-Mail finden Sie unter *[Browserbasierte Installation starten auf Seite 5-19](#)*.

Installation über die Web-Installationsseite

Prozedur

1. Melden Sie sich mit dem integrierten Administratorkennwort am Endpunkt an.



Hinweis

Auf Windows 7-, Windows 8- bzw. Windows 8.1-Plattformen müssen Sie zunächst das integrierte Administratorkonto aktivieren. Unter Windows 7, Windows 8 und Windows 8.1 wird das Administratorkonto standardmäßig deaktiviert. Weitere Informationen finden Sie auf der Support-Website von Microsoft (<http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx>).

2. Wenn das Programm auf Endpunkten unter Windows XP, Vista, Server 2008, 7, 8, 8.1 oder Server 2012 installiert wird, führen Sie die folgenden Schritte durch:
 - a. Starten Sie Internet Explorer und fügen Sie die URL des OfficeScan Servers (wie z. B. `https://<OfficeScan server name>:4343/officescan`) zur Liste der vertrauenswürdigen Websites hinzu. Öffnen Sie unter Windows XP Home die Registerkarte **Extras** > **Internetoptionen** > **Sicherheit**, wählen Sie das Symbol **Vertrauenswürdige Sites**, und klicken Sie auf **Sites**.
 - b. Ändern Sie die Sicherheitseinstellung des Internet Explorers, um die Option **Automatische Eingabeaufforderung für ActiveX-Steuerelemente** zu aktivieren. Öffnen Sie unter Windows XP die Registerkarte **Extras** > **Internetoptionen** > **Sicherheit**, und klicken Sie auf **Stufe anpassen**.
3. Öffnen Sie ein Internet Explorer Browser-Fenster, und geben Sie Folgendes ein:
`https://<OfficeScan server name>:<port>/officescan`
4. Klicken Sie auf der Anmeldeseite auf den **Installer**-Link, um die folgenden Installationsoptionen anzuzeigen:
 - **Agent-Installation über Webbrowser** (nur Internet Explorer): Befolgen Sie die angezeigten Anweisungen für Ihr Betriebssystem.
 - **MSI-Agent-Installation**: Laden Sie das 32-Bit- bzw. 64-Bit-Paket für Ihr Betriebssystem herunter und befolgen Sie die angezeigten Anweisungen.

**Hinweis**

Lassen Sie die Installation des ActiveX-Steuerelements zu, wenn Sie dazu aufgefordert werden.

5. 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 14-28*.

Browserbasierte 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 5-40*.
 - Überprüfen Sie die Einhaltung der Sicherheitsrichtlinien. Weitere Informationen finden Sie unter *Einhaltung der Sicherheitsrichtlinien für nicht verwaltete Endpunkte auf Seite 14-74*.

Browserbasierte Installation starten

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

AutoPec.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 OfficeScan Agent nicht auf Endpunkten installiert, auf denen bereits OfficeScan Server ausgeführt wird.



Hinweis

Diese Installationsmethode steht für Endpunkte unter Windows XP Home, Windows Vista Home Basic und Home Premium sowie 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) 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 Vista:
 - a. Aktivieren Sie ein integriertes Domänenadministratorkonto und richten Sie das Kennwort für das Konto ein.
 - b. Klicken Sie auf **Start > Systemsteuerung > Sicherheit > Windows Firewall > Einstellungen ändern**.

- c. Klicken Sie auf die Registerkarte **Ausnahmen** und aktivieren Sie die Ausnahme **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 oder Windows Server 2012:
 - 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 aus und klicken Sie anschließend auf **Hinzufügen**.
 - Geben Sie den Endpunkt-Namen in das Feld **Nach Endpunkten suchen** oben auf der Seite ein und drücken Sie die EINGABETASTE, um nach einem bestimmten Endpunkt-Namen zu suchen.

OfficeScan fordert Sie auf, für den Zielcomputer 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 Ziel-Endpunkt wird in der Tabelle **Ausgewählte Endpunkte** angezeigt.

5. Wiederholen Sie die Schritte 3 und 4, um weitere Computer 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 Ziel-Endpunkte kopiert werden, wird ein Fortschrittsfenster angezeigt.

Wenn OfficeScan die Installation auf einen Ziel-Endpunkt abgeschlossen hat, wird der Endpunkt-Name aus der Liste **Ausgewählte Endpunkte** entfernt und in der Liste **Domänen und Endpunkte** mit einem roten Häkchen versehen 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 16-16](#)). 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 Anmeldeskript Sie geändert haben. AutoPcc.exe installiert den OfficeScan Agent jedoch auf Computern unter Windows Vista, 7, 8, 8.1, Server 2008 und Server 2012 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.

Die Skripts für Windows Server 2003, 2008 und 2012

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:

- <Servername> ist der Endpunkt-Name oder die IP-Adresse des OfficeScan Server-Endpunkts.
- "ofcscan" ist der Name des Freigabeordners von OfficeScan auf dem Server.
- "autopcc" ist der Link zu der 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

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 Agents oder von Komponenten auf agents an Standorten 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:

- 350 MB 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. Wenn Benutzer das EXE-Paket auf Endpunkten unter Windows Vista, Server 2008, 7, 8, 8.1 oder Server 2012 installieren möchten, fordern Sie diese Benutzer auf, mit der rechten Maustaste auf die EXE-Datei zu klicken und dann **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 5-32](#) oder [Ein MSI-Paket über Microsoft SMS verteilen auf Seite 5-34](#).

4. Starten Sie das MSI-Paket über die Eingabeaufforderung, damit der OfficeScan Agent unbeaufsichtigt auf einem Remote-Endpunkt unter Windows XP, Vista, Server 2008, 7, 8, 8.1 oder Server 2012 installiert wird.

Suchmethodenrichtlinien für Agent Pakete

Wählen Sie für das Paket die Suchmethode aus. Weitere Informationen finden Sie unter [Suchmethodenentypen 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 6-30](#).

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**.

Automatische Agent-Gruppierung					
Hinzufügen		Löschen			
Gruppenpriorität	Name	Quelle	Status	Name:	
1	2E	IP-Adresse	Aktiviert	11F	
2	5E	IP-Adresse	Aktiviert		
3	6E	IP-Adresse	Aktiviert	Quelle:	
4	7E	IP-Adresse	Aktiviert		
5	8E	IP-Adresse	Aktiviert	Ziel:	
6	9E	IP-Adresse	Aktiviert	11F	
7	10E	IP-Adresse	Aktiviert		
8	11E	IP-Adresse	Aktiviert		
9	12E	IP-Adresse	Aktiviert		
10	13E	IP-Adresse	Aktiviert		

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 Domännennamen, 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 5-28](#).

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. 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 5-27*.

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-Verwaltungskontrolle**. 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:
 - a. Öffnen Sie die **Gruppenrichtlinien-Verwaltungskontrolle**. 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 5-27*.

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 5-72](#)*.

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

Das Paket lokal erhalten

Prozedur

- Öffnen Sie die **SMS Administrator**-Konsole.
- Klicken Sie auf der Registerkarte **Struktur** auf **Pakete**.
- 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.

- Klicken Sie auf **Weiter**.

Das Fenster **Paketdefinition** wird angezeigt.

- Klicken Sie auf **Durchsuchen**.

Das Fenster **Öffnen** wird angezeigt.

- 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.

- Klicken Sie auf **Weiter**.

Das Fenster **Quelldateien** wird angezeigt.

- 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 5-27](#)*.
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 Domännennamen 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 5-41*
- *Netzwerktopologie und -architektur auf Seite 5-41*
- *Software/Hardware-Spezifikationen auf Seite 5-42*
- *Domänenstruktur auf Seite 5-42*
- *Netzwerkdatenverkehr auf Seite 5-43*
- *Netzwerkgröße auf Seite 5-43*

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.

SETUP	EFFEKTIVITÄT DES VULNERABILITY SCANNERS
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 Vista Home Basic, Windows Vista Home Premium, Windows 7 Home Basic, Windows 7 Home Premium, Windows 8 (Basic-Versionen) oder Windows 8.1 (Basic-Versionen) ausgeführt.

**Hinweis**

Sie können den OfficeScan Agent auf dem Ziel-Host-Rechner mit anderen Installationsmethoden installieren. Diese werden unter [Überlegungen zur Verteilung auf Seite 5-11](#) erläutert.

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

- Unter Windows Vista (Business, Enterprise oder Ultimate Edition) oder Windows 7 (Professional, Enterprise, Ultimate Edition), Windows 8 (Pro, Enterprise), Windows 8.1 (Pro, Enterprise), Windows Server 2012 (Standard):
 1. Aktivieren Sie ein integriertes Administratorkonto, und richten Sie das Kennwort für das Konto ein.
 2. Klicken Sie auf **Start > 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.
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 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, Vista, 7, 8, 8.1 oder Server 2012 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 Computer ein, die Sie überprüfen möchten.
 - a. Geben Sie einen IPv4-Adressbereich ein.

**Hinweis**

Vulnerability Scanner kann IPv4-Adressbereiche nur dann abfragen, wenn das Tool auf einem reinen IPv4- oder Dual-Stack-Host-Rechner 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 Ziel-Host-Rechner eine IP-Adresse verwendet, kann Vulnerability Scanner das Betriebssystem des Host-Rechners ermitteln. Weitere Informationen finden Sie unter Ping-Einstellungen auf Seite 5-63.
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 5-60.
Produktabfrage:	Vulnerability Scanner kann feststellen, ob auf den Endpunkten Sicherheitssoftware vorhanden ist.

OPTION	BEZEICHNUNG
	Weitere Informationen finden Sie unter Produktabfrage auf Seite 5-56 .
OfficeScan 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 5-64.  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 5-43.
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 5-61.
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 5-62.

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.

EINSTELLUNG	BESCHREIBUNG
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, Vista, 7, 8, 8.1 oder Server 2012 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 5-56.
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 5-64.  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 5-43.
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 5-61.
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 5-62.

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 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, Vista, 7, 8, 8.1 oder Server 2012 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 Computer ein, die Sie überprüfen möchten.
 - a. Geben Sie einen IPv4-Adressbereich ein.

**Hinweis**

Vulnerability Scanner kann IPv4-Adressbereiche nur dann abfragen, wenn das Tool auf einem reinen IPv4- oder Dual-Stack-Host-Rechner 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 5-46](#).
 - 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 Ziel-Host-Rechner eine IP-Adresse verwendet, kann Vulnerability Scanner das Betriebssystem des Host-Rechners ermitteln. Weitere Informationen finden Sie unter Ping-Einstellungen auf Seite 5-63.
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 5-60.
Produktabfrage:	Vulnerability Scanner kann feststellen, ob auf den Endpunkten Sicherheitssoftware vorhanden ist. Weitere Informationen finden Sie unter Produktabfrage auf Seite 5-56.

OfficeScan 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 5-64. 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 5-43.
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 5-61.
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 5-62.

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 16-3](#).

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.
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.

PRODUCT	BESCHREIBUNG
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/intercan.dll
Trend Micro Internet Security™ (PC-cillin)	Der Vulnerability Scanner verwendet Port 40116, um zu überprüfen, ob Trend Micro Internet Security installiert ist.
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 5-45](#).

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 5-45](#).

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 5-45*.

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 5-45](#).

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 5-45*.

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:
- Navigieren Sie zu *<Installationsordner des Servers>\PCCSRV\Admin\Utility\TMVS*, und öffnen Sie TMVS.ini mit Hilfe eines Texteditors, z. B. Notepad.
 - 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.
 - 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 5-43*.

- 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 5-45](#).

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 mit Hilfe der IP-Adresse den OfficeScan Agent auf einen Ziel-Endpunkt.

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 Vista Home Basic, Windows Vista Home Premium, Windows 7™ Starter, Windows 7 Home Basic, Windows 7 Home Premium, Windows 8 (Basic-Versionen) oder Windows 8.1 (Basic-Versionen) ausgeführt. Wählen Sie eine andere Installationsmethode bei Computern mit diesen Betriebssystemen. Weitere Informationen finden Sie unter [*Überlegungen zur Verteilung auf Seite 5-11*](#).
3. Wenn auf dem Ziel-Endpunkt Windows Vista (Business, Enterprise oder Ultimate Edition), Windows 7 (Professional, Enterprise oder Ultimate Edition), Windows 8 (Pro, Enterprise), Windows 8.1 (Pro, Enterprise) oder Windows Server 2012 (Standard) ausgeführt wird, führen Sie die folgenden Schritte auf dem Endpunkt aus:
 - 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 Security-Software 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 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.

Den OfficeScan Agent installieren

Prozedur

1. Navigieren Sie zu **Bewertung > Nicht verwaltete Endpunkte**.
2. Klicken Sie oben in der agent-Hierarchie auf **Installieren**.
 - Wenn auf dem Endpunkt bereits eine frühere OfficeScan Agent-Version installiert ist und Sie auf **Installieren** klicken, wird die Installation übersprungen und der agent wird nicht auf diese Version aktualisiert. Eine Einstellung muss deaktiviert werden, um ein Upgrade des agents vorzunehmen.
 - a. Navigieren Sie zu **Agents > Agent-Verwaltung**.
 - b. Klicken Sie auf die Registerkarte **Einstellungen > Berechtigungen und andere Einstellungen > Andere Einstellungen**.

- c. Deaktivieren Sie die Einstellung **OfficeScan Agents können Komponenten aktualisieren, aber kein Upgrade des Agents durchführen oder Hotfixes verteilen**.
 3. Geben Sie für jeden Endpunkt das Anmeldekonto für den Administrator an und klicken Sie auf Endpunkt **Anmelden**. OfficeScan startet die Installation des agents auf dem Ziel-Endpunkt.
 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 5-11](#) 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 Zielpunkt 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 5-73*
- *Programmliste auf Seite 5-73*
- *OfficeScan Agent-Dienste auf Seite 5-73*
- *OfficeScan Agent -Installationsprotokolle auf Seite 5-74*

OfficeScan Agent Verknüpfung

Die OfficeScan Agent-Verknüpfungen werden im Windows Start-Menü auf dem agent Endpunkt angezeigt.

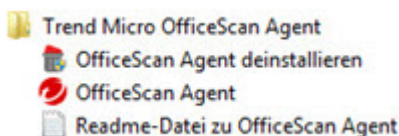


ABBILDUNG 5-2. OfficeScan Agent Verknüpfung

Programmliste

Security 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 Echtzeitsuche (NTRtScan.exe)
- OfficeScan NT Proxy-Dienst (TmProxy.exe)



Hinweis

Der OfficeScan NT Proxy-Dienst ist auf Windows 7/8/8.1- oder Windows Server 2008 R2/2012-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 5-76*
- *Das Programm zur Deinstallation des OfficeScan Agents ausführen auf Seite 5-78*

Wenn der OfficeScan Agent nicht mit Hilfe der oben erwähnten Methode deinstalliert werden kann, deinstallieren Sie den OfficeScan Agent manuell. Weitere Informationen finden Sie unter [Den OfficeScan Agent manuell deinstallieren auf Seite 5-78](#).

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 Stammsymbol () , um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
 3. Klicken Sie auf **Aufgaben > Agent-Deinstallation**.
 4. Klicken Sie im Fenster **Agent-Deinstallation** auf **Deinstallation starten**. Der Server sendet eine Benachrichtigung an die agents.
 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 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 **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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 beim agent Endpunkt als Administrator 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 und Windows Server 2012 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 14-96*.
-

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 Firewall
- OfficeScan NT Echtzeitsuche
- OfficeScan NT Proxy-Dienst



Hinweis

Der OfficeScan NT Proxy-Dienst ist auf Windows 7, 8, 8.1- oder Windows Server 2008R2, 2012-Plattformen nicht vorhanden.

- Trend Micro Unauthorized Change Prevention Service
- Gemeinsames Client Solution Framework für Trend Micro

4. Entfernen Sie die Verknüpfung des OfficeScan Agent aus dem Start-Menü.

- Unter Windows 8, 8.1 und Windows Server 2012:
 - 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 **Vom Startmenü 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:
 - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

64-Bit-Computer:

`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`

64-Bit-Computer:

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfcWatchDog`
 - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp`

64-Bit-Computer:


```
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
 - tmcfw
 - tmcomm
 - TmFilter

- TmListen
- tmpfw
- TmPreFilter
- TmProxy



Hinweis

TmProxy ist auf Windows 8-/8.1- und Windows Server 2012-Plattformen nicht vorhanden.

- tmttdi



Hinweis

tmttdi ist auf Windows 8-/8.1- und Windows Server 2012-Plattformen nicht vorhanden.

- VSApiNt
- tmlwf (für Computer mit Windows Vista/Server 2008/7/8/8.1/Server 2012)
- tmwfp (für Computer mit Windows Vista/Server 2008/7/8/8.1/Server 2012)
- tmactmon
- TMBMServer
- TMebc
- tmevtmgr
- tmeevw (für Windows 8/8.1/Server 2012)
- tmusa (für Windows 8/8.1/Server 2012)
- tmnciesc
- tmeext (für Windows XP/2003)

9. Schließen Sie den Registrierungseditor.
10. Klicken Sie auf **Starten > Einstellungen > Systemsteuerung**, und doppelklicken Sie auf **System**.

**Hinweis**

Für Windows 8-/8.1- und Windows Server 2012-Systeme überspringen Sie diesen Schritt.

11. Klicken Sie auf die Registerkarte **Hardware**, und klicken Sie anschließend auf **Gerätemanager**.

**Hinweis**

Für Windows 8-/8.1- und Windows Server 2012-Systeme überspringen Sie diesen Schritt.

12. Klicken Sie auf **Ansicht > Ausgeblendete Geräte anzeigen**.

**Hinweis**

Für Windows 8-/8.1- und Windows Server 2012-Systeme überspringen Sie diesen Schritt.

13. Erweitern Sie **Nicht-PnP-Treiber**, und deinstallieren Sie anschließend die folgenden Geräte (für Windows XP/Vista/7/Server 2003/Server 2008):
 - tmcomm
 - tmactmon
 - tmevtmgr
 - Trend Micro Filter
 - Trend Micro PreFilter
 - Trend Micro TDI-Treiber
 - Trend Micro VSAPI NT
 - Trend Micro Unauthorized Change Prevention Service

- Trend Micro WFP Callout Driver (für Computer mit Windows Vista/Server 2008/7)

14. Löschen Sie Trend Micro Treiber manuell mit einem Befehlszeilen-Editor (nur Windows 8/8.1/Server 2012) unter Verwendung der folgenden Befehle:

- `sc delete tmcomm`
- `sc delete tmactmon`
- `sc delete tmevtmgr`
- `sc delete tmfilter`
- `sc delete tmprefilter`
- `sc delete tmwfp`
- `sc delete vsapint`
- `sc delete tmeevw`
- `sc delete tmusa`
- `sc delete tmebc`



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.

- 15.** Deinstallieren Sie den Treiber für die allgemeine Firewall.
- a. Klicken Sie mit der rechten Maustaste auf **Netzwerkumgebung**, und klicken Sie auf **Eigenschaften**.
 - b. Klicken Sie mit der rechten Maustaste auf **LAN-Verbindung**, und klicken Sie auf **Eigenschaften**.
 - c. Wählen Sie auf der Registerkarte **Allgemein** den **Trend Micro Treiber für die allgemeine Firewall**, und klicken Sie auf **Deinstallieren**.

**Hinweis**

Die folgenden Schritte gelten nur für die Betriebssysteme Windows Vista/Server 2008/7/8/8.1/Server 2012. Fahren Sie bei Agents mit anderen Betriebssystemen mit Schritt 15 fort.

- d. Klicken Sie mit der rechten Maustaste auf **Netzwerk**, und klicken Sie auf **Eigenschaften**.
 - e. Klicken Sie auf **Netzwerkverbindungen verwalten**.
 - f. Klicken Sie mit der rechten Maustaste auf **LAN-Verbindung**, und klicken Sie auf **Eigenschaften**.
 - g. Wählen Sie auf der Registerkarte **Netzwerk** den **Trend Micro NDIS 6.0 Filter-Treiber**, und klicken Sie auf **Deinstallieren**.
16. Starten Sie den agent-Endpunkt neu.
 17. Wenn keine anderen Produkte von Trend Micro auf dem Endpunkt installiert sind, löschen Sie den Trend Micro Installationsordner (normalerweise C:\Programme\Trend Micro). Auf 64-Bit-Computern befindet sich der Installationsordner unter C:\Programme (x86)\Trend Micro.
 18. Wenn andere Produkte von Trend Micro installiert sind, löschen Sie die folgenden Ordner:
 - *<Installationsordner des Agents>*
 - Den Ordner BM unter dem Trend Micro Installationsordner (normalerweise C:\Programme\Trend Micro\BM für 32-Bit-Systeme und C:\Programme (x86)\Trend Micro\BM für 64-Bit-Systeme)

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 6-14*
- *OfficeScan Server-Updates auf Seite 6-17*
- *Updates für den integrierten Smart Protection Server auf Seite 6-30*
- *OfficeScan Agent Updates auf Seite 6-30*
- *Update-Agents auf Seite 6-58*
- *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 diese Konfigurationsdateien, um neue Einstellungen zu übernehmen. Bei jeder Änderung der OfficeScan Einstellungen über die Webkonsole ändern sich auch die Konfigurationsdateien.

Die Komponenten sind wie folgt gruppiert:

- *[Antiviren-Komponenten auf Seite 6-2](#)*
- *[Damage Cleanup Services-Komponenten auf Seite 6-7](#)*
- *[Anti-Spyware-Komponenten auf Seite 6-7](#)*
- *[Firewall-Komponenten auf Seite 6-8](#)*
- *[Web-Reputation-Komponenten auf Seite 6-9](#)*
- *[Komponenten der Verhaltensüberwachung auf Seite 6-9](#)*
- *[Programme auf Seite 6-11](#)*
- *[Komponenten des Diensts für verdächtige Verbindungen auf Seite 6-13](#)*
- *[Lösung für Browser-Schwachstellen auf Seite 6-14](#)*

Antiviren-Komponenten

Antivirus-Komponenten umfassen die folgenden Pattern, Treiber und Engines:

- *[Virus-Pattern auf Seite 6-3](#)*
- *[Viren-Scan-Engine auf Seite 6-4](#)*
- *[Virensuchtreiber auf Seite 6-5](#)*

- *IntelliTrap Pattern auf Seite 6-6*
- *IntelliTrap Ausnahme-Pattern auf Seite 6-6*
- *Pattern der Arbeitsspeicherprüfung auf Seite 6-6*

Virus-Pattern

Das auf dem agent-Endpunkt verfügbare Viren-Pattern richtet sich nach der auf dem agent verwendeten Suchmethode.

Weitere Informationen zu Suchmethoden finden Sie unter *Suchmethodentypen auf Seite 7-9*.

TABELLE 6-1. Virus-Pattern

SUCHMETHODE	PATTERN IN VERWENDUNG
Herkömmliche Suche	Das Viren-Pattern enthält Informationen, die OfficeScan dabei unterstützen, die neuesten Viren-/Malware-Bedrohungen und kombinierten Bedrohungen zu erkennen. Trend Micro erstellt und veröffentlicht mehrmals pro Woche und bei jeder Entdeckung besonders schädlicher Viren- oder Malware-Programme ein neues Viren-Pattern. Trend Micro empfiehlt, dass zeitgesteuerte automatische Updates mindestens ein Mal pro Stunde durchgeführt werden. Dies ist die Standardeinstellung bei allen ausgelieferten Produkten.

SUCHMETHODE	PATTERN IN VERWENDUNG
Intelligente Suche	Im intelligenten Suchmodus verwenden OfficeScan Agents zwei einfache Pattern, die zusammen denselben Schutz wie herkömmliche Anti-Malware- und Anti-Spyware-Pattern bieten. Eine Smart Protection Quelle hostet das Pattern der intelligenten Suche. Dieses Pattern wird stündlich aktualisiert und enthält die Mehrzahl der Pattern-Definitionen. 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. Die agent-Update-Adresse (der OfficeScan-Server oder eine benutzerdefinierte Update-Adresse) hostet das Agent-Pattern der intelligenten Suche. Dieses Pattern wird täglich aktualisiert und enthält alle anderen Pattern-Definitionen, die im Pattern der intelligenten Suche nicht gefunden wurden. Agents laden dieses Pattern aus der Update-Adresse genau so herunter, wie sie andere OfficeScan-Komponenten herunterladen. Weitere Informationen finden zu Pattern der intelligenten Suche und Agent-Pattern der intelligenten Suche finden Sie unter Pattern-Dateien von Smart Protection auf Seite 4-8.

Viren-Scan-Engine

Das Herzstück aller Trend Micro Produkte bildet die Scan Engine, die ursprünglich als Reaktion auf die ersten dateibasierten Endpunkt-Viren entwickelt wurde. In ihrer heutigen Form kann sie verschiedene [Viren und Malware auf Seite 7-2](#) erkennen. Die Scan Engine entdeckt ebenfalls kontrollierte Viren, die für Forschungszwecke 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

OfficeScan kann entdeckte Viren/Malware entfernen und die Integrität der Datei wiederherstellen.

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.

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. Dieser Treiber ist in zwei Versionen verfügbar. Es handelt sich dabei um TmXPFlt.sys und TmPreFlt.sys. TmXPFlt.sys wird für die Echtzeitkonfiguration der Viren-Scan-Engine und TmPreFlt.sys zur Überwachung der Benutzeraktionen verwendet.



Hinweis

Diese Komponente wird nicht in der Konsole angezeigt. Um die Version dieser Komponente zu überprüfen, wechseln Sie zum Ordner *<Installationsordner des Servers>* \PCCSRV\Pcent\Drv. Klicken Sie mit der rechten Maustaste auf die .sys-Datei, wählen Sie **Eigenschaften**, und navigieren Sie zur Registerkarte **Version**.

IntelliTrap Pattern

Das IntelliTrap Pattern (weitere Informationen hierzu finden Sie unter [IntelliTrap auf Seite E-7](#)). Das Pattern erkennt in Echtzeit komprimierte Dateien, die als ausführbare Dateien gepackt sind.

IntelliTrap Ausnahme-Pattern

Das IntelliTrap Ausnahme-Pattern enthält eine Liste "zulässiger" komprimierter Dateien.

Pattern der Arbeitsspeicherprüfung

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.

Damage Cleanup Services-Komponenten

Die Komponenten der Damage Cleanup Services umfassen die folgende Engine und Vorlage.

- *Viren-Cleanup-Engine auf Seite 6-7*
- *Viren-Cleanup-Template auf Seite 6-7*
- *Early Boot Cleanup Driver auf Seite 6-7*

Viren-Cleanup-Engine

Die Viren-Cleanup-Engine sucht und entfernt Trojaner und Trojaner-Prozesse. Diese Engine unterstützt 32-Bit- und 64-Bit-Plattformen.

Viren-Cleanup-Template

Die Viren-Cleanup-Template wird von der Viren-Cleanup-Engine verwendet, um Trojaner-Dateien oder -Prozesse zu erkennen und zu beseitigen.

Early Boot Cleanup Driver

Der Trend Micro Early Boot Cleanup Driver wird vor den Betriebssystemtreibern geladen und ermöglicht das Erkennen und Sperren von Boot-Rootkits. Nachdem der OfficeScan Agent geladen wurde, werden vom Trend Micro Early Boot Cleanup Driver die Damage Cleanup Services zum Säubern des Rootkits aufgerufen.

Anti-Spyware-Komponenten

Die Anti-Spyware-Komponenten umfassen die folgende Engine und die folgenden Patterns:

- *Spyware-Pattern auf Seite 6-8*

- *Spyware-Scan-Engine auf Seite 6-8*
- *Spyware-Aktivmonitor-Pattern auf Seite 6-8*

Spyware-Pattern

Das Spyware-Pattern erkennt Spyware/Grayware in Dateien und Programmen, Speichermodulen, der Windows Registrierung und URL-Verknüpfungen.

Spyware-Scan-Engine

Die Spyware-Scan-Engine sucht nach Spyware/Grayware und nimmt die entsprechenden Suchaktion vor. Diese Engine unterstützt 32-Bit- und 64-Bit-Plattformen.

Spyware-Aktivmonitor-Pattern

Das Spyware-Aktivmonitor-Pattern wird bei der Echtzeitsuche nach Spyware und 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.

Firewall-Komponenten

Die Firewall-Komponenten umfassen den folgenden Treiber und das folgende Pattern:

- *Treiber für die allgemeine Firewall auf Seite 6-9*
- *Pattern der allgemeinen Firewall auf Seite 6-9*

Treiber für die allgemeine Firewall

Der Treiber für die allgemeine Firewall wird mit dem Pattern der allgemeinen Firewall verwendet, um Netzwerkviren auf agent-Computern zu suchen. Dieser Treiber unterstützt 32-Bit- und 64-Bit-Plattformen.

Pattern der allgemeinen Firewall

Ähnlich dem Viren-Pattern unterstützt das Allgemeine Firewall-Pattern OfficeScan bei der Suche nach Virensignaturen (speziellen Abfolgen von Bits und Bytes, die auf einen Netzwerkvirus hinweisen).

Web-Reputation-Komponenten

Die Web Reputation-Komponente ist die URL-Filter-Engine.

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.

Komponenten der Verhaltensüberwachung

Die Komponenten der Verhaltensüberwachung umfassen die folgenden Pattern, Treiber und Dienste:

- *Erkennungs-Pattern der Verhaltensüberwachung auf Seite 6-10*
- *Treiber der Verhaltensüberwachung auf Seite 6-10*
- *Kerndienst der Verhaltensüberwachung auf Seite 6-10*
- *Pattern zur Konfiguration der Verhaltensüberwachung auf Seite 6-10*
- *Pattern für digitale Signaturen auf Seite 6-10*

- *Pattern der Richtliniendurchsetzung auf Seite 6-11*

Erkennungs-Pattern der Verhaltensüberwachung

Dieses Pattern enthält die Regeln für die Erkennung von verdächtigem Bedrohungsverhalten.

Treiber der Verhaltensüberwachung

Dieser Treiber im Kernelmodus überwacht Systemereignisse und leitet sie an den Kerndienst der Verhaltensüberwachung zwecks Durchsetzung von Sicherheitsrichtlinien weiter.

Kerndienst der Verhaltensüberwachung

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 Verhaltensüberwachungstreiber verwendet dieses Pattern, um normale Systemereignisse zu erkennen und diese bei der Durchsetzung von Sicherheitsrichtlinien auszuschließen.

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.

Pattern zum Auslösen der Arbeitsspeichersuche

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 6-6*](#).

Programme

OfficeScan nutzt die folgenden Programme und Produkt-Updates:

- [*OfficeScan Agent Programm auf Seite 6-11*](#)
- [*Info über Hotfixes, Patches und Service Packs auf Seite 6-12*](#)

OfficeScan Agent Programm

Das OfficeScan Agent-Programm dient dem Schutz vor Sicherheitsrisiken.

Info über 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://www.trendmicro.com/download/emea/?lng=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>`

Komponenten des Diensts für verdächtige Verbindungen

Der Dienst für verdächtige Verbindungen besteht aus der folgenden Liste und dem folgenden Pattern:

- *Globale C&C-IP-Liste auf Seite 6-13*
- *Pattern der Relevanzregel auf Seite 6-14*

Globale C&C-IP-Liste

Zusammen mit der Prüf-Engine für Netzwerkinhalte (Network Content Inspection Engine, NCIE) sorgt die globale C&C-IP-Liste dafür, dass Netzwerkverbindungen mit

bekannten C&C-Servern erkannt werden. NCIE erkennt Kontakte mit C&C-Servern in allen Netzwerkkanälen.

OfficeScan protokolliert alle Daten der Verbindungen mit Servern in der globalen C&C-IP-Liste, damit sie ausgewertet werden können.

Pattern der Relevanzregel

Der Dienst für verdächtige Verbindungen nutzt das Pattern der Relevanzregel für die Erkennung eindeutiger Malware-Signaturen in den Headern von Netzwerkpaketen.

Lösung für Browser-Schwachstellen

Die Lösung für Browser-Schwachstellen besteht aus den folgenden Pattern:

- *Pattern zur Erkennung von Browser-Schwachstellen auf Seite 6-14*
- *Pattern der Skriptanalyse auf Seite 6-14*

Pattern zur Erkennung von Browser-Schwachstellen

Dieses Pattern identifiziert die neuesten Webbrowser-Schwachstellen und verhindert, dass der Webbrowser eine Gefährdung darstellt.

Pattern der Skriptanalyse

Dieses Pattern analysiert Skripts in Webseiten und identifiziert bösartige Skripts.

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 einem Smart 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 6-2. 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.

UPDATE-OPTION	BESCHREIBUNG	EMPFEHLUNG
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.
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 6-3. 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.
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 6-4. Vom OfficeScan Server heruntergeladene Komponenten

KOMPONENTE	VERTEILUNG	
	HERKÖMMLICHE SUCHE AGENTS	INTELLIGENTE SUCHE AGENTS
Virenschutz		
Agent-Pattern der intelligenten Suche	Nein	Ja
Viren-Pattern	Ja	Nein
IntelliTrap Pattern	Ja	Ja
IntelliTrap Ausnahme-Pattern	Ja	Ja
Pattern der Arbeitsspeicherprüfung	Ja	Ja
Viren-Scan-Engine (32 Bit)	Ja	Ja
Viren-Scan-Engine (64 Bit)	Ja	Ja
Anti-spyware		
Spyware-Pattern	Ja	Ja
Spyware-Aktivmonitor-Pattern	Ja	Nein
Spyware-Scan-Engine (32 Bit)	Ja	Ja
Spyware-Scan-Engine (64 Bit)	Ja	Ja
Damage Cleanup Services		
Viren-Cleanup-Template	Ja	Ja
Viren-Cleanup-Engine (32 Bit)	Ja	Ja
Viren-Cleanup-Engine (64 Bit)	Ja	Ja
Early Boot Cleanup Driver (32 Bit)	Ja	Ja
Early Boot Cleanup Driver (64 Bit)	Ja	Ja
Firewall		

KOMPONENTE	VERTEILUNG	
	HERKÖMMLICHE SUCHE AGENTS	INTELLIGENTE SUCHE AGENTS
Pattern der allgemeinen Firewall	Ja	Ja
Komponenten der Verhaltensüberwachung		
Erkennungs-Pattern der Verhaltensüberwachung (32 Bit)	Ja	Ja
Treiber der Verhaltensüberwachung (32 Bit)	Ja	Ja
Kerndienst der Verhaltensüberwachung (32 Bit)	Ja	Ja
Erkennungs-Pattern der Verhaltensüberwachung (64 Bit)	Ja	Ja
Treiber der Verhaltensüberwachung (64 Bit)	Ja	Ja
Kerndienst der Verhaltensüberwachung (64 Bit)	Ja	Ja
Pattern zur Konfiguration der Verhaltensüberwachung	Ja	Ja
Pattern der Richtliniendurchsetzung	Ja	Ja
Pattern für digitale Signaturen	Ja	Ja
Pattern zum Auslösen der Arbeitsspeichersuche (32 Bit)	Ja	Ja
Pattern zum Auslösen der Arbeitsspeichersuche (64 Bit)	Ja	Ja
C&C-Kontaktalarmdienst		
Globale C&C-IP-Liste	Ja	Ja
Pattern der Relevanzregel	Ja	Ja

KOMPONENTE	VERTEILUNG	
	HERKÖMMLICHE SUCHE AGENTS	INTELLIGENTE SUCHE AGENTS
Lösung für Browser-Schwachstellen		
Pattern zur Erkennung von Browser-Schwachstellen	Ja	Ja
Pattern der Skriptanalyse	Ja	Ja

Update-Hinweise und -Empfehlungen:

- 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.
- Ein reiner IPv6 OfficeScan Server kann Updates nicht direkt an reine IPv4-agents verteilen. Analog kann ein reiner IPv4 OfficeScan Server Updates auch nicht direkt an reine IPv6-agents verteilen. Ein Dual-Stack-Proxy-Server wie beispielsweise DeleGate, der IP-Adressen konvertieren kann, muss ermöglichen, dass der OfficeScan Server Updates auf die agents verteilen kann.
- Damit der agent-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 6-23](#).
- 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 derzeitigen Komponenten-Versionen anzuzeigen und die Anzahl der aktualisierten und veralteten agents festzustellen.

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 6-26*.

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 konfigurieren

Prozedur

1. Navigieren Sie zu **Administration > Einstellungen > Proxy**.
 2. Klicken Sie auf die Registerkarte **Externer Proxy**.
 3. Navigieren Sie zum Abschnitt **Updates des OfficeScan Servers**.
 4. Wählen Sie **Für Pattern-, Engine- und Lizenz-Updates einen Proxy-Server verwenden** aus.
 5. Geben Sie das Proxy-Protokoll, den Servernamen oder die IPv4-/IPv6-Adresse sowie die Portnummer an.
 6. Falls der Proxy-Server eine Authentifizierung verlangt, geben Sie den Benutzernamen und das Kennwort ein.
 7. 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 6-21](#)*.

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 6-23](#).

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
- Agent-Pattern der intelligenten Suche
- Viren-Cleanup-Template

- IntelliTrap Ausnahme-Pattern
- Spyware-Pattern
- Spyware-Aktivmonitor-Pattern

Szenario einer Komponentenduplizierung

Das folgende Beispiel erläutert den Dupliziervorgang für den Server:

TABELLE 6-5. 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 6-21*.
 - 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 6-21*.
 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 6-30*.



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 6-28*.
 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 6-28*.
- **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 6-29*.

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 13-40*.

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 4-20*.

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 6-17*.

In der folgenden Tabelle sind alle Komponenten aufgeführt, die Update-Adressen auf agents verteilen, sowie die Komponenten, die bei Benutzung einer bestimmten Suchmethode verwendet werden.

TABELLE 6-6. OfficeScan Komponenten, die verteilt werden auf Agents

KOMPONENTE	VERTEILUNG	
	AGENTS DER HERKÖMMLICHEN SUCHE	AGENTS DER INTELLIGENTEN SUCHE:
Virenschutz		
Agent-Pattern der intelligenten Suche	Nein	Ja
Viren-Pattern	Ja	Nein
IntelliTrap Pattern	Ja	Ja
IntelliTrap Ausnahme-Pattern	Ja	Ja
Viren-Scan-Engine (32 Bit)	Ja	Ja
Viren-Scan-Engine (64 Bit)	Ja	Ja
Pattern der Arbeitsspeicherprüfung	Ja	Ja
Anti-spyware		
Spyware/Grayware-Pattern	Ja	Ja
Spyware-Aktivmonitor-Pattern	Ja	Nein
Spyware/Grayware-Scan-Engine (32 Bit)	Ja	Ja
Spyware/Grayware-Scan-Engine (64 Bit)	Ja	Ja
Damage Cleanup Services		
Damage Cleanup Template	Ja	Ja
Damage-Cleanup-Engine (32 Bit)	Ja	Ja
Damage-Cleanup-Engine (64 Bit)	Ja	Ja

KOMPONENTE	VERTEILUNG	
	AGENTS DER HERKÖMMLICHEN SUCHE	AGENTS DER INTELLIGENTEN SUCHE:
Early Boot Cleanup Driver (32 Bit)	Ja	Ja
Early Boot Cleanup Driver (64 Bit)	Ja	Ja
Web-Reputation-Dienste		
URL-Filter-Engine	Ja	Ja
Firewall		
Firewall-Pattern	Ja	Ja
Firewall-Treiber (32 Bit)	Ja	Ja
Firewall-Treiber (64 Bit)	Ja	Ja
Komponenten der Verhaltensüberwachung		
Erkennungs-Pattern der Verhaltensüberwachung (32 Bit)	Ja	Ja
Kerntreiber der Verhaltensüberwachung (32 Bit)	Ja	Ja
Kerndienst der Verhaltensüberwachung (32 Bit)	Ja	Ja
Erkennungs-Pattern der Verhaltensüberwachung (64 Bit)	Ja	Ja
Kerntreiber der Verhaltensüberwachung (64 Bit)	Ja	Ja
Kerndienst der Verhaltensüberwachung (64 Bit)	Ja	Ja
Pattern zur Konfiguration der Verhaltensüberwachung	Ja	Ja
Pattern der Richtliniendurchsetzung	Ja	Ja

KOMPONENTE	VERTEILUNG	
	AGENTS DER HERKÖMMLICHEN SUCHE	AGENTS DER INTELLIGENTEN SUCHE:
Pattern für digitale Signaturen	Ja	Ja
Pattern zum Auslösen der Arbeitsspeichersuche (32 Bit)	Ja	Ja
Pattern zum Auslösen der Arbeitsspeichersuche (64 Bit)	Ja	Ja
Verdächtige Verbindungen		
Globale C&C-IP-Liste	Ja	Ja
Pattern der Relevanzregel	Ja	Ja
Browser-Schwachstellen		
Pattern zur Erkennung von Browser-Schwachstellen	Ja	Ja
Pattern der Skriptanalyse	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 Agents auf Seite 6-34](#) und [Benutzerdefinierte Update-Adressen für OfficeScan Agents auf Seite 6-35](#).

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 Agents

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 6-33*](#).

Die Standard-Update-Adresse für OfficeScan Agents 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 Agents auf Seite 6-34](#) 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 Agents

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 Agents konfigurieren

Prozedur

1. Navigieren Sie zu **Updates > Agents > Update-Adresse**.
2. Wählen Sie **Benutzerdefinierte Update-Adresse**, und klicken Sie 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. Geben Sie die Update-Adresse an. Sie können einen Update-Agent auswählen, falls vorhanden, oder den URL einer benutzerdefinierten Adresse eingeben.

**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 agent-Updates finden Sie unter *OfficeScan Agent Update-Adressen auf Seite 6-33*.

5. Klicken Sie auf **Speichern**.
6. Verschiedene Aufgaben im angezeigten Fenster durchführen.
 - a. Wählen Sie eine der folgenden Einstellungen aus: Weitere Informationen darüber, wie diese Einstellungen funktionieren, finden Sie unter *OfficeScan Agent-Update-Prozess auf Seite 6-35*.
 - **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**
 - b. Wenn Sie mindestens einen Update-Agent als Quelle festgelegt haben, klicken Sie auf **Update-Agent - Analysebericht**, um einen Bericht zu erstellen, der den Update-Status der agents anzeigt. Weitere Informationen zum Bericht finden Sie unter [Update-Agent - Analysebericht auf Seite 6-67](#).
 - c. Klicken Sie auf den Link IP-Adressbereich, um eine Update-Adresse zu bearbeiten. Bearbeiten Sie im daraufhin angezeigten Fenster die Einstellungen, und klicken Sie auf **Speichern**.
 - d. Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Löschen**, um eine Update-Adresse aus der Liste zu entfernen.
 - e. Klicken Sie auf den Aufwärts- oder Abwärtspfeil, um eine Update-Adresse zu verschieben. Es kann jeweils nur eine Adresse verschoben werden.
7. 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 6-62](#) 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 6-7. 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. Navigieren Sie zum Abschnitt **Updates**.
 3. 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 6-52](#).

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-Computern durchführen.

TABELLE 6-8. 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 brauchen nur inkrementelle Pattern herunterzuladen. Dadurch wird weniger Zeit für die Aktualisierung benötigt (weitere Informationen zu inkrementellen Pattern finden Sie unter OfficeScan Server-Komponentenduplizierung auf Seite 6-23). Regelmäßige Updates können jedoch die Serverleistung negativ beeinflussen, insbesondere wenn eine hohe Anzahl von agents gleichzeitig aktualisiert wird. Wenn sich agents im Roaming-Modus befinden und Sie diese agents auch aktualisieren möchten, wählen Sie "Auch auf Roaming- und Offline-agent verteilen". Weitere Informationen zum Roaming-Modus finden Sie unter OfficeScan AgentRoaming-Berechtigungen auf Seite 14-20.
Agents beginnen nach dem Neustart und dem Herstellen einer Verbindung mit dem OfficeScan Server mit dem Komponenten-Update (Ausnahme: Roaming-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 (Ausnahme: Roaming-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 Download der Komponenten keine Update-Benachrichtigung an die 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 Address 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**
 - **Auch auf Roaming- und Offline-Agents verteilen**
 - **Agents beginnen nach dem Neustart und dem Herstellen einer Verbindung mit dem OfficeScan Server mit dem Komponenten-Update (Ausnahme: Roaming-Agents)**
 - **Nach dem Update 'Jetzt durchsuchen' ausführen (Ausnahme: Roaming-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 regelmäßig. 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, in dem der OfficeScan Server Benachrichtigungen zum Update der Komponenten an die agents versenden soll.



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 mehrmals 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: Roaming-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 Address 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 Agents 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 **Auch auf Roaming- und Offline-Agents verteilen**:
 - Roaming 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 Stammsymbol , um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
 - d. Klicken Sie auf **Komponenten-Update starten**.



Hinweis

Der Server benachrichtigt alle agent, 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, zum Beispiel "Jetzt aktualisieren" und zeitgesteuerte Updates aktivieren.

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. 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, versucht der 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 können Komponenten aktualisieren, aber kein Upgrade des Agents durchführen oder Hotfixes verteilen	Bei Aktivierung dieser Option können Komponenten-Updates durchgeführt werden, aber die Verteilung von Hotfixes und OfficeScan Agent-Upgrades wird verhindert.  Hinweis Durch Deaktivieren dieser Option kann die Serverleistung erheblich beeinträchtigt werden, da alle agents für das Upgrade oder zum Installieren eines Hotfixes gleichzeitig eine Verbindung zum Server herstellen.

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 für Agents auf Seite 14-54.
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.  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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

Reservierten Festplattenspeicher für OfficeScan Agents-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. Navigieren Sie zum Abschnitt **Reservierter Festplattenspeicher**.
 3. Wählen Sie **Reservieren__ MB des Festplattenspeichers für Updates** aus.
 4. Wählen Sie die gewünschte Speicherplatzmenge aus.
 5. 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 6-9. Beim Update von OfficeScan Agent-Komponenten verwendete Proxy-Einstellungen

UPDATE-METHODE	VERWENDETE PROXY-EINSTELLUNGEN	VERWENDUNG
Automatisches Update	• Automatische Proxy-Einstellungen. Weitere Informationen finden Sie unter Automatische Proxy-Einstellungen für OfficeScan Agent auf Seite 14-56. • Interne Proxy-Einstellungen. Weitere Informationen finden Sie unter Interner Proxy für OfficeScan Agents auf Seite 14-52.	1. OfficeScan Agents verwenden beim Komponenten-Update zunächst die automatischen Proxy-Einstellungen. 2. Sind keine automatischen Proxy-Einstellungen aktiviert, werden interne Proxy-Einstellungen verwendet. 3. Sind beide Optionen deaktiviert, verwenden die agents keine Proxy-Einstellungen.

UPDATE-METHODE	VERWENDETE PROXY-EINSTELLUNGEN	VERWENDUNG
Jetzt aktualisieren	• Automatische Proxy-Einstellungen. Weitere Informationen finden Sie unter Automatische Proxy-Einstellungen für OfficeScan Agent auf Seite 14-56. • Benutzerdefinierte Proxy-Einstellungen. Sie können agent-Benutzern die Berechtigung zur Konfiguration der Proxy-Einstellungen erteilen. Weitere Informationen finden Sie unter Proxy-Konfiguration – Berechtigungen für Agents auf Seite 14-54.	1. OfficeScan Agents verwenden beim Komponenten-Update zunächst die automatischen Proxy-Einstellungen. 2. Sind keine automatischen Proxy-Einstellungen aktiviert, werden benutzerkonfigurierte Proxy-Einstellungen verwendet. 3. Sind beide Optionen deaktiviert, oder sind die automatischen Proxy-Einstellungen deaktiviert und die agent-Benutzer verfügen nicht über die erforderliche Berechtigung, verwenden die agents beim Komponenten-Update keine Proxy-Einstellungen.

OfficeScan Agent-Update-Benachrichtigungen konfigurieren

OfficeScan benachrichtigt agent-Benutzer, wenn Update-bezogene Ereignisse auftreten.

Prozedur

1. Navigieren Sie zu **Agents > Globale Agent-Einstellungen**.
2. Navigieren Sie zum Abschnitt **Alarmeinstellungen**.
3. 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.

4. 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 13-40*.

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 Richtlinien Einhaltung 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 14-60](#).

Rollback der Komponenten durchführen für OfficeScan Agents

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 funktionieren, sollten Sie ein Rollback auf die vorherige Version durchführen. OfficeScan behält die aktuelle und die vorherige

Version der Viren-Scan-Engine und 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 Stammsymbol , 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 OfficeScan 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 <Zielfdateiname> <Quelldateiname>
```

Wobei gilt:

- **<Zielfdateiname>** 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 Zielfdatei an die Systemzeit des Endpunkts angepasst. Das Platzhalterzeichen (*) darf im Zielfdateinamen, 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 agents. Auf diese Weise erhalten die 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 Agents 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 Agents 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 Agents auf Seite 6-35*.



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 erste 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 6-23](#).

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 5-11*.

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 Agents auf Seite 6-35*.

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 Agents

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 7-59*
- *Allgemeine Sucheinstellungen auf Seite 7-76*
- *Benachrichtigungen bei Sicherheitsrisiken auf Seite 7-87*
- *Sicherheitsrisiko-Protokolle auf Seite 7-98*
- *Ausbrüche von Sicherheitsrisiken auf Seite 7-114*

Info über Sicherheitsrisiken

Sicherheitsrisiko ist der Oberbegriff für Viren/Malware und Spyware/Grayware. OfficeScan schützt Computer vor Sicherheitsrisiken. Hierbei werden zunächst Dateien durchsucht und anschließend wird eine bestimmte Aktion für jedes entdeckte Sicherheitsrisiko durchgeführt. Eine große Anzahl entdeckter Sicherheitsrisiken innerhalb kurzer Zeit deutet auf einen Virenausbruch hin. Durch Anwendung von Ausbruchspräventionsrichtlinien und die Isolierung infizierter Computer, bis keine Bedrohung mehr von ihnen ausgeht, kann OfficeScan helfen, schädliche Auswirkungen zu vermeiden bzw. zu minimieren. 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
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 böartigem Code bereitzustellen. Rootkits werden auf Systemen über Social Engineering, bei der Ausführung von Malware oder einfach durch das Surfen auf einer böartigen 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 Bedrohungszyklopädie: 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 Werbefbanner 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 bössartiger 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 unternehmensinterner 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 Haftungsansprüchen	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

OfficeScan Agents können bei der Suche nach Sicherheitsrisiken eine von zwei Suchmethoden anwenden: die intelligente Suche und die herkömmliche Suche.

- **Intelligente Suche**

Agents die die intelligente Suche anwenden, werden in diesem Dokument als **agents der intelligenten Suche** bezeichnet. agents der intelligenten Suche profitieren von der lokalen Suche und von webbasierten Abfragen, die die File-Reputation-Dienste ermöglichen.

- **Herkömmliche Suche**

Agents , die keine intelligente Suche anwenden, heißen **agents der herkömmlichen Suche**. Ein agent der herkömmlichen Suche speichert alle OfficeScan Komponenten auf dem agent 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 OfficeScan Server verwalteten agents die intelligente Suche verwenden, sofern Sie nach einer Erstinstallation nicht die Suchmethode über die Webkonsole ändern.

Wenn Sie den OfficeScan Server von einer früheren Version upgraden und das automatische agent-Upgrade aktiviert ist, verwenden alle vom Server verwalteten agents weiterhin die Suchmethode, die vor dem Upgrade konfiguriert wurde. Beispielsweise benutzen mit einem Upgrade von OfficeScan 10, das sowohl die intelligente Suche als auch die herkömmliche Suche unterstützt, alle agents mit intelligenter Suche, bei denen ein Upgrade durchgeführt wurde, weiterhin die intelligente Suche, und alle agents mit herkömmlicher Suche benutzen weiterhin 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-Adresse verfügbaren Komponenten, außer das Agent-Pattern der intelligenten Suche	Alle unter der Update-Adresse 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 Stammsymbol () , 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

Wechsel von der intelligenten Suche zur herkömmlichen Suche

Bedenken Sie Folgendes, wenn Sie die agents auf die herkömmliche Suche umschalten:

1. Anzahl der umzuschaltenden agents

Wenn Sie eine relativ kleine Anzahl von agents gleichzeitig umschalten, werden die Ressourcen von OfficeScan Server und Smart Protection Server effizient genutzt. Diese Server können andere wichtige Aufgaben ausführen, während agents ihre Suchmethoden ändern.

2. Timing

Wenn Sie wieder auf die herkömmliche Suche umschalten, werden die agents wahrscheinlich die vollständige Version des Viren-Patterns und des Spyware-Aktivmonitor-Patterns vom OfficeScan Server herunterladen. Diese Pattern-Dateien werden nur von den agents der herkömmlichen 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 auf den agents die Funktion "Jetzt aktualisieren", und aktivieren Sie sie wieder, nachdem die Umschaltung der agents zur intelligenten Suche beendet wurde.

3. Agent-Hierarchieeinstellungen

Die Suchmethode ist eine granulare Einstellung, die auf Stamm- oder Domänenebene oder für einen einzelnen agent festgelegt werden kann. Bei der Umschaltung zur herkömmlichen Suche können Sie tun:

- 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. Roaming-agents werden benachrichtigt, wenn sie wieder online gehen, oder, falls der agent über Berechtigungen für zeitgesteuerte Updates verfügt, wenn das zeitgesteuerte Update ausgeführt wird. Vergewissern Sie sich auch, dass der OfficeScan Server über die neuesten Komponenten verfügt, weil die 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 6-17.
Anzahl der umzuschaltenden agents	Wenn Sie eine relativ kleine Anzahl von agents gleichzeitig umschalten, werden die Ressourcen von OfficeScan Server effizient genutzt. Der OfficeScan Server kann andere wichtige Aufgaben ausführen, während agents ihre Suchmethoden ändern.

ÜBERLEGUNG	DETAILS
Timing	Wenn Sie zum ersten Mal auf die intelligente Suche umschalten, müssen agents die vollständige Version des Agent-Patterns der intelligenten Suche vom OfficeScan Server herunterladen. Das Pattern der intelligenten Suche 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 auf den agents 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 granulare Einstellung, die auf Stamm- oder Domänenebene oder für einen einzelnen agent 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. Ein agent, den Sie in diese Domäne verschieben, wird 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 individuelle 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 OfficeScan keine Sicherheitsrisiken erkennt, verbleibt die Datei an ihrem Speicherort und Benutzer können weiterhin auf die Datei zugreifen. Wenn OfficeScan 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 Such-Zwischenspeicher, 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 agents und Domänen bzw. für alle 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 Stammsymbol (🌐), 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 7-29*
 - *Zu durchsuchende Dateien auf Seite 7-29*
 - *Sucheinstellungen auf Seite 7-30*
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 7-40 • Gleiche Aktion für alle Arten von Viren/Malware auf Seite 7-42 • Bestimmte Aktion für jede Art von Viren/Malware auf Seite 7-42  Hinweis Weitere Informationen zu den einzelnen Aktionen finden Sie unter Viren-/Malware-Suchaktionen auf Seite 7-39. Zusätzliche Viren-/Malware-Aktionen: • Quarantäne-Ordner auf Seite 7-43 • Dateien vor dem Säubern sichern auf Seite 7-45 • Damage Cleanup Services auf Seite 7-45 • Bei Viren-/Malware-Fund Benachrichtigung anzeigen auf Seite 7-46 • Bei Viren-/Malware-Verdacht Benachrichtigung anzeigen auf Seite 7-46
Spyware-/Grayware-Aktion	Primäraktion: • Spyware-/Grayware-Suchaktionen auf Seite 7-52 Zusätzliche Spyware-/Grayware-Aktion: • Bei Spyware-/Grayware-Fund Benachrichtigung anzeigen auf Seite 7-53

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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 Stammsymbol () , 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 7-29](#)
- [Sucheinstellungen auf Seite 7-30](#)
- [CPU-Auslastung auf Seite 7-32](#)

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 7-40 • Gleiche Aktion für alle Arten von Viren/Malware auf Seite 7-42 • Bestimmte Aktion für jede Art von Viren/Malware auf Seite 7-42  Hinweis Weitere Informationen zu den einzelnen Aktionen finden Sie unter Viren-/Malware-Suchaktionen auf Seite 7-39. Zusätzliche Viren-/Malware-Aktionen: • Quarantäne-Ordner auf Seite 7-43 • Dateien vor dem Säubern sichern auf Seite 7-45 • Damage Cleanup Services auf Seite 7-45
Spyware-/Grayware-Aktion	Primäraktion: • Spyware-/Grayware-Suchaktionen auf Seite 7-52

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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 Stammsymbol () , 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**

Wenn Sie die Suche nach Viren/Malware deaktivieren, wird auch die Suche nach Spyware/Grayware deaktiviert.

5. Konfigurieren Sie auf der Registerkarte **Ziel** die folgenden Suchkriterien:
 - *Zeitplan auf Seite 7-33*
 - *Benutzerdefinierte Aktionen für Dateien auf Seite 7-29*
 - *Zu durchsuchende Dateien auf Seite 7-29*
 - *Sucheinstellungen auf Seite 7-30*
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 7-40 • Gleiche Aktion für alle Arten von Viren/Malware auf Seite 7-42 • Bestimmte Aktion für jede Art von Viren/Malware auf Seite 7-42  Hinweis Weitere Informationen zu den einzelnen Aktionen finden Sie unter Viren-/Malware-Suchaktionen auf Seite 7-39. Zusätzliche Viren-/Malware-Aktionen: • Quarantäne-Ordner auf Seite 7-43 • Dateien vor dem Säubern sichern auf Seite 7-45 • Damage Cleanup Services auf Seite 7-45 • Bei Viren-/Malware-Fund Benachrichtigung anzeigen auf Seite 7-46 • Bei Viren-/Malware-Verdacht Benachrichtigung anzeigen auf Seite 7-46
Spyware-/Grayware-Aktion	Primäraktion: • Spyware-/Grayware-Suchaktionen auf Seite 7-52 Zusätzliche Spyware-/Grayware-Aktion: • Bei Spyware-/Grayware-Fund Benachrichtigung anzeigen auf Seite 7-53

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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

Jetzt durchsuchen

"Jetzt durchsuchen" wird remote von OfficeScan Administratoren über die Webkonsole initialisiert und kann für einen oder mehrere agent-Computer ausgeführt werden.

Sie können die Einstellungen für 'Jetzt durchsuchen' für einen oder mehrere agents und Domänen bzw. für alle 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 Stammsymbol () , 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**

Wenn Sie die Suche nach Viren/Malware deaktivieren, wird auch die Suche nach Spyware/Grayware deaktiviert.

5. Konfigurieren Sie auf der Registerkarte **Ziel** die folgenden Suchkriterien:
 - *[Zu durchsuchende Dateien auf Seite 7-29](#)*
 - *[Sucheinstellungen auf Seite 7-30](#)*
 - *[CPU-Auslastung auf Seite 7-32](#)*
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): • <i>ActiveAction verwenden auf Seite 7-40</i> • <i>Gleiche Aktion für alle Arten von Viren/Malware auf Seite 7-42</i> • <i>Bestimmte Aktion für jede Art von Viren/Malware auf Seite 7-42</i>
	 Hinweis Weitere Informationen zu den einzelnen Aktionen finden Sie unter <i>Viren-/Malware-Suchaktionen auf Seite 7-39</i> .
	Zusätzliche Viren-/Malware-Aktionen: • <i>Quarantäne-Ordner auf Seite 7-43</i> • <i>Dateien vor dem Säubern sichern auf Seite 7-45</i> • <i>Damage Cleanup Services auf Seite 7-45</i>

AKTION	NACHSCHLAGEWERKE
Spyware-/Grayware-Aktion	Primäraktion: • Spyware-/Grayware-Suchaktionen auf Seite 7-52

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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

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 Systemarbeitspeicher 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 bis zur angegebenen Anzahl von Komprimierungsebenen sucht und tiefere Ebenen übergeht. OfficeScan säubert oder löscht auch 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 OfficeScan Agents, die von einem Server verwaltet werden, überprüfen diese Einstellung während der manuellen Suche, Echtzeitsuche, zeitgesteuerten Suche und 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 innerhalb einer Datei eingebettet ist, bei der zweiten Schicht handelt es sich um ein Microsoft Excel Tabellenblatt, das innerhalb des Word Dokuments eingebettet ist, und innerhalb des Tabellenblatts befindet

sich eine .exe-Datei (dritte Schicht). OfficeScan durchsucht das Word Dokument und das Excel Tabellenblatt 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*.

- **Bootbereich durchsuchen:** Durchsucht während der manuellen Suche, zeitgesteuerten Suche und der Funktion "Jetzt durchsuchen" den Bootsektor der Festplatte des agent Endpunkt 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 Montagstag oder an einem bestimmten Wochentag im Monat stattfinden sollen.

- **Ein bestimmter Montagstag:** 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.



Tip

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
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
.	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 Verzeichnisses 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>*

- 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™ for 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 zudem OfficeScan so, dass Microsoft Exchange 2000/2003 Verzeichnisse ausgeschlossen werden. Navigieren Sie dazu zum Abschnitt **Sucheinstellungen** von **Agents** > **Globale Agent-Einstellungen**. 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.

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 Dateierweiterung einer der Erweiterungen in dieser Ausschlussliste entspricht. Es können maximal 256 Dateierweiterungen angegeben werden. Ein Punkt (.) ist bei der Angabe der Dateierweiterung nicht erforderlich.

Bei der Angabe von Dateierweiterungen sollten Sie für die Echtzeitsuche ein Sternchen (*) als Platzhalterzeichen angeben. Wenn Sie beispielsweise alle Dateien nicht durchsuchen möchten, deren Erweiterung mit D beginnt, wie z. B. DOC, DOT oder DAT, geben Sie **D*** ein.

Verwenden Sie bei der manuellen Suche, zeitgesteuerten Suche und bei der Funktion "Jetzt durchsuchen" ein Fragezeichen (?) oder Sternchen (*) als Platzhalterzeichen.

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 später entfernte Chris JPG von der Ausschlussliste für die Echtzeitsuche, jedoch übernahm er die Suchausschlüsseinstellungen 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.
Quarantäne	OfficeScan benennt die infizierte Datei um und verschiebt sie anschließend in das temporäre Quarantäne-Verzeichnis auf dem agent Endpunkt unter dem Pfad <Installationsordner des Agents>\Suspect. Der OfficeScan Agent sendet anschließend die Dateien in Quarantäne an den vorgesehenen Quarantäne-Ordner. Weitere Informationen finden Sie unter Quarantäne-Ordner auf Seite 7-43. Das standardmäßige Quarantäne-Verzeichnis befindet sich auf dem OfficeScan Server unter dem Pfad <Installationsordner des Servers>\PCCSRV\Virus. OfficeScan verschlüsselt Dateien in Quarantäne, die an dieses Verzeichnis gesendet wurden. Mit der "Zentralen Quarantänewiederherstellung" können Sie beliebige Dateien in der Quarantäne wiederherstellen. Weitere Informationen finden Sie unter Dateien in der Quarantäne wiederherstellen auf Seite 7-47.

AKTION	BESCHREIBUNG
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.
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 infizierte 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
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.
Andere	Säubern	Quarantäne	Säubern	Quarantäne

VIREN-/MALWARE-TYP	ECHTZEITSUCHE		MANUELLE SUCHE/ ZEITGESTEUERTE SUCHE/JETZT DURCHSUCHEN	
	ERSTE AKTION	ZWEITE AKTION	ERSTE AKTION	ZWEITE AKTION
Wahrscheinlich Virus/Malware	Zugriff verweigern oder vom Benutzer konfigurierte Aktion	n. v.	Übergehen oder vom Benutzer konfigurierte Aktion	n. v.

Die Standardaktion bei Viren-/Malware-Verdacht ist während einer Echtzeitsuche die Option "Zugriff verweigern" und während einer manuellen Suche, einer zeitgesteuerten Suche und bei der Funktion "Jetzt durchsuchen" die Option "Übergehen". 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 7-48*.

Übernehmen Sie den Quarantäne-Ordner, der sich standardmäßig auf dem OfficeScan Server-Computer befindet. Das Verzeichnis ist im URL-Format und enthält den Host-Namen oder die IP-Adresse des Servers.

- Verwaltet der Server sowohl IPv4- als auch IPv6-agents, verwenden Sie den Host-Namen, damit alle agents Quarantäne-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-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-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. 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-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 OfficeScan Server-Computer	URL	http:// <osceserver>	Dabei handelt es sich um das Standardverzeichnis.
	UNC-Pfad	\\<osceserver>\ofcscan\Virus	Sie können die Einstellungen für dieses Verzeichnis konfigurieren, z. B. die Größe des Quarantäne-Ordners. Weitere Informationen finden Sie unter Quarantäne-Manager auf Seite 13-62 .
Ein Verzeichnis auf einem anderen OfficeScan Server-Computer (falls sich in Ihrem Netzwerk andere OfficeScan Server befinden)	URL	http:// <osceserver2>	Vergewissern Sie sich, dass 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".
	UNC-Pfad	\\<osceserver2>\ofcscan\Virus	
Anderer Endpunkt im Netzwerk	UNC-Pfad	\\<computer_name>\temp	
Ein anderes Verzeichnis auf dem OfficeScan Agent	Absoluter Pfad	C:\temp	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.

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 7-48*.

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 SHA1-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 7-106](#).

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 <i><Installationsordner des Agents>\SUSPECT\Backup</i> , 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 7-43 .
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
/u	Startet die Benutzeroberfläche des Tools
/r <Zielordner>	Der Ordner, in dem eine Datei wiederhergestellt wird

PARAMETER	BESCHREIBUNG
/s <Ursprünglicher Dateiname>	Der Dateiname der ursprünglich verschlüsselten Datei

Sie können beispielsweise VSEncode [/d] [/debug] eingeben, um Dateien im Ordner Suspect zu entschlüsseln und ein Debug-Protokoll zu erstellen. Wenn Sie eine Datei ent- oder verschlüsseln, erstellt 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 7-56.
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 zulässigen Spyware/Grayware auf Seite 7-54.
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 zulässigen Spyware/Grayware

OfficeScan 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 OfficeScan die Liste der zulässigen Software und führt bei einer Übereinstimmung keine Aktion aus.

Sie können die Liste der zulässigen Software auf einen oder mehrere agents und Domänen bzw. auf alle 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 zulässigen Spyware/Grayware** befindet.



Hinweis

Die OfficeScan Liste der zulässigen Spyware/Grayware kann maximal 1024 Einträge enthalten.

Die Liste der zulässigen Spyware/Grayware verwalten

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 > Liste der zulässigen 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. OfficeScan aktualisiert die Tabelle mit den Namen, die dem Schlüsselbegriff entsprechen.
5. Klicken Sie auf **Hinzufügen**.
Die Namen werden in die Tabelle **Zulässige Liste** 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 7-111](#)*.

Ausgeschlossene Prozesse verwalten

Sie können OfficeScan 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 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.



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 OfficeScan 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 Stammsymbol () , 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 CSV-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 CSV-Datei aus.
 - b. Klicken Sie auf **Importieren**.
9. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

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 7-60*.
- Benutzer können die zeitgesteuerte Suche verschieben, beenden oder überspringen. Weitere Informationen finden Sie unter *Zeitgesteuerte Suchberechtigungen und andere Einstellungen auf Seite 7-62*.
- 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 7-68*.
- Der OfficeScan Agent kann Cache-Einstellungen verwenden, um die Suchleistung zu verbessern. Weitere Informationen finden Sie unter *Cache-Einstellungen für die Suche auf Seite 7-70*.
- Die Benutzer können eine individuelle Liste der vertrauenswürdigen Programme anpassen. Weitere Informationen finden Sie unter *Berechtigung für die Liste der vertrauenswürdigen Programme auf Seite 7-74*.

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 Stammsymbol () , 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 für die Verschiebung unter **Agents > Globale Agent-Einstellungen** ändern. 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 Stammsymbol () , 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. Um die Anzahl der Minuten festzulegen, wechseln Sie zu **Agents > Globale Agent-Einstellungen**. Ändern Sie im Abschnitt **Einstellungen für zeitgesteuerte Suche** die Einstellung **Benutzer __ Minuten vor Suchbeginn an die zeitgesteuerte Suche erinnern**.

8. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

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**.

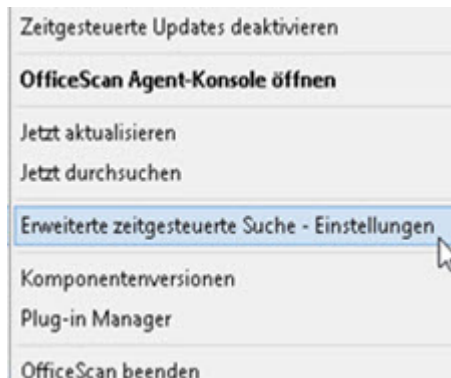


ABBILDUNG 7-2. Option Zeitgesteuerte Suche – Erweiterte Einstellungen



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 7-63](#).

- 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.

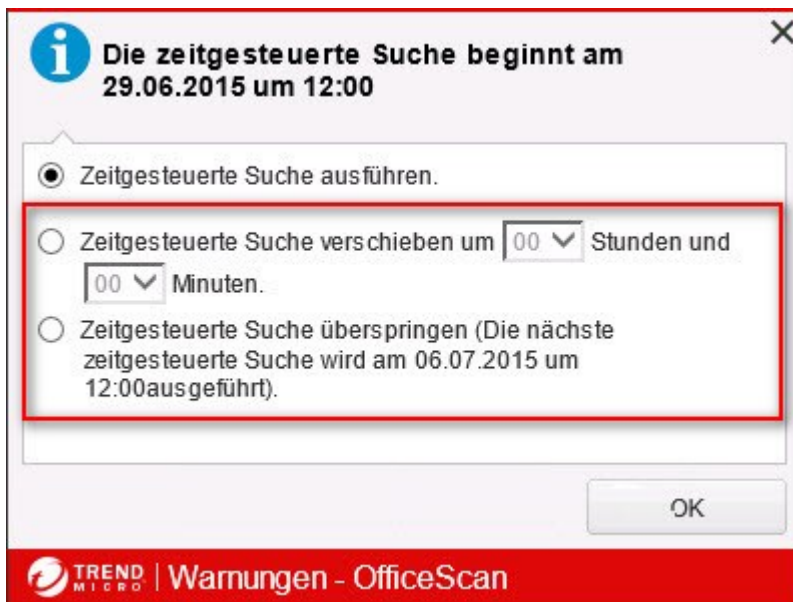


ABBILDUNG 7-3. Berechtigungen für die zeitgesteuerte Suche auf dem OfficeScan Agent Endpunkt

- 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.

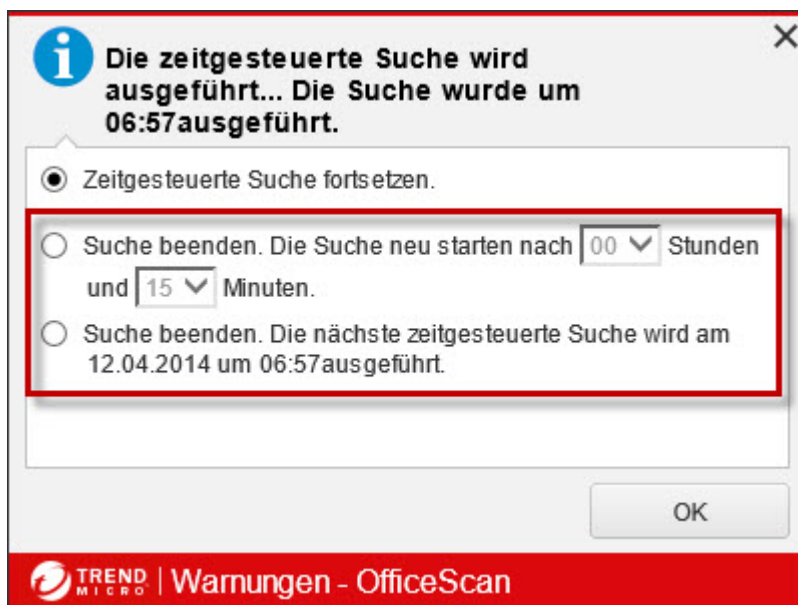


ABBILDUNG 7-4. Berechtigungen zur zeitgesteuerten Suche auf dem OfficeScan Agent Endpunkt

Mail-Scan-Berechtigungen und andere Einstellungen

Wenn 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 7-69. - 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 - Suchergebnisse werden nicht an den Server gesendet
Weitere Hinweise	Teilt sich den OfficeScan NT Proxy-Dienst (TMPProxy.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 Stammsymbol () , 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 wurde.

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-Serverplattformen automatisch deaktiviert (64-Bit-Unterstützung für Windows XP, 2003 und Vista ohne SP1 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 auf der Webkonsole konfiguriert werden kann. Agents wenden dieses Verfahren an, 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 nach vertrauenswürdigen 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-Endpunkt 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 Ausschluss 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 Stammsymbol () , 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 Stammsymbol () , 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

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. Konfigurieren Sie die allgemeinen Sucheinstellungen in jedem der verfügbaren Abschnitte.
 - *[Abschnitt "Sucheinstellungen" auf Seite 7-77](#)*
 - *[Abschnitt "Einstellungen für die zeitgesteuerte Suche" auf Seite 7-83](#)*
 - *[Abschnitt "Bandbreiteneinstellungen des Viren-/Malware-Protokolls" auf Seite 7-86](#)*
 3. Klicken Sie auf **Speichern**.
-

Abschnitt "Sucheinstellungen"

Im Abschnitt **Sucheinstellungen** des Fensters **Globale Agent-Einstellungen** können Administratoren Folgendes konfigurieren:

- *Manuelle Suche zum Windows Kontextmenü auf OfficeScan Agents hinzufügen auf Seite 7-77*
- *Den Ordner der OfficeScan Server-Datenbank von der Echtzeitsuche ausschließen auf Seite 7-78*
- *Ordner und Dateien des Microsoft Exchange-Servers von den Suchvorgängen ausschließen auf Seite 7-78*
- *Verzögerte Suche für Dateivorgänge aktivieren auf Seite 7-79*
- *Sucheinstellungen für große, komprimierte Dateien konfigurieren auf Seite 7-79*
- *Infizierte Dateien in komprimierten Dateien säubern/löschen auf Seite 7-80*
- *Bewertungsmodus aktivieren auf Seite 7-82*
- *Nach Cookies suchen auf Seite 7-83*

Manuelle Suche zum Windows Kontextmenü auf OfficeScan Agents 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.

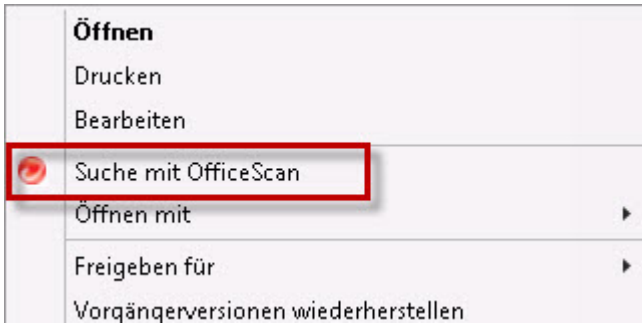


ABBILDUNG 7-6. Suche mit OfficeScan-Option

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 6-28*.

Sucheinstellungen für große, komprimierte Dateien konfigurieren

Alle OfficeScan Agents, die vom Server verwaltet werden, überprüfen bei der Durchsuchung komprimierter Dateien nach Viren/Malware und Spyware/Grayware während einer manuellen Suche, Echtzeitsuche, zeitgesteuerten Suche und der Funktion "Jetzt durchsuchen" die folgenden Einstellungen:

- **Sucheinstellungen für große, komprimierte Dateien konfigurieren:** Wählen Sie diese Option aus, um die Behandlung komprimierter Dateien festzulegen.

- Konfigurieren Sie die folgenden Einstellungen separat für die Echtzeitsuche und die anderen Suchtypen ("Manuelle Suche", "Zeitgesteuerte Suche", "Jetzt durchsuchen"):
 - **Keine Dateien in komprimierten Dateien durchsuchen, die größer als __ MB sind:** OfficeScan durchsucht keine Dateien, die diesen Grenzwert überschreiten.
 - **In einer komprimierten Datei nur die ersten __ Dateien durchsuchen:** Nach dem Entpacken der komprimierten Datei durchsucht OfficeScan die angegebene Anzahl von Dateien und ignoriert etwaige verbleibende Dateien.

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 (Umbenennen, 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 zulässigen 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 7-84*
- *Zeitgesteuerte Suche verschieben um __ Stunden und __ Minuten auf Seite 7-84*

- *Zeitgesteuerte Suche automatisch beenden, wenn die Suche länger dauert als __ Stunden und __ Minuten auf Seite 7-85*
- *Zeitgesteuerte Suche überspringen, wenn die Akkulaufzeit eines Wireless-Endpunkts weniger als __ % beträgt und der AC-Adapter nicht angeschlossen ist auf Seite 7-85*
- *Eine übersprungene zeitgesteuerte Suche fortsetzen auf Seite 7-85*

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 7-62*.

Abschnitt "Bandbreiteneinstellungen des Viren-/Malware-Protokolls"

Im Abschnitt "Bandbreiteneinstellungen des Viren-/Malware-Protokolls" der allgemeinen Sucheinstellungen können Administratoren Folgendes konfigurieren:

OfficeScan Agents so konfigurieren, dass sie für erneute Funde desselben Virus/ derselben Malware innerhalb einer Stunde nur einen Protokolleintrag erstellen auf Seite 7-86

OfficeScan Agents so konfigurieren, dass sie für erneute Funde desselben Virus/derselben Malware innerhalb einer Stunde nur einen Protokolleintrag erstellen

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.

Abschnitt "Certified Safe Software Services"

Im Abschnitt **Certified Safe Software Services** von **Allgemeine Sucheinstellungen** können Administratoren Folgendes konfigurieren:

Certified Safe Software Service für Verhaltensüberwachung, Firewall und Virensuchen aktivieren auf Seite 7-87

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 14-52*), 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.

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 7-88*.

Weitere Informationen zu den an OfficeScan Agent-Benutzer gesendeten Benachrichtigungen finden Sie unter *Benachrichtigungen bei Sicherheitsrisiken für OfficeScan Agent Benutzer auf Seite 7-94*.

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	<i>Benachrichtigungen bei Sicherheitsrisiken für Administratoren konfigurieren auf Seite 7-89</i>
Spyware/Grayware	<i>Benachrichtigungen bei Sicherheitsrisiken für Administratoren konfigurieren auf Seite 7-89</i>
Übertragungen digitaler Assets	<i>Benachrichtigung zur Funktion "Prävention vor Datenverlust" für Administratoren konfigurieren auf Seite 10-57</i>
C&C-Callbacks	<i>C&C-Callback-Benachrichtigungen für Administratoren konfigurieren auf Seite 11-19</i>



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 13-36*.

Benachrichtigungen bei Sicherheitsrisiken für Administratoren konfigurieren

Prozedur

1. Navigieren Sie zu **Administration > Benachrichtigungen > Administrator**.
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. Übernehmen oder ändern Sie die Standardbetreffzeile und -nachricht. Sie können Token-Variablen als Platzhalter für Daten in den Feldern **Betreff** und **Nachricht** verwenden.

TABELLE 7-22. Token-Variablen für Benachrichtigungen über Sicherheitsrisiken

VARIABLE	BESCHREIBUNG
Viren-/Malware-Funde	
%v	Viren-/Malware-Name
%s	Endpunkt mit Viren/Malware
%i	IP-Adresse des Endpunkts
%c	MAC-Adresse des Endpunkts
%m	Domäne des Endpunkts
%p	Fundort des Virus/der Malware
%y	Datum und Uhrzeit des Viren-/Malware-Funds
%e	Viren-Scan-Engine-Version
%r	Version der Viren-Pattern-Datei
%a	Für das Sicherheitsrisiko durchgeführte Aktionen
%n	Name des Benutzers, der am infizierten Endpunkt angemeldet ist
Spyware-/Grayware-Funde	
%s	Endpunkt mit Spyware/Grayware
%i	IP-Adresse des Endpunkts
%m	Domäne des Endpunkts
%y	Datum und Uhrzeit des Spyware-/Grayware-Funds
%n	Name des Benutzers, der zum Zeitpunkt des Funds 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	Viren-/Malware-Name
%s	Endpunkt mit Viren/Malware
%i	IP-Adresse des Endpunkts
%c	MAC-Adresse des Endpunkts
%m	Domäne des Endpunkts
%p	Fundort des Virus/der Malware
%y	Datum und Uhrzeit des Viren-/Malware-Funds
%e	Viren-Scan-Engine-Version
%r	Version der Viren-Pattern-Datei
%a	Für das Sicherheitsrisiko durchgeführte Aktionen
%n	Name des Benutzers, der am infizierten Endpunkt angemeldet ist
Spyware-/Grayware-Funde	
%s	Endpunkt mit Spyware/Grayware
%i	IP-Adresse des Endpunkts
%m	Domäne des Endpunkts

VARIABLE	BESCHREIBUNG
%y	Datum und Uhrzeit des Spyware-/Grayware-Funds
%n	Name des Benutzers, der zum Zeitpunkt des Funds am Endpunkt angemeldet ist
%T	Spyware-/Grayware-Suchergebnis
%v	Spyware-/Grayware-Name
%a	Für das Sicherheitsrisiko durchgeführte Aktionen

5. Auf der Registerkarte **NT-Ereignisprotokoll**:

- Gehen Sie zum Abschnitt **Viren/Malware Fund** oder **Spyware/Grayware Fund**.
- Wählen Sie **Benachrichtigung über NT-Ereignisprotokoll aktivieren**.
- 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	Viren-/Malware-Name
%s	Endpunkt mit Viren/Malware
%i	IP-Adresse des Endpunkts
%c	MAC-Adresse des Endpunkts
%m	Domäne des Endpunkts
%p	Fundort des Virus/der Malware
%y	Datum und Uhrzeit des Viren-/Malware-Funds

VARIABLE	BESCHREIBUNG
%e	Viren-Scan-Engine-Version
%r	Version der Viren-Pattern-Datei
%a	Für das Sicherheitsrisiko durchgeführte Aktionen
%n	Name des Benutzers, der am infizierten Endpunkt angemeldet ist
Spyware-/Grayware-Funde	
%s	Endpunkt mit Spyware/Grayware
%i	IP-Adresse des Endpunkts
%m	Domäne des Endpunkts
%y	Datum und Uhrzeit des Spyware-/Grayware-Funds
%n	Name des Benutzers, der zum Zeitpunkt des Funds am Endpunkt angemeldet ist
%T	Spyware-/Grayware-Suchergebnis
%v	Spyware-/Grayware-Name
%a	Für das Sicherheitsrisiko durchgeführte Aktionen

6. Klicken Sie auf **Speichern**.

Benachrichtigungen bei Sicherheitsrisiken für OfficeScan Agent Benutzer

OfficeScan kann Benachrichtigungen auf OfficeScan Agent Endpunkt 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 agent-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	<i>Viren/Malware-Benachrichtigungen konfigurieren auf Seite 7-96</i>
Spyware/Grayware	<i>Spyware-/Grayware-Benachrichtigungen konfigurieren auf Seite 7-97</i>
Firewall-Verstöße	<i>Den Inhalt der Firewall-Benachrichtigung ändern auf Seite 12-31</i>
Verstöße gegen die Web Reputation	<i>Benachrichtigungen über Internet-Bedrohungen ändern auf Seite 11-18</i>
Verstöße gegen die Gerätesteuerung	<i>Gerätesteuerungsbenachrichtigungen ändern auf Seite 9-18</i>
Verstöße gegen eine Verhaltensüberwachungs-Richtlinie	<i>Inhalt der Benachrichtigung ändern auf Seite 8-16</i>
Übertragungen digitaler Assets	<i>Benachrichtigung zur Funktion "Prävention vor Datenverlust" für Agents konfigurieren auf Seite 10-60</i>
C&C-Callbacks	<i>Benachrichtigungen über Internet-Bedrohungen ändern auf Seite 11-18</i>

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 Stammsymbol () , 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

Viren/Malware-Benachrichtigungen konfigurieren

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 Stammsymbol (🌐), 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 13-40](#).

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 Stammsymbol () , um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
 3. Klicken Sie auf **Protokolle > Viren-/Malware-Protokolle** oder **Protokolle anzeigen > 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:
 - Datum und Uhrzeit des Viren-/Malware-Funds
 - Endpunkt
 - Sicherheitsbedrohung
 - Infizierte Quelle
 - Infizierte(s) Datei/Objekt
 - Suchtyp, der Viren/Malware entdeckt hat
 - Suchergebnis

**Hinweis**

Weitere Informationen zu Suchergebnissen finden Sie unter [Viren-/Malware-Suchergebnisse auf Seite 7-100](#).

- IP-Adresse
 - MAC-Adresse
 - Protokolldetails (Klicken Sie auf **Anzeigen**, um die Details anzuzeigen.)
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.

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.

ERGEBNIS	BESCHREIBUNG
	• "Wahrscheinlich Virus oder Malware" wurde während der Echtzeitsuche erkannt. • 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 Endpunkt beschädigt werden könnte. Führen Sie eine manuelle Suche aus, damit OfficeScan die Datei säubern oder in Quarantäne verschieben kann.
Übergangen	• Die erste Aktion ist „Übergehen“. OfficeScan hat 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 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/de/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 <i>Datei konnte nicht in Quarantäne verschoben/umbenannt werden auf Seite 7-102</i>.
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 <i>Datei konnte nicht gelöscht werden auf Seite 7-102</i>.
Datei konnte nicht gesäubert oder	Die erste Aktion ist „Säubern“. Die zweite Aktion ist „Umbenennen“, und beide Aktionen sind fehlgeschlagen.

ERGEBNIS	BESCHREIBUNG
umbenannt werden.	Lösung: Siehe <i>Datei konnte nicht in Quarantäne verschoben/umbenannt werden auf Seite 7-102.</i>
Datei konnte nicht in Quarantäne verschoben/umbenannt werden	Erklärung 1 Die infizierte Datei wird möglicherweise von einer anderen Anwendung gesperrt, gerade ausgeführt oder befindet sich auf einer CD. OfficeScan verschiebt die Datei in Quarantäne oder benennt sie um, nachdem sie wieder verfügbar ist oder ausgeführt wurde. Lösung Bei infizierten Dateien auf einer CD sollten Sie die CD nicht verwenden, da der Virus andere Computer 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 möglicherweise in einer komprimierten Datei, und die Einstellung Infizierte Dateien in komprimierten Dateien säubern/löschen unter Agents > Globale Agent-Einstellungen 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 wird möglicherweise von einer anderen Anwendung gesperrt, gerade ausgeführt oder befindet sich auf einer CD. OfficeScan löscht die Datei, nachdem sie wieder verfügbar ist oder ausgeführt wurde. Lösung Bei infizierten Dateien auf einer CD sollten Sie die CD nicht verwenden, da der Virus andere Computer im Netzwerk infizieren könnte. Erklärung 3 Die infizierte Datei befindet sich im Ordner "Temporary Internet Files" auf dem OfficeScan Agent-Endpunkt. Da der Endpunkt die Dateien während des Surfs 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 die Datei in den Ordner \Suspect auf dem OfficeScan Agent Endpunkt in Quarantäne verschoben hat, kann sie nicht an den angegebenen Quarantäne-Ordner gesendet werden. Lösung Überprüfen Sie, bei welchem Suchtyp (manuelle Suche, Echtzeitsuche, zeitgesteuerte Suche oder "Jetzt durchsuchen") die Viren/die Malware entdeckt wurden, sowie den Quarantäne-Ordner, der auf der Registerkarte Agents > Agent-Verwaltung > Einstellungen > {Suchtyp} > Aktion angegeben ist. 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.

ERGEBNIS	BESCHREIBUNG
	2. Bei Quarantäne-Ordern im URL-Format: - Vergewissern Sie sich, dass der nach http:// angegebene Endpunktname korrekt ist. - 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. - 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): - Überprüfen Sie die Verbindung zwischen OfficeScan Agent und Endpunkt. - Stellen Sie sicher, dass der Quarantäne-Ordner für die Gruppe „Jeder“ freigegeben ist, und dass Sie dieser Gruppe Lese- und Schreibberechtigungen zugewiesen haben. - Überprüfen Sie, ob der Quarantäne-Ordner vorhanden ist. - Überprüfen Sie, ob der UNC-Pfad korrekt ist. Wenn sich der Quarantäne-Ordner in einem anderen Ordner auf dem OfficeScan Agent Endpunkt befindet (Sie können nur den absoluten Pfad für dieses Szenario verwenden), überprüfen Sie, ob der Quarantäne-Ordner vorhanden ist.

ERGEBNIS	BESCHREIBUNG
Die Datei konnte nicht gesäubert werden	Erklärung 1 Die infizierte Datei befindet sich möglicherweise in einer komprimierten Datei, und die Einstellung „Infizierte Dateien in komprimierten Dateien säubern/löschen“ unter Agents > Globale Agent-Einstellungen 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 Temporary Internet Files 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-17.
Aktion erforderlich	OfficeScan kann die konfigurierte Aktion für die infizierte Datei nicht ohne Eingreifen eines Benutzers abschließen. Bewegen Sie 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

ERGEBNIS	BESCHREIBUNG
	'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 – Führen Sie eine vollständige Systemsuche durch.“

Protokolle der zentralen Quarantänewiederherstellung anzeigen

Nach dem Säubern von Malware sichern die OfficeScan Agents die Malware-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 Malware-Sicherungsdaten wiederhergestellt wurden, welcher Endpunkt betroffen 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 erstellt Protokolle, wenn er Spyware oder Grayware 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 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. Sehen Sie die Protokolle ein. Die Protokolle enthalten die folgenden Informationen:
 - Datum und Uhrzeit des Spyware-/Grayware-Funds
 - Betroffen Endpunkt
 - Spyware-/Grayware-Name

- Suchtyp, der Spyware/Grayware entdeckt hat
 - Einzelheiten über die Spyware-/Grayware-Suchergebnisse (ob die Suchaktion erfolgreich durchgeführt werden konnte oder nicht) Weitere Informationen finden Sie unter [Spyware-/Grayware-Suchergebnis auf Seite 7-108](#).
 - IP-Adresse
 - MAC-Adresse
 - Protokolldetails (Klicken Sie auf **Anzeigen**, um die Details anzuzeigen.)
6. Fügen Sie der Liste der zulässigen Spyware/Grayware die Spyware/Grayware hinzu, die Sie als harmlos erachten.
7. 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.

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

ERGEBNIS	BESCHREIBUNG
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: • <i>Übergangen</i> • <i>Die Spyware/Grayware richtet beim Säubern möglicherweise Schaden an</i> • <i>Suche nach Spyware/Grayware wurde vorzeitig beendet. Führen Sie eine vollständige Suche durch</i> • <i>Spyware/Grayware gesäubert. Neustart erforderlich. Starten Sie den Computer neu</i> • <i>Spyware/Grayware kann nicht entfernt werden</i> • <i>Unbekanntes Spyware-/Grayware-Suchergebnis. Wenden Sie sich an den technischen Support von Trend Micro</i>

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 zulässigen Spyware/Grayware die Spyware/Grayware hinzu, die Sie als harmlos erachten.

ERGEBNIS	BESCHREIBUNG	LÖSUNG
Die Spyware/Grayware richtet beim Säubern möglicherweise Schaden an	: Diese Nachricht informiert Sie, ob die Spyware Scan Engine versucht, einen Ordner zu säubern, 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 E:).	Wenden Sie sich an Ihren Support-Anbieter.
Suche nach Spyware/Grayware wurde vorzeitig 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.
Spyware/Grayware gesäubert. Neustart erforderlich. Starten Sie den Computer neu	OfficeScan hat die Spyware-/Grayware-Komponenten gesäubert. Um den Vorgang abzuschließen, ist ein Neustart des Endpunkts erforderlich.	Starten Sie den Endpunkt umgehend neu.
Spyware/Grayware kann nicht entfernt werden	Spyware/Grayware wurde auf einer CD-ROM oder einem Netzlaufwerk erkannt. OfficeScan kann an diesem Speicherort erkannte Spyware/Grayware nicht säubern.	Entfernen Sie die infizierte Datei manuell.

ERGEBNIS	BESCHREIBUNG	LÖSUNG
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 7-100](#).

- 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 Suchprotokoll, das Informationen über die 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 agents erzwungen oder der OfficeScan Echtzeitsuchdienst wurde unerwarteterweise 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 der Spyware-Pattern-Datei

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 eine Benachrichtigung erhalten, wenn folgende Ereignisse auftreten:

TABELLE 7-29. Typen von Sicherheitsrisiko-Ausbruchsbenachrichtigungen

Typ	NACHSCHLAGEWERKE
• Viren/Malware • Spyware/Grayware • Freigabebesitzung	<i>Ausbruchskriterien und Benachrichtigungen für Sicherheitsrisiken konfigurieren auf Seite 7-115</i>
Firewall-Verstöße	<i>Kriterien für den Ausbruch von Verstößen gegen die Firewall und Benachrichtigungen konfigurieren auf Seite 12-33</i>
C&C-Callbacks	<i>C&C-Callback-Ausbruchskriterien und -Benachrichtigungen konfigurieren auf Seite 11-24</i>

- Viren-/Malware-Ausbruch
- Spyware-/Grayware-Ausbruch
- Ausbruch von Firewall-Verstößen
- Ausbruch bei Freigabesitzung

Ein Ausbruch wird durch die Anzahl der Vorfälle in einem bestimmten Zeitraum definiert. Ein Ausbruch wird angezeigt, wenn die Anzahl der Funde während des festgelegten Zeitraums die festgelegte Anzahl überschreitet.

OfficeScan verfügt über zahlreiche Standardbenachrichtigungen, die Sie und andere OfficeScan Administratoren über Ausbrüche informieren. Sie können diese Benachrichtigungen ändern und zusätzliche Benachrichtigungseinstellungen konfigurieren, die Ihren Anforderungen entsprechen.



Hinweis

OfficeScan kann Benachrichtigungen über Sicherheitsrisiko-Ausbrüche per E-Mail, SNMP-Trap und Windows NT Ereignisprotokolle senden. Bei Ausbrüchen bei 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 13-36](#).

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 7-117](#)*.
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 7-117](#)*.
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 Stammsymbol () , 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 7-120](#)*
 - *[Gefährdete Ports sperren auf Seite 7-121](#)*
 - *[Schreibzugriff auf Dateien und Ordner verweigern auf Seite 7-123](#)*
 - *[Zugriff auf ausführbare komprimierte Dateien verweigern auf Seite 7-125](#)*
 - *[Mutex-Behandlung von Malware-Prozessen/-Dateien auf Seite 7-124](#)*

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 7-120*
- *Gefährdete Ports sperren auf Seite 7-121*
- *Schreibzugriff auf Dateien und Ordner verweigern auf Seite 7-123*
- *Zugriff auf ausführbare komprimierte Dateien verweigern auf Seite 7-125*
- *Mutex-Behandlung von Malware-Prozessen/-Dateien auf Seite 7-124*

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 Stammsymbol () , 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
 - **Vollständigen 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

Bei einem Ausbruch können Sie gefährdete Ports sperren, die Viren und Malware für den Zugriff auf OfficeScan Agent-Computer verwenden 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 Stammsymbol () , 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 **Gespernte 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.
 - **Häufig verwendete Ports:** Wählen Sie wenigstens eine Portnummer für OfficeScan, um die Einstellungen zum Sperren von Ports zu speichern.
 - **Trojaner-Ports:** Sperrt Ports, die häufig von Trojanern verwendet werden. Weitere Informationen finden Sie unter [Trojanerports auf Seite E-14](#).
 - **Eine Portnummer 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 Stammsymbol () , 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 Stammsymbol () , 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 Stammsymbol (🌐), 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

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 8-2*
- *Einstellungen der globalen Verhaltensüberwachung konfigurieren auf Seite 8-10*
- *Verhaltensüberwachungsberechtigungen auf Seite 8-13*
- *Benachrichtigungen der Verhaltensüberwachung für OfficeScan Agent-Benutzer auf Seite 8-15*
- *Verhaltensüberwachungsprotokolle auf Seite 8-16*

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 weder Windows XP noch Windows 2003 64-Bit-Plattformen.
 - Die Verhaltensüberwachung unterstützt Windows Vista 64-Bit-Plattformen mit SP1 oder höher.
 - Die Verhaltensüberwachung ist auf allen Versionen von Windows Server 2003, Windows Server 2008 und Windows Server 2012 standardmäßig deaktiviert. Vor der Aktivierung der Verhaltensüberwachung auf diesen Serverplattformen lesen Sie die unter *OfficeScan Agent Dienste auf Seite 14-7* beschriebenen Richtlinien und bewährten Methoden.
-

Sperrung bei Malware-Verhalten

Die Sperrung bei Malware-Verhalten bietet eine für zusätzlichen Schutz vor Bedrohungen durch Programme, die ein bösesartiges 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 bösesartiges Verhalten und sperrt die entsprechenden Programme. Verwenden Sie diese Funktion, um einen besseren Schutz vor neuen, unbekannten und aufkommenden Bedrohungen zu gewährleisten.

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.

Wenn ein Programm gesperrt wird und Benachrichtigungen aktiviert sind, zeigt OfficeScan auf dem OfficeScan Agent-Endpunkt eine Benachrichtigung an. Weitere Informationen zu Benachrichtigungen finden Sie unter [Benachrichtigungen der Verhaltensüberwachung für OfficeScan Agent-Benutzer auf Seite 8-15](#).

Ransomware-Schutz

Ransomware-Schutz verhindert die nicht autorisierte Änderung oder Verschlüsselung von Dateien auf OfficeScan Agents durch „Ransomware“-Bedrohungen. Ransomware ist eine Art von Malware, die den Zugriff auf Dateien einschränkt und die Wiederherstellung der betroffenen Dateien in Rechnung stellt.

Sie können die Verhaltensüberwachung so konfigurieren, dass diese eine bestimmte Sequenz von Ereignissen erkennt, die auf einen Ransomware-Angriff hinweisen. Wenn die Verhaltensüberwachung alle der folgenden Kriterien erfüllt, beendet OfficeScan das infizierte Programm und stellt es in die Quarantäne.

1. Ein Prozess, der nicht als sicher eingestuft wird, wenn versucht wird, drei Dateien innerhalb eines bestimmten Zeitraums zu ändern, zu löschen oder umzubenennen.
2. Der Prozess hat versucht, eine geschützte Dateierweiterung zu ändern.



Warnung!

OfficeScan kann die ersten Dateien nicht wiederherstellen, die vom Ransomware-Prozess betroffen sind.



Hinweis

Um zu vermeiden, dass OfficeScan einen sicheren Prozess als bösartig einstuft, stellen Sie sicher, dass OfficeScan Agent Zugriff auf das Internet hat, um weitere Verifizierungsprozesse unter Verwendung von Trend Micro Servern durchzuführen.

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 8-1. 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.

EREIGNISSE	BESCHREIBUNG
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.
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.

EREIGNISSE	BESCHREIBUNG
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 8-2. Aktionen bei überwachten Systemereignissen

AKTION	BESCHREIBUNG
Bewerten	OfficeScan lässt mit einem Ereignis verbundene Programme immer zu, zeichnet diese Aktion aber in den Protokollen zur Bewertung auf. Dies ist die Standardaktion für alle überwachten Systemereignisse.  Hinweis Diese Option wird nicht für DLL-Injektionen auf 64-Bit-Systemen unterstützt.
Zulassen	OfficeScan lässt mit einem Ereignis verbundene Programme immer zu.

AKTION	BESCHREIBUNG
Bei Bedarf nachfragen	OfficeScan fordert Benutzer auf, mit einem Ereignis verbundene Programme zuzulassen oder abzulehnen und die Programme der Ausschlussliste hinzuzufügen. Wenn der Benutzer nicht in einem bestimmten Zeitraum reagiert, lässt OfficeScan 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 8-10.  Hinweis Diese Option wird nicht für DLL-Injektionen auf 64-Bit-Systemen unterstützt.
Verweigern	OfficeScan sperrt alle mit einem Ereignis verbundenen Programme und zeichnet diese Aktion in den Protokollen auf. Wenn ein Programm gesperrt wird und Benachrichtigungen aktiviert sind, zeigt OfficeScan auf dem OfficeScan-Computer eine Benachrichtigung an. Weitere Informationen zu Benachrichtigungen finden Sie unter Benachrichtigungen der Verhaltensüberwachung für OfficeScan Agent-Benutzer auf Seite 8-15.

Ausschlussliste für Verhaltensüberwachung

Die Ausschlussliste für die Verhaltensüberwachung enthält Programme, die von der Verhaltensüberwachung nicht überprüft werden.

- **Genehmigte Programme:** Programme in dieser Liste können ausgeführt werden. Ein genehmigtes Programm wird von anderen OfficeScan Funktionen (wie der dateibasierten Suche) überprüft, bevor deren Ausführung zugelassen wird.
- **Gesperrte Programme:** Programme in dieser Liste können nie ausgeführt werden. Zum Konfigurieren dieser Liste muss die Ereignisüberwachung aktiviert sein.

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 8-13](#).

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 Stammsymbol () , um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
3. Klicken Sie auf **Einstellungen > Einstellungen der Verhaltensüberwachung**.
4. Sperren des Malware-Verhaltens aktivieren:
 - a. Wählen Sie **Sperrung bei Malware-Verhalten für bekannte und potenzielle Bedrohungen aktivieren**, und wählen Sie eine der folgenden Optionen aus:
 - **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 bössartige Verhaltensweisen
 - 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.
 - **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.

Weitere Informationen finden Sie unter [Ransomware-Schutz auf Seite 8-3](#).

5. Konfigurieren Sie die Einstellungen der Verhaltensüberwachung.
 - 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 8-4](#).

6. Konfigurieren Sie die Ausschlusslisten.
 - a. Geben Sie unter **Geben Sie den vollständigen Programmpfad ein** den vollständigen Pfad des Programms ein, das zugelassen oder gesperrt werden soll. Trennen Sie mehrere Einträge durch Strichpunkte (;) voneinander.
 - 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 maximal 100 zugelassene Programme und 100 gesperrte Programme möglich.

7. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser

Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

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. Navigieren Sie zum Abschnitt **Einstellungen der Verhaltensüberwachung**.
3. Konfigurieren Sie folgende Einstellungen bei Bedarf:

OPTIONEN	BESCHREIBUNG
Programm automatisch zulassen, wenn keine Reaktion vom Benutzer innerhalb von — Sekunden	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 8-4 .

OPTIONEN	BESCHREIBUNG
Benutzer fragen, bevor neu erkannte Programme ausgeführt werden, die über HTTP oder E-Mail-Anwendungen (Server-Plattformen ausgenommen) heruntergeladen wurden	Zusammen mit den Web-Reputation-Diensten überprüft die Verhaltensüberwachung die bisherige Verbreitung von Dateien, die über HTTP-Kanäle oder E-Mail-Anwendungen heruntergeladen werden. 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: • HTTP: .exe-Dateien werden überprüft. • E-Mail-Anwendungen: .exe-Dateien und komprimierte .exe-Dateien in unverschlüsselten .zip- und .rar-Dateien werden überprüft.  Hinweis • Damit diese Systemaufforderung angezeigt werden kann, müssen Administratoren die Web-Reputation-Dienste auf dem agent aktivieren und OfficeScan damit die Überwachung des HTTP-Datenverkehrs ermöglichen. • Für Windows 7/Vista/XP Systeme unterstützt diese Eingabeaufforderung nur die Ports 80, 81 und 8080. • OfficeScan stimmt mit den Dateinamen überein, die während des Ausführungsvorgangs über E-Mail-Anwendungen heruntergeladen wurden. Wenn der Dateiname geändert wurde, erhält der Benutzer eine Eingabeaufforderung.

4. 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 14-52](#)), 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 **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 8-1. 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 Stammsymbol () , 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 Stammsymbol () , 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser

Option werden die Einstellungen nicht auf Agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

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. Sie können die Standardmeldung im dafür vorgesehenen Textfeld bearbeiten.
 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 13-40](#).

Verhaltensüberwachungsprotokolle anzeigen

Prozedur

1. Navigieren Sie zu **Protokolle > Agents > Sicherheitsrisiken** oder **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 > 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
 - Endpunkt , auf dem der unbefugte Prozess erkannt wurde
 - Endpunkt-Domäne
 - 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
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 ofscan.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 9

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 9-2*
- *Berechtigungen für Speichergeräte auf Seite 9-4*
- *Berechtigungen für Nicht-Speichergeräte auf Seite 9-11*
- *Gerätesteuerungsbenachrichtigungen ändern auf Seite 9-18*
- *Protokolle der Gerätesteuerung auf Seite 9-19*

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 OfficeScan Administratoren 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 **"Computerstandort"** festgelegt haben (siehe *Endpunktspeicherort auf Seite 14-2*), 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 und Windows Server 2012 standardmäßig deaktiviert. Vor der Aktivierung der Gerätesteuerung auf diesen Serverplattformen lesen Sie die Richtlinien und bewährten Methoden, die beschrieben werden unter *OfficeScan Agent Dienste auf Seite 14-7*.
 - Eine Liste aller unterstützten Gerätemodelle finden Sie in der *Datenschutzliste* unter: <http://docs.trendmicro.com/de-de/enterprise/officescan.aspx>
-

Die Gerätearten, die OfficeScan überwachen kann, hängen davon ab, ob die Datenschutzlizenzen aktiviert ist. Der Datenschutz ist ein separat lizenziertes Modul, das vor seiner Verwendung aktiviert werden muss. Weitere Informationen über die Datenschutzlizenz finden Sie unter *Datenschutzlizenzen auf Seite 3-4*.

TABELLE 9-1. 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 10-36 .
	Disketten
	Netzlaufwerke
	USB-Speichergeräte

TABELLE 9-2. 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-Karte
	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 9-3. 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 Suchfunktion in OfficeScan wird durch Geräteberechtigungen ergänzt und kann die Geräteberechtigungen überschreiben. Wenn die Berechtigung z. B. zulässt, dass eine Datei geöffnet werden kann, OfficeScan 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 OfficeScan 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 9-4. 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 (<code>winword.exe</code>), das normalerweise unter <code>C:\Programme\Microsoft Office\Office</code> gespeichert ist. Wenn die Berechtigung für die USB-Speichergeräte "Nur Geräteinhalt auflisten" lautet, <code>C:\Programme\Microsoft Office\Office\winword.exe</code> 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 Programmpfad und -name angeben auf Seite 9-9.
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. "<code>E:\Installer\Setup.exe</code>", zu dieser Liste hinzu.	Programmpfad und -name oder Anbieter der digitalen Signatur Weitere Informationen finden Sie unter Programmpfad und -name angeben auf Seite 9-9 oder Anbieter der digitalen Signatur festlegen auf Seite 9-8.

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 ofescan.ini hinzufügen, die bis zu 1.000 Programme enthalten kann. Anweisungen zum Hinzufügen von Programmen zur Datei ofescan.ini finden Sie unter [*Programme zu Gerätesteuierungslisten mit Hilfe von ofescan.ini hinzufügen auf Seite 9-17*](#).

**Warnung!**

Programme, die zur Datei ofescan.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).

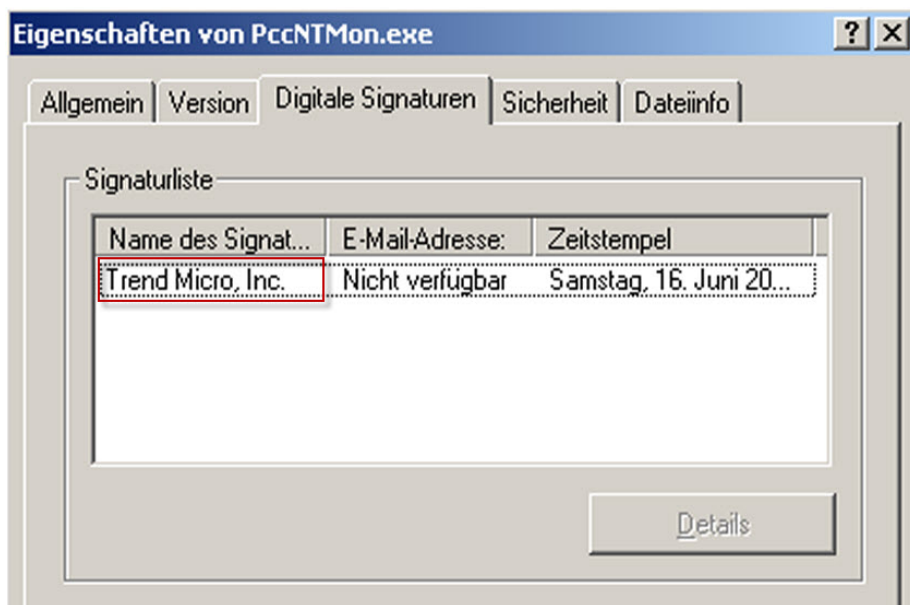


ABBILDUNG 9-1. Anbieter der digitalen Signatur für das OfficeScan Agent-Programm (PccNTMon.exe)

Programmpfad und -name angeben

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 Ordernamen verwendet werden. Sie müssen den exakten Namen eines Ordners angeben.

In den folgenden Beispielen wurden die Platzhalter richtig verwendet:

TABELLE 9-5. 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\?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 9-6. Falsche Verwendung von Platzhaltern

BEISPIEL	GRUND
??:\Buffalo\Password.exe	?? stellt zwei Zeichen dar, und Laufwerksbuchstaben bestehen nur aus einem alphabetischen Zeichen.
*:\Buffalo\Password.exe	* stellt mehrere Zeichen dar, und Laufwerksbuchstaben bestehen nur aus einem alphabetischen Zeichen.
C:*\Password.exe	Platzhalter können nicht für Ordernamen 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 Stammsymbol (🌐), 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. Klicken Sie 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** auswählen.
 - Auf der Registerkarte **Interne Agents** können Sie Einstellungen auf externe agents anwenden, indem Sie **Alle Einstellungen für externe Agents übernehmen** auswählen.

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 9-4*.

- 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 9-13*.

9. Bei allen Geräten, die keine Speichergeräte sind, wählen Sie **Zulassen** oder **Sperren**.
 10. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 9-6](#).

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 9-18](#).

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 9-4](#).

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 xv>\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 Stammsymbol () , 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. Klicken Sie 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** auswählen.
- Auf der Registerkarte **Interne Agents** können Sie Einstellungen auf externe agents anwenden, indem Sie **Alle Einstellungen für externe Agents übernehmen** auswählen.

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 9-12*](#).

10. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 9-6](#).

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.
-

Gerätesteueringbenachrichtigungen 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 13-40](#).

Protokolle der Gerätesteuerung anzeigen



Hinweis

Nur Zugriffsversuche auf **Speichergeräte** werden protokolliert. OfficeScan 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 Stammsymbol () , 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 10

Prävention vor Datenverlust verwenden

In diesem Kapitel wird erläutert, wie Sie die Funktion der Prävention vor Datenverlust verwenden.

Es werden folgende Themen behandelt:

- *Über Prävention vor Datenverlust (DLP) auf Seite 10-2*
- *Richtlinien für 'Prävention vor Datenverlust' auf Seite 10-3*
- *Datenbezeichnertypen auf Seite 10-6*
- *Vorlagen für 'Prävention vor Datenverlust' auf Seite 10-22*
- *DLP-Kanäle auf Seite 10-27*
- *Aktionen der Funktion "Prävention vor Datenverlust" auf Seite 10-41*
- *Ausnahmen für Prävention vor Datenverlust auf Seite 10-44*
- *Richtlinienkonfiguration der Funktion "Prävention vor Datenverlust" auf Seite 10-50*
- *Benachrichtigungen der Funktion "Prävention vor Datenverlust" auf Seite 10-56*
- *Protokolle für 'Prävention vor Datenverlust' auf Seite 10-61*

Über Prävention vor Datenverlust (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 14-2](#)), 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 10-1. 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 „Sperrern“ 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 10-6](#)*.

- **Dateiattribute:** Dateieigenschaften wie Dateityp und Dateigröße.

Weitere Informationen finden Sie unter *[Dateiattribute auf Seite 10-11](#)*.

- **Schlüsselwortlisten:** Eine Liste bestimmter Wörter oder Phrasen.

Weitere Informationen finden Sie unter *[Schlüsselwörter auf Seite 10-15](#)*.



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 10-6](#)* und *[Benutzerdefinierte Ausdrücke auf Seite 10-7](#)*.

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 Fehlalarme 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 10-8*.

Kriterien für benutzerdefinierte Ausdrücke

TABELLE 10-2. Kriterienoptionen für benutzerdefinierte Ausdrücke

KRITERIEN	REGEL	BEISPIEL
Keine	Keine	Alle - Namen gemäß den Angaben des Statistischen Bundesamtes der Vereinigten Staaten • Ausdruck: <code>[^\w]([A-Z][a-z]{1,12}(\s?,\s? [\s])\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]</code>
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: <code>[^\d]([0123678]\d{8})[^\d]</code> • 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: <code>\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-]</code> - 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: <code>[^\w.]([w\.] {1,20} @[a-z0-9]{2,20} [\.\.] [a-z]{2,5} [a-z\.\.] {0,10}) [^\w.]</code> - 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 10-8*):

- 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 10-36*.

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.sdc
 - *.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 10-15* und *Benutzerdefinierte Schlüsselwortlisten auf Seite 10-17*.

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:

First Name:_John_ **Last 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 **first name of our new employee from Switzerland is John. His** last 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 10-17](#).

Kriterien für benutzerdefinierte Schlüsselwortlisten

TABELLE 10-3. 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 aus der Schlüsselwortliste enthalten. Jedes Schlüsselwortpaar darf höchstens <x> Zeichen voneinander entfernt sein. Nehmen wir an, Ihre drei Schlüsselwörter sind WEB, DISK und USB, und die von Ihnen angegebene Anzahl von Zeichen beträgt 20. Wenn die Prävention vor Datenverlust alle Schlüsselwörter in der Reihenfolge DISK, WEB und USB erkennt, muss die Anzahl der Zeichen von "D" (in DISK) bis zu "W" (in WEB) und von "W" zu "U" (in USB) 20 Zeichen oder weniger betragen. Die folgenden Daten erfüllen die Kriterien: DISK####WEB#####USB Die folgenden Daten erfüllen die Kriterien nicht: DISK*****WEB****USB(23 Zeichen zwischen "D" und "W") Denken Sie bei der Auswahl der Zeichenanzahl daran, dass sich durch eine kleine Anzahl, wie z. B. 10, die Suchgeschwindigkeit in der Regel erhöht, aber nur ein relativ kleiner Bereich abgedeckt wird. Dadurch verringert sich die Wahrscheinlichkeit, dass sensible Daten entdeckt werden, vor allem in großen Dateien. Je größer die Anzahl, umso größer der abgedeckte Bereich, aber möglicherweise umso langsamer die Suche.

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 10-23](#) und [Vordefinierte DLP-Vorlagen auf Seite 10-22](#).



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-Bliley 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 10-23*.

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 10-4. 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 40 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 10-23](#).

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

OfficeScan 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 OfficeScan den Übertragungsumfang, den Sie konfigurieren müssen. Abhängig vom ausgewählten Umfang überwacht OfficeScan 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 10-31*](#).

E-Mail-Clients

OfficeScan überwacht E-Mails, die über unterschiedlichste E-Mail-agents übertragen werden. OfficeScan überprüft den Betreff, den Text und die Anhänge einer E-Mail nach Hinweisen auf Datenbezeichner. Eine Liste aller unterstützten E-Mail-agents finden Sie in der *Datenschutzliste* unter:

<http://docs.trendmicro.com/de-de/enterprise/officescan.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 OfficeScan zugelassen oder gesperrt.

Sie können nicht überwachte interne E-Mail-Domänen und überwachte Subdomänen festlegen.

- **Nicht überwachte E-Mail-Domänen:** OfficeScan erlaubt sofort die 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 OfficeScan 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 OfficeScan 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-agents 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 OfficeScan, 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 10-44*.

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 OfficeScan die anderen Listen.

Bei E-Mails, die über andere Protokolle gesendet werden, überprüft OfficeScan 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/de-de/enterprise/officescan.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/de-de/enterprise/officescan.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/de-de/enterprise/officescan.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 9-4*.

Eine Liste aller Anwendungen, die OfficeScan für den Zugriff auf freigegebene Dateien überwacht, finden Sie in der *Datenschutzliste* unter:

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

Übertragungsumfang und -ziele für Netzwerkkanäle

Mit dem Übertragungsumfang und den Übertragungszielen werden die Datenübertragungen in Netzwerkkanälen definiert, die OfficeScan überwachen muss. Bei zu überwachenden Übertragungen überprüft OfficeScan, ob Datenbezeichner

vorhanden sind, bevor die Übertragung erlaubt oder gesperrt wird. Bei nicht zu überwachenden Übertragungen überprüft OfficeScan nicht, ob Datenbezeichner vorhanden sind, und lässt die Übertragung sofort zu.

Übertragungsumfang: Alle Übertragungen

OfficeScan überwacht Daten, 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:** OfficeScan überwacht keine an folgende Ziele übertragene 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 OfficeScan bei nicht überwachten Zielen die Übertragung nicht protokolliert, während die Übertragung bei überwachten Zielen immer protokolliert wird.

- **Überwachte Ziele:** Dabei handelt es sich um spezielle Ziele innerhalb der nicht überwachten Ziele, die jedoch überwacht werden müssen. Überwachte Ziele sind:
 - Optional, wenn Sie nicht überwachte Ziele definiert haben.
 - Nicht konfigurierbar, wenn Sie keine nicht überwachten Ziele festgelegt haben.

Beispiel:

Folgende 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 10-44](#)*.

Übertragungsumfang: Nur Übertragungen außerhalb des lokalen Netzwerks

OfficeScan 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 OfficeScan bei nicht überwachten Zielen 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 10-44](#)*.

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

OfficeScan kann die folgenden 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/de-de/enterprise/officescan.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/de-de/enterprise/officescan.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 Stammsymbol () , 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 14-2](#).

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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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/de-de/enterprise/officescan.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/de-de/enterprise/officescan.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/de-de/enterprise/officescan.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-Endpoint installiert ist.
-

Eine Liste der unterstützten Wechselspeichermedien und Anwendungen, die die Datenübertragung ermöglichen, finden Sie in der *Datenschutzliste* unter:

<http://docs.trendmicro.com/de-de/enterprise/officescan.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 9-14*.

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/de-de/enterprise/officescan.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 10-5. 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	
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.
Verschlüsselt unterstützte Kanäle mit dem angegebenen Schlüssel/ Kennwort (nur verfügbar, wenn Endpoint Encryption installiert ist)	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.

AKTION	BESCHREIBUNG
Hinweis Diese Option ist nur für Wechseldatenträger- und Cloud-Speicher-Kanäle und bei Auswahl der Aktion Übergehen verfügbar.	• 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 OfficeScan die Daten erneut verschlüsselt, verschieben Sie die verschlüsselten Dateien auf ein lokales Laufwerk, bevor Sie auf die Daten zuzugreifen versuchen. • Bei Verwendung eines Web-Clients blockiert Prävention vor Datenverlust Versuche, Dateien in den Cloud Storage hochzuladen. Verschlüsseln Sie die Dateien manuell, bevor Sie den Upload mit einem Web-Client durchführen.

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 10-32*. 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 10-33*.

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 Ziele mit Portnummern und Portbereichen:

- 10.1.1.1:80
- host:5-20
- host.domain.com:20
- 10.1.1.1/32:20

4. Trennen Sie einzelne Ziele mit Kommas voneinander.

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:

my_archive.zip	= 10 MB bei der Dekomprimierung
\AAA.rar	= 25MB bei der Dekomprimierung
\BBB.zip	= 3MB bei der Dekomprimierung
\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 10-6. 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 "Sperrern" 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 10-3](#).

Richtlinie für Prävention vor Datenverlust erstellen

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 > 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 14-2](#).

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 10-52](#).
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 10-44](#)*.

10. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 10-22](#)*.

- 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 10-27](#)* und *[System- und Anwendungskanäle auf Seite 10-34](#)*.

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 10-31* 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 10-28*.

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 9-14*.

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 10-41*.



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 10-7. 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 10-57*.

Weitere Informationen zu den an agent-Benutzer gesendeten Benachrichtigungen finden Sie unter *Benachrichtigungen zur Funktion "Prävention vor Datenverlust" für Agent-Benutzer auf Seite 10-60*.

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 13-36*.

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**.

Verwenden Sie die rollenbasierte Administration, um Benutzern agent-Hierarchiedomänenberechtigungen zu gewähren. Bei einer Übertragung auf einem 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 10-8. 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 10-9. 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

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 10-9: Token-Variablen für Benachrichtigungen zur Funktion "Prävention vor Datenverlust" auf Seite 10-59.*

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 10-9: Token-Variablen für Benachrichtigungen zur Funktion "Prävention vor Datenverlust" auf Seite 10-59.*
 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 10-50.*

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 13-40](#).

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 10-10. Protokolldaten für Prävention vor Datenverlust

SPALTE	BESCHREIBUNG
Datum/Uhrzeit	Datum und Uhrzeit der Protokollierung des Vorfalls durch die Prävention vor Datenverlust
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 10-63.
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 10-65.

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 10-11. 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

KANAL	PROZESS
Wechseldatenträger	Prozessname der Anwendung, die Daten auf das Speichergerät oder innerhalb des Speichergeräts übertragen hat. Beispiel: explorer.exe
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\msnmsg.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

KANAL	PROZESS
PGP-Verschlüsselung	Vollständiger Pfad und Prozessname der PGP-Verschlüsselungssoftware Beispiel: C:\Programme\PGP Corporation\PGP Desktop\PGPmnApp.exe
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 10-12. 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
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 10-63 .
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

DETAIL	BESCHREIBUNG
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
Benutzerrechtigungsgrund	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 11

Computer vor Internet-Bedrohungen schützen

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 11-2*
- *Command & Control-Kontakalarmdienste auf Seite 11-2*
- *Web Reputation auf Seite 11-4*
- *Web-Reputation-Richtlinien auf Seite 11-5*
- *Verdächtiger Verbindungsdienst auf Seite 11-13*
- *Benachrichtigungen über Internet-Bedrohungen für Agent-Benutzer auf Seite 11-17*
- *C&C-Callback-Benachrichtigungen für Administratoren konfigurieren auf Seite 11-19*
- *C & C-Callback-Ausbrüche auf Seite 11-23*
- *Protokolle für Internet-Bedrohungen auf Seite 11-25*

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 Netzwerkanal zu erkennen.

Weitere Informationen zur Konfiguration der Sicherheitsstufe der Web-Reputation-Dienste finden Sie unter [Eine Web-Reputation-Richtlinie konfigurieren auf Seite 11-5](#).

TABELLE 11-1. 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 bössartiger Websites, um für erhöhten Schutz vor erweiterten Bedrohungen zu sorgen. Die Web-Reputation-Sicherheitsstufe legt anhand zugewiesener Risikostufen die Maßnahme fest, die bei bössartigen 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 13-33.
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 11-13.

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 11-19 .
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 11-22 .
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 11-23 .
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 11-27 .

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. Anschließend werden Websites durchsucht und Benutzer vom Zugriff auf infizierte Websites abgehalten.

OfficeScan Agents senden Abfragen an die Smart Protection Quellen, um die Zuverlässigkeit von Websites, auf die ein Benutzer zugreifen möchte, zu überprüfen. Die Reputation der Website steht in Zusammenhang mit der entsprechenden, auf den

Endpunkt angewendeten Web-Reputation-Richtlinie. Die jeweilige Richtlinie bestimmt, ob der OfficeScan Agent den Zugriff auf eine Website zulässt oder sperrt.



Hinweis

Weitere Informationen zu Smart Protection Quellen finden Sie unter [Liste der Smart Protection Quellen auf Seite 4-24](#).

Fügen Sie Websites, die Sie als sicher bzw. gefährlich einstufen, zur Liste der zulässigen bzw. gesperrten URLs hinzu. Erkennt der OfficeScan Agent einen Zugriff auf eine dieser Websites, wird der Zugriff automatisch zugelassen bzw. gesperrt und es werden keine weiteren Abfragen an die Smart Protection Quellen gesendet.

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 14-2](#)), um deren Standort und die erforderliche Richtlinie zu bestimmen. 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.

Anweisungen zum Konfigurieren der Proxy-Einstellungen finden Sie unter [Externer Proxy für OfficeScan Agents auf Seite 14-53](#).

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 XP, Vista, 7, 8 oder 8.1 ausgeführt wird, 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 Window XP, Vista, 7, 8 oder 8.1. Diese Einstellung gilt nicht für agents unter Windows Server 2003, Windows Server 2008 oder Windows Server 2012, selbst wenn sie zu den Domänen gehören.

- Um Richtlinien für agents zu konfigurieren, auf denen Windows Server 2003, Windows Server 2008 oder Windows Server 2012 ausgeführt wird, wählen Sie 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 für den agent-Standort, sofern 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 14-2](#).

5. Wählen Sie **Web-Reputation-Richtlinie auf den folgenden Betriebssystemen aktivieren** aus.

Welche Betriebssysteme in diesem Fenster aufgelistet werden, hängt davon ab, welche Ziele Sie in Schritt 1 gewählt haben.



Tipp

Trend Micro empfiehlt, die 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 **Auswertung aktivieren** aus.



Hinweis

Im Bewertungsmodus erlauben die agents den Zugriff auf alle Websites. Der Zugriff auf Websites, die gesperrt sein sollten, wenn die Bewertung deaktiviert ist, wird protokolliert. Trend Micro bietet einen Bewertungsmodus, mit dem Sie Websites zuerst überprüfen und dann geeignete Maßnahmen auf Grundlage der Bewertung ergreifen können. Sie können beispielsweise Websites, die Sie als sicher erachten, der Liste der zulässigen URLs hinzufügen.

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 bössartiger Webserver, die HTTPS nutzen, einfach gestaltet.

Aktivieren Sie das Prüfen von HTTPS-URLs, um die Gefährdung durch infizierte und bössartige Websites, die HTTPS verwenden, zu verringern. OfficeScan kann den HTTPS-Datenverkehr auf folgenden Browsern überwachen:

TABELLE 11-2. Browser, die den HTTPS-Datenverkehr unterstützen

BROWSER	VERSION
Microsoft Internet Explorer	• 6 mit SP2 oder höher • 7.x • 8.x • 9.x • 10.x • 11.x
Mozilla Firefox	3.5 oder höher
Chrome	n. v.



Wichtig

- Die HTTPS-Suchfunktion unterstützt nur Windows 8, Windows 8.1 und Windows 2012-Plattformen im Desktop-Modus.
- 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.

Für OfficeScan Agents, auf denen Firefox ausgeführt wird, müssen Benutzer das Add-On Trend Micro Osprey Firefox Extension 2.0.0.1061 im Browser-Pop-up-Fenster (oder im Bildschirm **Add-Ons > Erweiterungen**) aktivieren.

Für OfficeScan Agents, auf denen Internet Explorer 9, 10 oder 11 ausgeführt wird, müssen Benutzer das Add-On TmIEPlugInBHO Class im Browser-Pop-up-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 OfficeScan den gesamten Datenverkehr auf allen Ports.



Hinweis

Nicht unterstützt unter Windows 7, 8, 8.1 oder Windows Server 2008 R2, 2012 oder höheren Plattformen.

9. Wählen Sie **Abfragen an Smart Protection Server senden** aus, wenn Sie möchten, dass interne Agents Web-Reputation-Abfragen an Smart Protection Server senden.

- 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 4-24](#).

- 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 (konfiguriert in Schritt 10).
 - Wenn die agents sich über einen Proxy-Server mit den Smart Protection Servern verbinden sollen, legen Sie die Proxy-Einstellungen auf der Registerkarte **Administration > Einstellungen > Proxy > Interner Proxy** fest.
 - Aktualisieren Sie die Smart Protection Server regelmäßig, damit der Schutz stets aktuell ist.
 - Agents sperren keine nicht getesteten Websites. 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. Agent-Computer müssen mit dem Internet verbunden sein, um erfolgreich Abfragen senden zu können.
 - Wenn für die Verbindung mit dem Smart Protection Network eine Proxy-Server-Authentifizierung erforderlich ist, müssen Sie die Authentifizierungsdaten unter **Administration > Einstellungen > Proxy > Externer Proxy (Registerkarte) > OfficeScan Agent-Verbindung mit Trend Micro Servern** angeben.
 - Agents sperren nicht getestete Websites, wenn Sie in Schritt 9 **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 OfficeScan den Zugriff auf einen Link zulässt oder sperrt. Wenn zum Beispiel die Sicherheitsstufe auf Niedrig gestellt ist, sperrt OfficeScan nur Links, die als Internet-Bedrohung 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** in Schritt 7 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 böartigem Skript sperren**, um Webbrowser-Schwachstellen und böartige Skripts zu identifizieren und die Gefährdung des Webbrowsers durch diese Bedrohungen zu verhindern.

OfficeScan 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 11-3. 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.

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, erlauben die agents stets den Zugriff darauf, 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:

- Die Eingabe von `www.trendmicro.com/*` bedeutet, dass alle Seiten in der Trend Micro Website zugelassen werden.
- Die Eingabe von `*.trendmicro.com/*` bedeutet, dass alle Seiten aller Subdomänen von `trendmicro.com` zugelassen werden.

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 zur 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. Erlauben Sie den agents das Versenden von Protokollen, wenn Sie die von OfficeScan gesperrten URLs analysieren und bei als sicher eingestuften URLs eine entsprechende Aktion durchführen möchten.
16. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

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 11-14*.

- 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 11-15*.

- 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 11-15*.

Weitere Informationen zu GeneriClean finden Sie unter *GeneriClean auf Seite E-5*.

Aktivieren Sie den "Verdächtigen Verbindungsdienst" im Fenster **Zusätzliche Diensteseinstellungen**, um Agents vor C&C-Server-Callbacks zu schützen. Weitere Informationen finden Sie unter *Die Agent-Dienste von der Webkonsole aus aktivieren bzw. deaktivieren auf Seite 14-8*.

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. Navigieren Sie zum Abschnitt **Verdächtige Verbindungseinstellungen**.
3. Klicken Sie auf **Benutzerdefinierte IP-Liste bearbeiten**.
4. Fügen Sie auf der Registerkarte **Zulässige Liste** oder **Gesperrte Liste** 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 11-15*.

- 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**.
5. Aktivieren Sie das Kontrollkästchen neben einer Adresse, und klicken Sie auf **Löschen**, um IP-Adressen aus der Liste zu entfernen.
 6. Klicken Sie nach der Konfiguration der Listen auf **Schließen**, um zum Fenster **Globale Agent-Einstellungen** zurückzukehren.
-

Verdächtige Verbindungseinstellungen konfigurieren

OfficeScan kann alle Verbindungen zwischen agents und Adressen in der Globalen C&C-IP-Liste protokollieren. Im Fenster **Verdächtige Verbindungseinstellungen** können Sie auch IP-Adressen protokollieren, die in der benutzerdefinierten Liste mit gesperrten IP-Adressen konfiguriert sind, aber dennoch den Zugriff auf diese IP-Adressen erlauben.

OfficeScan kann außerdem Verbindungen überwachen, die das Ergebnis einer Botnet- oder sonstigen Malware-Bedrohung sind. Wenn eine Malware-Bedrohung erkannt wurde, kann OfficeScan versuchen, die Infektion zu beseitigen.

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 > Verdächtige Verbindungseinstellungen**.

Das Fenster **Verdächtige Verbindungseinstellungen** wird angezeigt.

4. Aktivieren Sie die Einstellung **Netzwerkverbindungen zu Adressen in der Globalen C&C-IP-Liste protokollieren**, um Verbindungen zu von Trend Micro bestätigten C&C-Servern zu überwachen.
 - 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 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 11-13](#).

5. Aktivieren Sie die Einstellung **Verbindungen mit Malware-Fingerabdruck für Netzwerk protokollieren**, um einen Pattern-Abgleich für Paket-Header durchzuführen. OfficeScan protokolliert 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 versuchen kann, Verbindungen zu C&C-Servern zu säubern. OfficeScan verwendet GeneriClean zum Säubern der Malware-Bedrohung und zum Beenden der Verbindung zum C&C-Server.

**Hinweis**

Sie müssen Verbindungen mit **Malware-Fingerabdruck für Netzwerk protokollieren** aktivieren, damit OfficeScan versuchen kann, die Verbindungen zu C&C-Servern zu säubern, die vom Paketstrukturabgleich erkannt wurden.

6. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

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 Stammsymbol () , 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 konfigurieren

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.

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**.

Verwenden Sie die rollenbasierte Administration, um Benutzern agent-Hierarchiedomänenberechtigungen zu gewähren. Bei einer Übertragung auf einem 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 11-4. 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 11-5. Token-Variablen für C&C-Callback-Benachrichtigungen

VARIABLE	BESCHREIBUNG
%CLIENTCOMPUTER%	Ziel-Endpunkt, der den Callback gesendet hat
%IP%	IP-Adresse des Ziel-Endpunkts
%DOMAIN%	Domäne des Computers
%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 11-5: Token-Variablen für C&C-Callback-Benachrichtigungen auf Seite 11-21*.
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 11-5: Token-Variablen für C&C-Callback-Benachrichtigungen auf Seite 11-21*.

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-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-Benachrichtigung aktivieren

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. 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

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 13-36*](#).

C&C-Callback-Ausbruchskriterien und -Benachrichtigungen konfigurieren

Prozedur

1. Navigieren Sie zu **Administration > Benachrichtigungen > Ausbruch**.
2. Konfigurieren Sie auf der Registerkarte **Kriterien** die folgenden Optionen:

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	Wählen Sie Jede Aktion , Protokolliert oder Gesperrt aus.
Erkannte Bedrohungen	Geben Sie die für die Definition eines Ausbruchs erforderliche Anzahl von Erkennungen an.
Zeitraum	Geben Sie die Anzahl der Stunden an, innerhalb der die Anzahl der Erkennungen auftreten muss.



Tipp

Trend Micro empfiehlt, die Standardeinstellungen in diesem Fenster zu übernehmen.

3. Auf der Registerkarte **E-Mail**:
 - a. Navigieren Sie zum Abschnitt **C&C-Callbacks**.
 - 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 11-6. Token-Variablen für C&C-Callback-Ausbruchsbenachrichtigungen

VARIABLE	BESCHREIBUNG
%C	Anzahl der C&C-Callback-Protokolle
%T	Zeitraum, in dem die C&C-Callback-Protokolle gesammelt wurden

- e. Wählen Sie aus, welche verfügbaren zusätzlichen C&C-Callback-Informationen in die E-Mail aufgenommen werden sollen.
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 11-6: Token-Variablen für C&C-Callback-Ausbruchsbenachrichtigungen auf Seite 11-25*.
 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 11-6: Token-Variablen für C&C-Callback-Ausbruchsbenachrichtigungen auf Seite 11-25*.
 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 13-40](#).

Web-Reputation-Protokolle anzeigen

Prozedur

1. Navigieren Sie zu **Protokolle > Agents > Sicherheitsrisiken** oder **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 anzeigen > Web-Reputation-Protokolle** oder **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

VORGANG	BESCHREIBUNG
Prozess	Prozess, über den die Kontaktaufnahme versucht wurde (Pfad\Anwendungsname)
Aktion	Hinsichtlich der Erkennung ergriffene Aktion

- Wenn eine URL nicht gesperrt werden soll, klicken Sie auf die Schaltfläche **Zur Liste der zulässigen Programme hinzufügen**, um die Website zur Liste der zulässigen Programme hinzuzufügen.
- 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.

C&C Callback-Protokolle anzeigen

Prozedur

- Navigieren Sie zu **Protokolle > Agents > Sicherheitsrisiken** oder **Agents > Agent-Verwaltung**.
- Klicken Sie in der agent-Hierarchie auf das Stammsymbol , um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
- Klicken Sie auf **Protokolle anzeigen > C&C Callback-Protokolle** oder auf **Protokolle > C&C Callback-Protokolle**.
- Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.
- Sehen Sie die Protokolle ein. Die Protokolle enthalten die folgenden Informationen:

VORGANG	BESCHREIBUNG
Datum/Uhrzeit	Zeitpunkt der Erkennung

VORGANG	BESCHREIBUNG
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
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 des Callbacks 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 11-14](#).

- 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 Verbindungen anzeigen

Prozedur

- Navigieren Sie zu **Protokolle > Agents > Sicherheitsrisiken** oder **Agents > Agent-Verwaltung**.
- Klicken Sie in der agent-Hierarchie auf das Stammsymbol () , um alle agents einzuschließen oder nur bestimmte Domänen oder agents auszuwählen.
- Klicken Sie auf **Protokolle anzeigen > Protokolle zu verdächtigen Verbindungen** oder **Protokolle > Protokolle zu verdächtigen Verbindungen**.
- Geben Sie die Protokollkriterien ein und klicken Sie anschließend auf **Protokolle anzeigen**.
- 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, der die Übertragung gestartet hat (Pfad \Anwendungsname)
Lokale IP-Adresse und lokaler Port	IP-Adresse und Portnummer des Quellendpunkts
Remote-IP-Adresse und Remote-Port	IP-Adresse und Portnummer des Zielendpunkts

VORGANG	BESCHREIBUNG
Ergebnis	Ergebnis der durchgeführten Aktion
Entdeckt durch	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.
-

Kapitel 12

Die OfficeScan Firewall verwenden

In diesem Kapitel werden die Funktionen und die Konfiguration der OfficeScan Firewall beschrieben.

Es werden folgende Themen behandelt:

- *Info über die OfficeScan Firewall auf Seite 12-2*
- *Die OfficeScan Firewall aktivieren oder deaktivieren auf Seite 12-7*
- *Firewall-Richtlinien und -Profile auf Seite 12-9*
- *Firewall-Berechtigungen auf Seite 12-25*
- *Allgemeine Firewall-Einstellungen auf Seite 12-27*
- *Benachrichtigungen bei Firewall-Verstößen für OfficeScan Agent-Benutzer auf Seite 12-30*
- *Firewall-Protokolle auf Seite 12-31*
- *Ausbrüche bei Firewall-Verstoß auf Seite 12-33*
- *Die OfficeScan Firewall testen auf Seite 12-35*

Info über die OfficeScan Firewall

Die OfficeScan Firewall schützt 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 Endpunkte unter Windows XP, auf denen auch die Windows Firewall aktiviert ist, aktiviert, konfiguriert und eingesetzt werden. Die Richtlinien sollten jedoch sorgfältig verwaltet 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 12-2](#)*
- *[Anwendungsfiler auf Seite 12-3](#)*
- *[Certified Safe Software Liste auf Seite 12-3](#)*
- *[Suche nach Netzwerkviren auf Seite 12-4](#)*
- *[Profile und Richtlinien benutzerdefiniert anpassen auf Seite 12-4](#)*
- *[Stateful Inspection auf Seite 12-4](#)*
- *[Intrusion Detection System auf Seite 12-4](#)*
- *[Firewall-Verstoß-Ausbruchsmontor auf Seite 12-6](#)*
- *[OfficeScan Agent Firewall-Berechtigungen auf Seite 12-6](#)*

Den Datenverkehr filtern

Die OfficeScan Firewall filtert den gesamten ein- und ausgehenden Datenverkehr und sperrt bestimmte Typen von Datenverkehr anhand folgender Kriterien:

- Richtung (eingehend/ausgehend)
- Protokoll (TCP/UDP/ICMP/ICMPv6)
- Zielports
- Quell- und Ziel- Endpunkte

Anwendungsfilter

Die OfficeScan Firewall filtert den eingehenden und ausgehenden Datenverkehr nach bestimmten Anwendungen und ermöglicht, dass diese Anwendungen auf das Netzwerk zugreifen. Die Netzwerkverbindungen hängen jedoch von den Richtlinien ab, die vom Administrator festgelegt werden.



Hinweis

OfficeScan unterstützt spezifische Anwendungsausnahmen auf Windows 8-, Windows 8.1- und Windows Server 2012-Plattformen nicht. Auf Endpunkte mit diesen Plattformen lässt OfficeScan den gesamten Anwendungsdatenverkehr zu bzw. verweigert ihn.

Certified Safe Software Liste

Bei der Certified Safe Software Liste handelt es sich um eine Liste der Anwendungen, die die Sicherheitsebenen der Firewall-Richtlinie umgehen können. Wenn die Sicherheitsebene auf "Mittel" oder "Hoch" gesetzt ist, lässt OfficeScan weiterhin zu, dass die Anwendungen ausgeführt werden und auf das Netzwerk zugreifen können.

Sie können die Abfrage der globalen Certified Safe Software Liste aktivieren, die eine vollständigere Liste bereitstellt. Diese Liste wird dynamisch von Trend Micro aktualisiert.



Hinweis

Diese Funktion arbeitet mit der Verhaltensüberwachung zusammen. Stellen Sie sicher, dass die Dienste "Trend Micro Unauthorized Change Prevention Service" und "Certified Safe Software Service" aktiviert sind, bevor Sie die globale Certified Safe Software Liste 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 ist eine Stateful-Inspection-Firewall. Sie überwacht alle Verbindungen des OfficeScan Agent und hinterlegt den jeweiligen Verbindungsstatus in einer Datei. Sie kann bestimmte Zustände in den Verbindungen ermitteln, zu ergreifende Aktionen vorschlagen und Störungen des Normalzustands feststellen. Aus diesem Grund umfasst die effektive Nutzung der Firewall nicht nur das Erstellen von Profilen und Richtlinien, sondern auch die Analyse von Verbindungen und das Filtern von Paketen, die die Firewall passieren.

Intrusion Detection System

Die OfficeScan Firewall beinhaltet außerdem ein Intrusion Detection System (IDS). Das aktivierte IDS kann bestimmte Muster in Netzwerkpaketen erkennen, die möglicherweise auf einen OfficeScan Agent-Angriff hindeuten. Mit der OfficeScan Firewall können die folgenden bekannten Eindringversuche verhindert werden:

INTRUSION	BESCHREIBUNG
Fragment zu groß	Ein Denial-of-Service-Angriff, bei dem ein Hacker ein übergroßes TCP/UDP-Paket an ein Endpunkt-Zielgerät weiterleitet. Dies kann auf dem Endpunkt zu einem Pufferüberlauf führen, der die Leistung des Endpunkt stark einschränkt oder zu einem Absturz führt.
Ping-of-Death	Ein Denial-of-Service-Angriff, bei dem ein Hacker ein übergroßes ICMP/ICMPv6-Paket an ein Endpunkt-Zielgerät weiterleitet. Dies kann auf dem Endpunkt zu einem Pufferüberlauf führen, der die Leistung des Endpunkt stark einschränkt oder zu einem Absturz führt.
ARP-Konflikt	Ein Angriff, bei dem ein Hacker eine ARP-Anforderung (Address Resolution Protocol) mit der gleichen Quell- und Ziel-IP-Adresse an ein Ziel-Endpunkt sendet. Das Endpunkt-Zielgerät sendet daraufhin ununterbrochen eine ARP-Antwort (seine MAC-Adresse) an sich selbst und verursacht dadurch einen Systemabsturz.
SYN-Flooding	Ein Denial-of-Service-Angriff, bei dem ein Programm mehrere TCP-SYN-Pakete (Synchronisierungspakete) Pakete an ein Endpunkt sendet. Daraufhin sendet das Endpunkt ständig Synchronisierungsbestätigungen (SYN/ACK). Dies überlastet auf Dauer den Arbeitsspeicher des Endpunkt und kann zum Absturz des Endpunkt führen.
Überlappendes Fragment	Ähnlich einem Teardrop-Angriff sendet dieser Denial-of-Service-Angriff überlappende TCP-Fragmente an einen Endpunkt. Dadurch werden die Header-Informationen im ersten TCP-Fragment überschrieben und können dann eine Firewall passieren. Daraufhin können weitere Fragmente mit böartigem Code an das Endpunkt-Zielgerät 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 beim Zusammensetzen der Fragmente zum Absturz des Endpunkt-Zielgeräts führen.

INTRUSION	BESCHREIBUNG
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 das Endpunkt-Zielgerät gesendet werden, das diese Pakete nicht ordnungsgemäß weiterverarbeiten kann. Dies schränkt die Leistung des Endpunkt stark ein oder kann zu einem Absturz führen.
LAND Attack	Bei diesem Angriff werden IP-SYN-Pakete (Synchronisierungspakete) mit der gleichen Quell- und Zieladresse an den Endpunkt gesendet. Daraufhin sendet der Endpunkt die Synchronisierungsbestätigung (SYN/ACK) laufend an sich selbst. Dies schränkt die Leistung des Endpunkt 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 14-7*.

Sie können die Firewall auf allen oder auf ausgewählten OfficeScan Agent-Endpunkten aktivieren bzw. deaktivieren.

Die OfficeScan Firewall auf ausgewählten Endpunkten aktivieren bzw. deaktivieren

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 <i>Eine Firewall-Richtlinie hinzufügen oder ändern auf Seite 12-11</i>. 2. Wenden Sie die Richtlinie auf die OfficeScan Agents an.

METHODE	VERFAHREN
Aktivieren/ Deaktivieren Sie den Firewall-Dienst über die Webkonsole	Weitere Informationen über die einzelnen Schritte finden Sie unter OfficeScan Agent Dienste auf Seite 14-7.  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 in ausgewählten Endpunkte zu aktivieren bzw. zu deaktivieren.

METHODE	VERFAHREN
Den Firewall-Treiber aktivieren/ deaktivieren	- Öffnen Sie die Windows Netzwerkverbindungseigenschaften. - Aktivieren oder deaktivieren Sie das Kontrollkästchen Trend Micro Treiber für die allgemeine Firewall über die Netzwerkkarte.
Den Firewall-Dienst aktivieren/ deaktivieren	- Öffnen Sie ein Befehlszeilenfenster, und geben Sie <code>services.msc</code> ein. - Starten oder stoppen Sie die OfficeScan NT Firewall über die Microsoft Management-Konsole (MMC).

Die OfficeScan Firewall auf allen Endpunkten aktivieren bzw. deaktivieren

Prozedur

- Navigieren Sie zu **Administration > Einstellungen > Produktlizenz**.
- Gehen Sie zum Abschnitt **Zusätzliche Dienste**.
- 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 Firewall-Richtlinien können Sie bestimmte Typen von Netzwerkdatenverkehr sperren oder zulassen, die nicht in einer Richtlinien Ausnahme

angegeben sind. Eine Richtlinie definiert auch, welche Firewall-Funktionen aktiviert oder deaktiviert werden. Ordnen Sie eine Richtlinie einem oder mehreren Firewall-Profilen zu.

OfficeScan wird mit mehreren Standardrichtlinien ausgeliefert, die Sie ändern oder löschen können.

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 Standard-Firewall-Richtlinien aufgeführt.

TABELLE 12-1. Standard-Firewall-Richtlinien

NAME DER RICHTLINIE	SICHERHEITSSSTUFE	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

Sie können auch neue Richtlinien erstellen, wenn Ihre Anforderungen nicht von den Standardrichtlinien abgedeckt werden.

Alle Standard- und benutzerdefinierten Firewall-Richtlinien werden in der Liste der Firewall-Richtlinien auf der Webkonsole angezeigt.

Die Richtlinienliste der Firewall konfigurieren

Prozedur

1. Navigieren Sie zu **Agents > Firewall > -Richtlinien**.
2. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie hinzuzufügen.

Wenn Sie eine neue Richtlinie erstellen möchten, die ähnliche Einstellungen wie eine vorhandene Richtlinie hat, wählen Sie die vorhandene Richtlinie, und klicken Sie auf **Kopieren**. Um eine bestehende Richtlinie zu bearbeiten, klicken Sie auf den Namen der entsprechenden Richtlinie.

Ein Fenster zur Konfiguration der Richtlinie wird angezeigt. Weitere Informationen finden Sie unter [Eine Firewall-Richtlinie hinzufügen oder ändern auf Seite 12-11](#).

3. Zum Löschen einer vorhandenen Richtlinie aktivieren Sie das Kontrollkästchen neben der betreffenden Richtlinie, und klicken Sie auf **Löschen**.
4. Zum Bearbeiten der Firewall-Ausnahmevorlage klicken Sie auf **Ausnahmevorlage bearbeiten**.

Weitere Informationen finden Sie unter [Die Ausnahmevorlage der Firewall bearbeiten auf Seite 12-15](#).

Der Ausnahmevorlagen-Editor wird geöffnet.

Eine Firewall-Richtlinie hinzufügen oder ändern

Konfigurieren Sie für jede Richtlinie Folgendes:

- **Sicherheitsstufe:** Eine allgemeine Einstellung, mit der der gesamte ein- und/oder ausgehende Datenverkehr auf dem OfficeScan Agent Endpunkt gesperrt oder zugelassen wird

- **Firewall-Funktionsmerkmale:** 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 über das IDS finden Sie unter *Intrusion Detection System auf Seite 12-4*.
- **Certified Safe Software Liste:** Geben Sie an, ob die Anwendungen auf der Certified Safe Liste eine Verbindung zum Netzwerk aufbauen dürfen. Unter *Certified Safe Software Liste auf Seite 12-3* finden Sie weitere Informationen zu dem Thema Certified Safe Software Liste.
- **Liste der RichtlinienAusnahmen:** Eine Liste mit konfigurierbaren Ausnahmen zum Sperren oder Zulassen unterschiedlicher Arten von Netzwerkdatenverkehr

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 12-31*.
 - 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 12-15](#).

- 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 Ausnahmeevorlage der Firewall bearbeiten

Über die Ausnahmeevorlage 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 12-2. 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

Prozedur

1. Navigieren Sie zu **Agents > Firewall > -Richtlinien**.
2. Klicken Sie auf **Ausnahmavorlage 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 ausführen soll (Sie können den Datenverkehr, der die Ausnahmekriterien erfüllt, sperren oder zulassen), 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 ausgeführt werden soll.
9. Wählen Sie die IP-Adressen der OfficeScan Agent Endpunkt aus, die in die Ausnahme mit einbezogen werden sollen. Wenn Sie beispielsweise Netzwerkdatenverkehr ablehnen (eingehend und ausgehend) wählen und die IP-Adresse für einen einzigen Endpunkt im Netzwerk eingeben, kann kein OfficeScan Agent, dessen Richtlinie diese Ausnahme enthält, Daten an diese IP-Adresse senden oder Daten von dort 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**.

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-Profil

Mit Firewall-Profilen können Sie außerdem überprüfen, ob einzelne agents oder agents-Gruppen bestimmte Attribute aufweisen, bevor sie eine Richtlinie anwenden. 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 unter einer bestimmten Plattform
- **Anmeldename:** OfficeScan Agent Endpunkte, an denen bestimmte Benutzer angemeldet sind
- **NIC-Beschreibung:** Ein OfficeScan Agent-Endpunkt mit einer übereinstimmenden NIC-Beschreibung
- **Verbindungsstatus des Agents:** Online- oder Offline-Status des OfficeScan Agents

**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 12-22*.

4. Zum Löschen einer vorhandenen Richtlinie aktivieren Sie das Kontrollkästchen neben der betreffenden Richtlinie, und klicken Sie 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 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 13-34*). Bei der Aktivierung eines Referenzservers geht OfficeScan von folgenden Annahmen aus:
 - Mit Referenzservern verbundene OfficeScan Agents sind online, auch wenn 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 Auswahlménü der agent-Hierarchie die **Firewall-Ansicht** aus.
 - 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 die agent-Hierarchie zu öffnen und dort die Domänen auszuwählen.



Hinweis

Nur Benutzer mit vollständigen Domänenberechtigungen können Domänen auswählen.

- Endpunkt-Name: Klicken Sie auf die entsprechende Schaltfläche, um die agent-Hierarchie zu öffnen und dort die OfficeScan 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.

- Agent-Verbindungsstatus

7. 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 12-3. Firewall-Berechtigungen

BERECHTIGUNG	BESCHREIBUNG
Firewall-Einstellungen auf der OfficeScan Agent-Konsole anzeigen	Die Option Firewall zeigt alle Firewall-Einstellungen auf dem OfficeScan Agent an.

BERECHTIGUNG	BESCHREIBUNG
Clients dürfen Firewall, Intrusion Detection System (IDS) und Warnmeldung der Firewall aktivieren/deaktivieren	Die OfficeScan Firewall mit Stateful-Inspection-Technologie schützt agents und Server im Netzwerk durch leistungsstarkes Suchen und Entfernen von Netzwerkviren. Wenn Sie Benutzern die Berechtigung geben, 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.
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 12-31. Wenn Sie diese Option auswählen, konfigurieren Sie den Zeitplan für das Senden des Protokolls unter Agents > Globale Agent-Einstellungen. 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 12-27.

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 12-25*
 - *Clients dürfen Firewall, Intrusion Detection System (IDS) und Warnmeldung der Firewall aktivieren/deaktivieren auf Seite 12-26*
 - *OfficeScan Agents dürfen Firewall-Protokolle an den OfficeScan Server senden auf Seite 12-26*
6. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

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 12-25](#).

- **OfficeScan Firewall-Treiber nur nach einem Neustart des Systems aktualisieren**

Ermöglichen Sie dem OfficeScan Agent, nur dann ein Update des Treibers für die allgemeine Firewall 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 Treiber für die allgemeine Firewall 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 einmal pro Stunde an den OfficeScan Server. Weitere Informationen über Firewall-Protokolle finden Sie unter [Firewall-Protokolle auf Seite 12-31](#).

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 14-52](#)), 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. Gehen Sie zu den folgenden Abschnitten und konfigurieren Sie die Einstellungen:

TABELLE 12-4. Allgemeine Firewall-Einstellungen

ABSCHNITT	EINSTELLUNGEN
Firewall-Einstellungen	• Firewall-Protokolle an den Server senden auf Seite 12-27 • OfficeScan Firewall-Treiber nur nach einem Neustart des Systems aktualisieren auf Seite 12-28
Firewall-Protokollzähler	Firewall-Protokollinformationen stündlich an den OfficeScan Server senden, um die Möglichkeit eines Firewall-Ausbruchs festzustellen auf Seite 12-28
Einstellungen für Certified Safe Software Service	Certified Safe Software Service für Verhaltensüberwachung, Firewall und Virensuchen aktivieren auf Seite 12-28

3. 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 die Firewall-Richtlinien verstößt, eine Benachrichtigung auf agents 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 [Eine Firewall-Richtlinie hinzufügen oder ändern auf Seite 12-11](#).

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 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 **Benutzer dürfen Firewall, Intrusion Detection System (IDS) und Warnmeldung der Firewall aktivieren/deaktivieren**.

6. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

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 12-25](#).

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 13-40*](#).

Firewall-Protokolle anzeigen

Prozedur

1. Navigieren Sie zu **Protokolle > Agents > Sicherheitsrisiken** oder **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 > Firewall-Protokolle** oder **Protokolle anzeigen > Firewall-Protokolle**.
4. Um sicherzustellen, dass die aktuellsten 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:
 - Datum und Uhrzeit der Erkennung eines Firewall-Verstoßes
 - Endpunkt , auf dem der Firewall-Verstoß aufgetreten ist
 - Endpunkt -Domäne, in der der Firewall-Verstoß aufgetreten ist
 - IP-Adresse des externen Hosts
 - IP-Adresse des lokalen Hosts
 - Protokoll
 - Portnummer

- **Richtung:** Gibt an, ob eingehender oder ausgehender Datenverkehr gegen eine Firewall-Richtlinie verstoßen hat
 - **Prozess:** Das ausführbare Programm/der Dienst auf dem Endpunkt, der den Firewall-Verstoß verursacht hat
 - **Beschreibung:** Beschreibt das tatsächliche Sicherheitsrisiko (z. B. Netzwerkvirus oder IDS-Angriff) oder den Verstoß gegen eine Firewall-Richtlinie
7. 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.
-

Ausbrüche bei Firewall-Verstoß

Definieren Sie einen Ausbruch von Verstößen gegen die Firewall durch die Anzahl 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-Ausbruchsbearbeitungen 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 13-36](#).

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 Netzwerkviroprotokollen.
- d. Bestimmen 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 Netzwerkviroprotokolle 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 12-5. 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.

VARIABLE	BESCHREIBUNG
%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.

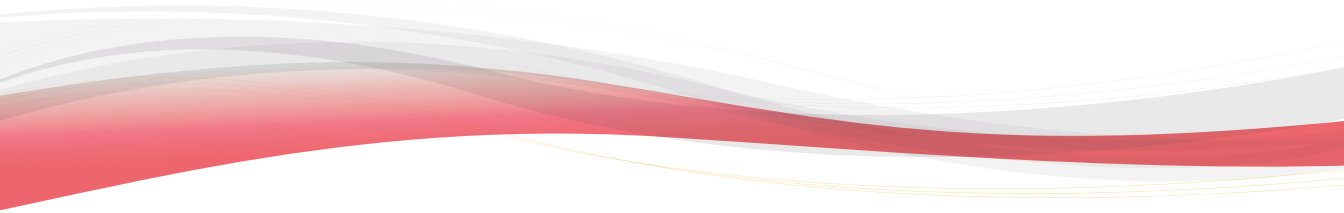
Prozedur

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 13

Den OfficeScan Server verwalten

In diesem Kapitel werden Verwaltung und Konfiguration von OfficeScan Servern beschrieben.

Es werden folgende Themen behandelt:

- *Rollenbasierte Administration auf Seite 13-3*
- *Trend Micro Control Manager auf Seite 13-25*
- *Einstellungen für Liste der verdächtigen Objekte auf Seite 13-32*
- *Referenzserver auf Seite 13-34*
- *Einstellungen für die Administratorbenachrichtigungen auf Seite 13-36*
- *Systemereignisprotokolle auf Seite 13-38*
- *Protokollmanagement auf Seite 13-40*
- *Lizenzen auf Seite 13-44*
- *OfficeScan Datenbanksicherung auf Seite 13-47*
- *SQL Server Migration Tool auf Seite 13-49*
- *Einstellungen des OfficeScan Webservers/ Agents auf Seite 13-54*
- *Kommunikation zwischen Server und Agents auf Seite 13-55*

- *[Kennwort der Webkonsole auf Seite 13-61](#)*
- *[Einstellungen der Webkonsole auf Seite 13-62](#)*
- *[Quarantäne-Manager auf Seite 13-62](#)*
- *[Server Tuner auf Seite 13-64](#)*
- *[Smart Feedback auf Seite 13-66](#)*

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 13-4](#).
2. Benutzerkonten konfigurieren und jedem Benutzerkonto eine bestimmte Rolle zuweisen. Weitere Informationen finden Sie unter [Benutzerkonten auf Seite 13-14](#).

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)

Benutzerrollen

Eine Benutzerrolle bestimmt, auf welche Menüpunkte der Webkonsole ein Benutzer Zugriff hat. Einer Rolle wird für jeden einzelnen Menüpunkt eine Berechtigung zugewiesen.

Weisen Sie Folgendem Berechtigungen zu:

- *Berechtigungen im Menü auf Seite 13-4*
- *Menüpunkt-Arten auf Seite 13-4*
- *Menüelemente für Server und Agents auf Seite 13-5*
- *Menüelemente für verwaltete Domänen auf Seite 13-8*

Berechtigungen im Menü

Berechtigungen bestimmen die Zugriffsrechte auf jeden Menüpunkt. Die Berechtigung für einen Menüpunkt kann sein:

- **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:** Der Benutzer ist nur berechtigt, Einstellungen, Aufgaben und Daten eines Menüpunktes anzuzeigen.
- **Kein Zugriff:** Menüelemente werden nicht angezeigt.

Menüpunkt-Arten

Es gibt zwei Arten von konfigurierbaren Menüelementen für OfficeScan-Benutzerrollen.

TABELLE 13-1. Menüpunkt-Arten

Typ	Bereich
Menüelemente für Server/Agents	• Servereinstellungen, Aufgaben und Daten • Globale agent-Einstellungen, Aufgaben und Daten Eine vollständige Liste aller verfügbaren Menüelemente finden Sie unter Menüelemente für Server und Agents auf Seite 13-5.
Menüelemente für verwaltete Domänen	Granuläre agent-Einstellungen, Aufgaben und Daten, die außerhalb der agent-Hierarchie verfügbar sind Eine vollständige Liste aller verfügbaren Menüelemente finden Sie unter Menüelemente für verwaltete Domänen auf Seite 13-8.

Menüelemente für Server und Agents

Die folgenden Tabellen enthalten die verfügbaren Menüelemente für Server/agents.



Hinweis

Menüelemente werden erst nach der Aktivierung des entsprechenden Plug-in-Programms angezeigt. Wenn beispielsweise das Modul "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 13-2. Menüelemente für "Agents"

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT
Agents	• Agent-Verwaltung • Agent-Gruppierung • Globale Agent-Einstellungen • Endpunktspeicherort • Verbindungsüberprüfung • Ausbruchsprävention

TABELLE 13-3. Menüelemente für "Protokolle"

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT
Protokolle	• Agents • Sicherheitsrisiken • Agent-Komponenten-Update • Server-Update • Systemereignisse • Protokollwartung

TABELLE 13-4. Menüelemente für "Updates"

ÜBERGEORDNETES MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Updates	Server	• Zeitgesteuertes Update • Manuelles Update • Update-Adresse
	Agents	• Automatisches Update • Update-Adresse
	Rollback	n. v.

TABELLE 13-5. Menüelemente für "Administration"

ÜBERGEORDNETE S MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Administration	Kontenverwaltung	• Benutzerkonten • Benutzerrollen  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

ÜBERGEORDNETE S MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
		• Datenbanksicherung • Liste der verdächtigen Objekte

Menüelemente für verwaltete Domänen

Die folgende Tabelle enthält die verfügbaren Menüelemente für verwaltete Domänen.

TABELLE 13-6. Menüelemente für "Dashboard"

HAUPTMENÜPUNKT	MENÜELEMENT
Dashboard  Hinweis Alle Benutzer können unabhängig von der Berechtigung auf diese Seite zugreifen.	n. v.

TABELLE 13-7. Menüelemente für "Bewertung"

ÜBERGEORDNETE S MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Bewertung	Einhaltung von Sicherheitsrichtlinien Nicht verwaltete Endpunkte	• Manueller Bericht • Zeitgesteuerter Bericht n. v.

TABELLE 13-8. Menüelemente für "Agents"

ÜBERGEORDNETE S MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Agents	Firewall	• Richtlinien • Profile
	Agent-Installation	• Browserbasiert • Remote

TABELLE 13-9. Menüelemente für "Protokolle"

ÜBERGEORDNETE S MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Protokolle	Agents	• Verbindungsüberprüfung • Zentrale Quarantänewiederherstellung • Spyware/Grayware-Wiederherstellung

TABELLE 13-10. Menüelemente für "Updates"

ÜBERGEORDNETE S MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Updates	Zusammenfassung	n. v.
	Agents	Manuelles Update

TABELLE 13-11. Menüelemente für "Administration"

ÜBERGEORDNETE S MENÜELEMENT	MENÜELEMENT	UNTERMENÜELEMENT
Administration	Benachrichtigungen	Administrator

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 13-12. 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.
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.

Benutzerdefiniert

Sie können benutzerdefinierte Rollen erstellen, wenn keine der integrierten Rollen Ihre Anforderungen erfüllen.

Nur Benutzer mit der integrierten Administratorrolle und solche, die das Root-Konto verwenden, das während der OfficeScan Installation erstellt wurde, können benutzerdefinierte Rollen erstellen und diese Rollen den Benutzerkonten zuweisen.

Eine benutzerdefinierte Rolle hinzufügen

Prozedur

1. Navigieren Sie zu **Administration > Kontenverwaltung > Benutzerrollen**.
2. Klicken Sie auf **Hinzufügen**. Wenn Sie eine Richtlinie erstellen möchten, die ähnliche Einstellungen wie eine vorhandene Richtlinie hat, wählen Sie die vorhandene Richtlinie, und klicken Sie auf **Kopieren**.

Ein neues Fenster wird angezeigt.

3. Geben Sie den Namen für die Rolle ein. Optional können Sie dabei eine Beschreibung angeben.
4. Klicken Sie auf **Menüelemente für Server/Agents**, und geben Sie die Berechtigung für jedes verfügbare Menüelement an. Eine Liste aller verfügbaren Menüelemente finden Sie unter *[Menüelemente für Server und Agents auf Seite 13-5](#)*.
5. Klicken Sie auf **Menüelemente für verwaltete Domänen**, und geben Sie die Berechtigung für jedes verfügbare Menüelement an. Eine Liste aller verfügbaren Menüelemente finden Sie unter *[Menüelemente für verwaltete Domänen auf Seite 13-8](#)*.
6. Klicken Sie auf **Speichern**.

Die neue Rolle wird in der Liste der Benutzerrollen angezeigt.

Eine benutzerdefinierte Rolle ändern

Prozedur

1. Navigieren Sie zu **Administration > Kontenverwaltung > Benutzerrollen**.
2. Klicken Sie den Rollennamen.

Ein neues Fenster wird angezeigt.

3. Sie können folgende Optionen ändern:
 - Beschreibung
 - Rollenberechtigungen
 - **Menüelemente für Server/Agents**
 - **Menüelemente für verwaltete Domänen**
 4. Klicken Sie auf **Speichern**.
-

Eine benutzerdefinierte Rolle löschen

Prozedur

1. Navigieren Sie zu **Administration > Kontenverwaltung > Benutzerrollen**.
 2. Wählen Sie das Kontrollkästchen neben der Rolle.
 3. Klicken Sie auf **Löschen**.
-



Hinweis

Eine Rolle kann nicht gelöscht werden, wenn sie mindestens einem Benutzerkonto zugewiesen wurde.

Benutzerdefinierte Rollen importieren oder exportieren

Prozedur

1. Navigieren Sie zu **Administration > Kontenverwaltung > Benutzerrollen**.
2. Benutzerdefinierte Rollen in eine .DAT-Datei exportieren:
 - a. Wählen Sie die Rollen aus und klicken Sie auf **Export**.
 - 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 **Export Rolleneinstellungen**.
 - 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.

Benutzerkonten

Benutzerkonten einrichten und jedem Benutzer eine bestimmte Rolle zuweisen. Die Benutzerrolle bestimmt, welche Menübefehle ein Benutzer auf der Webkonsole sehen und konfigurieren kann.

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.

Sie können benutzerdefinierte Konten oder Active Directory-Konten hinzufügen. Alle Benutzerkonten werden in der Liste der Benutzerkonten auf der Webkonsole angezeigt.

Weisen Sie Benutzerkonten die Berechtigung zum Anzeigen oder Konfigurieren der detaillierten agent-Einstellungen, Aufgaben und Daten zu, die in der agent-Hierarchie verfügbar sind. Eine vollständige Aufstellung aller verfügbaren Menüelemente in der agent-Hierarchie finden Sie unter [Menüelemente der Agent-Verwaltung auf Seite 13-15](#).



Hinweis

Nach dem Aktualisieren des OfficeScan Servers müssen Sie alle benutzerdefinierten Konten bearbeiten und alle neuen Funktionen im Bildschirm **Schritt 3 Agent-Hierarchiemenu definieren** für zuvor hinzugefügte benutzerdefinierte Konten manuell aktivieren. Weitere Informationen zu Berechtigungen finden Sie unter [Definieren von Berechtigungen für Domänen auf Seite 13-20](#).

OfficeScan Benutzerkonten eignen sich für die Ausführung von "Single Sign-On". Single Sign-On ermöglicht es Benutzern, von der OfficeScan-Konsole aus auf die Trend Micro Control Manager-Webkonsole zuzugreifen. Einzelheiten finden Sie in den Beschreibungen der nachfolgenden Verfahren.

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 "Prävention vor Datenverlust" nicht aktiviert ist, werden in der Liste keine Menüelemente für die Prävention vor Datenverlust angezeigt.

TABELLE 13-13. 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 • Update-Agent-Einstellungen • Berechtigungen und andere Einstellungen • Zusätzliche Diensteeinstellungen • Liste der zulässigen Spyware/Grayware • Liste der vertrauenswürdigen Programme • 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 • 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 benutzerdefiniertes Konto hinzufügen

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 zum Erstellen von Benutzerrollen finden Sie unter [Benutzerdefiniert auf Seite 13-11](#).

5. Geben Sie den Benutzernamen, die Beschreibung und das Kennwort ein, und bestätigen Sie anschließend das Kennwort.

**Wichtig**

Sie können den Benutzernamen nicht als Kennwort für das Konto verwenden. Geben Sie ein Kennwort ein, das sich vom Benutzernamen unterscheidet.

6. Geben Sie eine E-Mail-Adresse für das Konto ein.

**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 7-88](#).

7. Klicken Sie auf **Weiter**.

Das Fenster **Schritt 2 Agent-Domänensteuerung** wird angezeigt.

8. Definieren Sie den Bereich der agent-Hierarchie, indem Sie die Root-Domäne oder mindestens eine Domäne in der agent-Hierarchie auswählen.

Nur die Domänen sind an dieser Stelle definiert worden. Die Zugriffsrechte für die ausgewählten Domänen werden in Schritt 10 definiert.

9. Klicken Sie auf **Weiter**.

Das Fenster **Schritt 3 Agent-Hierarchiemenü definieren** wird angezeigt.

10. 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 13-15](#).

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 13-14. 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
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.

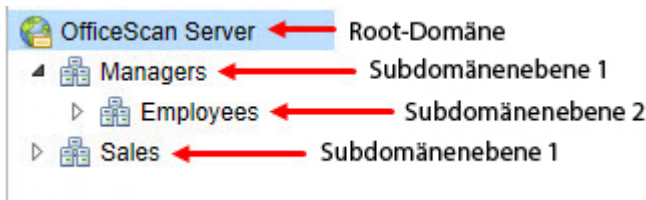
11. Klicken Sie auf **Fertig stellen**.

12. 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 13-15. Berechtigungen für das Benutzerkonto „Chris“

DOMÄNE	GEWÜNSCHTE BERECHTIGUNGEN
OfficeScan Server	Keine bestimmten Berechtigungen.
Managers	Protokolle anzeigen

DOMÄNE	GEWÜNSCHTE BERECHTIGUNGEN
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.

Ein benutzerdefiniertes Konto ändern



Hinweis

Nach dem Aktualisieren des OfficeScan Servers müssen Sie alle benutzerdefinierten Konten bearbeiten und alle neuen Funktionen im Bildschirm **Schritt 3 Agent-Hierarchiemenu definieren** für zuvor hinzugefügte benutzerdefinierte Konten manuell aktivieren. Weitere Informationen zu Berechtigungen finden Sie unter [Definieren von Berechtigungen für Domänen auf Seite 13-20](#).

Prozedur

1. Navigieren Sie zu **Administration > Kontenverwaltung > Benutzerkonten**.
2. Klicken Sie auf das Benutzerkonto.
3. Aktivieren oder deaktivieren Sie das Konto mit Hilfe des vorgesehenen Kontrollkästchens.
4. Ändern Sie Folgendes:
 - Rolle
 - Beschreibung
 - Kennwort

**Hinweis**

Sie können nicht das zuvor konfigurierte Kennwort erneut eingeben, während Sie ein Konto bearbeiten. Verändern Sie nicht das **Kennwort**-Feld, um das zuvor konfigurierte Kennwort weiter zu verwenden.

- E-Mail-Adresse
5. Klicken Sie auf **Weiter**.
 6. Definieren Sie den Bereich der Agent-Hierarchie.
 7. Klicken Sie auf **Weiter**.
 8. 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 13-15](#)*.
 9. Klicken Sie auf **Fertig stellen**.
 10. Senden Sie die neuen Kontodaten an den Benutzer.

Active Directory-Konten oder -Gruppen hinzufügen

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 zum Erstellen von Benutzerrollen finden Sie unter *[Benutzerdefiniert auf Seite 13-11](#)*.
5. Wählen Sie **Active Directory-Benutzer oder -Gruppe** aus.

6. Suchen Sie nach einem Konto (Benutzername oder Gruppe), indem Sie den Benutzernamen und die Domäne angeben, zu der das Konto gehört.

**Hinweis**

Verwenden Sie das Platzhalterzeichen (*), um nach mehreren Konten zu suchen. Wenn Sie das Platzhalterzeichen nicht angeben, müssen Sie den vollständigen Kontonamen eingeben. OfficeScan gibt kein Ergebnis zurück, wenn die Kontonamen unvollständig sind oder die Standardgruppe "Domänenbenutzer" verwendet wird.

7. Wenn OfficeScan ein gültiges Konto findet, wird der Name des Kontos unter **Benutzer und Gruppen** angezeigt. Klicken Sie auf das Symbol für "Vor" (>), um das Konto unter **Ausgewählte Benutzer und Gruppen** zu verschieben.

Wenn Sie eine Active Directory-Gruppe angeben, erhalten alle Mitglieder, die der Gruppe angehören, dieselbe Rolle. Wenn ein bestimmtes Konto zu wenigstens zwei Gruppen gehört und sich die Rollen für beide Gruppen unterscheiden:

- Die Berechtigungen für beide Rollen werden zusammengeführt. Wenn ein Benutzer eine bestimmte Einstellung konfiguriert und ein Konflikt zwischen den Berechtigungen für diese Einstellung besteht, erhält die höhere Berechtigung Vorrang.
- Alle Benutzerrollen werden in den Systemereignisprotokollen angezeigt. Beispielsweise ist der Benutzer "John Doe" mit den folgenden Rollen angemeldet: Administrator, Hauptbenutzer.

8. Klicken Sie auf **Weiter**.

Das Fenster **Schritt 2 Agent-Domänensteuerung** wird angezeigt.

9. Definieren Sie den Bereich der Agent-Hierarchie.

10. Klicken Sie auf **Weiter**.

Das Fenster **Schritt 3 Agent-Hierarchiemenü definieren** wird angezeigt.

11. 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 13-15*.

12. Klicken Sie auf **Fertig stellen**.
 13. Weisen Sie die Benutzer darauf hin, sich an der Webkonsole mit ihrem Domännennamen und Kennwort anzumelden.
-

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 verfügbaren Richtlinienkonfigurationen.

TABELLE 13-16. OfficeScan Richtlinienverwaltungstypen in Control Manager

RICHTLINIENTYP	FUNKTIONEN
OfficeScan Antivirus- und Agent-Einstellungen	• Zusätzliche DienstEinstellungen • Einstellungen der Verhaltensüberwachung • Einstellungen der Gerätesteuerung • Einstellungen für manuelle Suche • Berechtigungen und andere Einstellungen • Einstellungen für Echtzeitsuche • Liste der zulässigen Spyware/ Grayware • Suchmethoden • Einstellungen für Jetzt durchsuchen • Einstellungen für die zeitgesteuerte Suche • Verdächtige Verbindungseinstellungen • Update-Agent-Einstellungen • Web-Reputation-Einstellungen
Datenschutz	Einstellungen der Richtlinien für 'Prävention vor Datenverlust'  Hinweis Verwalten Sie die Gerätesteuerungsberechtigungen für den Datenschutz in den OfficeScan Agent-Richtlinien.

- Die folgenden Einstellungen von einem OfficeScan Server auf einen anderen von der Control Manager Konsole aus replizieren:

- *Datenbezeichnertypen auf Seite 10-6*
- *Vorlagen für 'Prävention vor Datenverlust' auf Seite 10-22*

**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.

TABELLE 13-17. Unterstützte Versionen von Control Manager

OFFICESCAN SERVER	CONTROL MANAGER VERSION	
	6.0 ODER HÖHER	5.5 SP1
Dual-stack	Ja	Ja
Reines IPv4	Ja	Ja
Reines IPv6	Ja	Nein

**Hinweis**

IPv6-Unterstützung für Control Manager ist ab Version 5.5 Service Pack 1 verfügbar.

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/emca/?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

Prozedur

1. Navigieren Sie zu **Administration > Einstellungen > Control Manager**.
2. Geben Sie den Anzeigenamen des Elements an, bei dem es sich um den Namen des OfficeScan Servers handelt, der im Control Manager angezeigt wird.

Standardmäßig besteht der Anzeigenamen des Elements aus dem Hostnamen des Server-Computers und diesem Produktnamen (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 Sie den Typ des Control Managers FQDN oder die IPv4-Adresse ein.
 - Bei einem reinen IPv6 OfficeScan Server geben Sie den Typ des Control Managers FQDN oder die IPv6-Adresse ein.



Hinweis

Nur Control Manager 5.5 SP1 und höhere Versionen unterstützen IPv6.

4. Erfordert der IIS Webserver des Control Manager eine Authentifizierung, geben Sie den Benutzernamen und das Kennwort ein.
5. 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
6. 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.
7. 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.

8. 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).
 9. 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.
 10. Klicken Sie auf **Registrierung aufheben**, wenn OfficeScan nicht mehr vom Control Manager Server verwaltet werden soll.
-

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.
-

Richtlinien-Export-Tool

Das Trend Micro OfficeScan Server Richtlinien-Export-Tool hilft Administratoren beim Exportieren von OfficeScan Richtlinieneinstellungen, die von Control Manager 6.0 oder höher unterstützt werden. Administratoren benötigen darüber hinaus das Control Manager Import-Tool zum Importieren der Richtlinien. Das Richtlinien-Export-Tool unterstützt OfficeScan 10.6 Service Pack 1 und höher.

• Einstellungen für Echtzeitsuche	• Einstellungen der Verhaltensüberwachung
• Einstellungen für die zeitgesteuerte Suche	• Einstellungen der Gerätesteuerung
• Einstellungen für manuelle Suche	• Einstellungen für 'Prävention vor Datenverlust'

- Einstellungen für Jetzt durchsuchen
- Update-Agent-Einstellungen
- Web-Reputation-Einstellungen
- Suchmethode
- Berechtigungen und andere Einstellungen
- Zusätzliche Diensteinstellungen
- Liste der zulässigen Spyware/Grayware
- Verdächtige Verbindungseinstellungen

Richtlinien-Export-Tool verwenden

Prozedur

1. Gehen Sie auf dem OfficeScan Server-Computer zu *<Installationsordner des Servers>* \PCCSRV\Admin\Utility\PolicyExportTool.
2. Doppelklicken Sie auf PolicyExportTool.exe, um das Richtlinien-Export-Tool zu starten.

Eine Befehlszeilenschnittstelle wird geöffnet, und das Richtlinien-Export-Tool beginnt mit dem Export der Einstellungen. Dabei werden zwei Ordner (PolicyClient und PolicyDLP) im Ordner PolicyExportTool erstellt, in die die exportierten Einstellungen eingefügt werden.

3. Kopieren Sie die beiden Ordner in den Installationsordner von Control Manager.
4. Führen Sie das Richtlinien-Import-Tool auf dem Control Manager Server aus.

Einzelheiten zum Richtlinien-Import-Tool erhalten Sie in der *Readme-Datei zum Richtlinien-Import-Tool* auf dem Control Manager Server (Installationsordner für TMCM \WebUI\WebApp\widget\common\tool\PolicyImport\).

**Hinweis**

Das Richtlinien-Import-Tool exportiert keine benutzerdefinierten Datenbezeichner und benutzerdefinierte DLP-Vorlagen. Zum Export benutzerdefinierter Datenbezeichner und DLP-Vorlagen ist ein manueller Export aus der OfficeScan Konsole und ein anschließender manueller Import über die Control Manager Konsole erforderlich.

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 gegen diese Objekte aus einem Control Manager Server abrufen, der mit Deep Discovery (für OfficeScan Version 10.6) verbunden ist.

Aktivieren Sie nach dem Abonnieren von Control Manager die Typen der verdächtigen Objekte, um C&C-Callbacks oder möglicherweise gezielte Angriffe zu überwachen, die von agents im Netzwerk identifiziert wurden. Zu den verfügbaren Listen gehören:

- Liste der verdächtigen URLs
- Liste der verdächtigen IPs
- Liste der verdächtigen Dateien

**Hinweis**

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 *Connected Threat Defense Primer*.

Einstellungen für Liste der verdächtigen Objekte konfigurieren

Bei der Registrierung 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 13-28*](#).

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)
- Administratoren können jederzeit eine manuelle Synchronisierung der Liste der verdächtigen Objekte vornehmen, indem sie auf die Schaltfläche **Jetzt synchronisieren** klicken.
3. Geben Sie im Abschnitt **Update-Einstellungen für Agent** den Zeitpunkt für die Aktualisierung der Listen der verdächtigen Objekte an.
 - **OfficeScan Agents basierend auf Komponenten-Update-Zeitplan des Agent benachrichtigen:** OfficeScan Agents aktualisieren die Listen der verdächtigen Objekte basierend auf dem aktuellen Update-Zeitplan.
 - **OfficeScan Agents nach der Aktualisierung der Liste der verdächtigen Objekte auf dem Server automatisch benachrichtigen:** OfficeScan Agents

aktualisiert die Listen der verdächtigen Objekte automatisch, wenn der Server die aktualisierten Listen erhält.

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-Profil 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 an Sie oder andere OfficeScan Administratoren senden, wenn folgendes entdeckt wurde:

TABELLE 13-18. Funde, die Administratorbenachrichtigungen auslösen

ERKANNTE BEDROHUNGEN	BENACHRICHTIGUNGSKANÄLE		
	E-MAIL	SNMP-TRAP	WINDOWS NT EREIGNISPROTOKOL LE
Viren und Malware	Ja	Ja	Ja
Spyware und Grayware	Ja	Ja	Ja
Übertragungen digitaler Assets	Ja	Ja	Ja
C&C-Callbacks	Ja	Ja	Ja
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

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** entweder eine IPv4-/IPv6-Adresse oder einen Endpunktnamen an.
 - b. Geben Sie eine Portnummer zwischen 1 und 65535 ein.

- c. Geben Sie eine E-Mail-Adresse ein.

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 aus:
- **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 kryptographischen 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.
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 13-40](#).

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 13-19. 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

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 wurden und 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 7-98*
- *Spyware/Grayware-Protokolle anzeigen auf Seite 7-107*

- *Spyware-/Grayware-Wiederherstellungsprotokolle anzeigen auf Seite 7-111*
- *Firewall-Protokolle anzeigen auf Seite 12-32*
- *Web-Reputation-Protokolle anzeigen auf Seite 11-26*
- *Protokolle zu verdächtigen Verbindungen anzeigen auf Seite 11-29*
- *Protokolle zu verdächtigen Dateien anzeigen auf Seite 7-111*
- *C&C Callback-Protokolle anzeigen auf Seite 11-27*
- *Verhaltensüberwachungsprotokolle anzeigen auf Seite 8-16*
- *Protokolle der Gerätesteuerung anzeigen auf Seite 9-19*
- *Protokolle zu Suchvorgängen anzeigen auf Seite 7-113*
- *Protokolle der Funktion "Prävention vor Datenverlust" anzeigen auf Seite 10-61*
- *OfficeScan Agent Update-Protokolle anzeigen auf Seite 6-55*
- *Verbindungsüberprüfungsprotokolle anzeigen auf Seite 14-47*

Der OfficeScan Server erstellt die folgenden Protokolle:

- *OfficeScan Server-Update-Protokolle auf Seite 6-29*
- *Systemereignisprotokolle auf Seite 13-38*

Die folgenden Protokolle sind auch auf dem OfficeScan Server und den OfficeScan Agents verfügbar:

- *Windows Ereignisprotokolle auf Seite 16-24*
- *OfficeScan Serverprotokolle auf Seite 16-3*
- *OfficeScan Agent Protokolle auf Seite 16-15*

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 Stammsymbol () , 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 die Protokollarten aus, die gelöscht werden sollen. Nur die folgenden Protokolle können manuell gelöscht werden:
 - Verhaltensüberwachungsprotokolle
 - C&C-Callback-Protokolle
 - Protokolle für 'Prävention vor Datenverlust'
 - Protokolle der Gerätesteuerung
 - Firewall-Protokolle
 - 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 aus, ob alle Protokolle der angegebenen Protokollarten oder nur diejenigen gelöscht werden sollen, die älter als eine bestimmte Anzahl von Tagen sind.
 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 14-82](#).

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 13-20. 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.
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 13-38](#).



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 2008 R2 SP2 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.



Wichtig

Vor dem Ausführen des SQL Server Migration Tools unter Windows Server 2008 oder höher unter der Verwendung der Anmeldedaten zur Windows-Authentifizierung des Domänenbenutzers

- müssen Sie die Option **Benutzerzugriffskontrolle** ausschalten
 - Der OfficeScan Master Service kann nicht unter der Verwendung des Benutzerkontos der Domäne ausgeführt werden, das für die Anmeldung beim SQL Server verwendet wird
-

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. Wählen Sie den Migrationstyp aus:

OPTION	BEZEICHNUNG
Neue SQL Server 2008 R2 SP2 Express-Version installieren und OfficeScan-Datenbank migrieren	Installiert SQL Server 2008 R2 SP2 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: <Host-Name oder IP-Adresse des SQL Servers>\<Instanzname>
- Für Migrationen des SQL Servers: <Host-Name oder IP-Adresse des SQL Servers>,<Portnummer>\<Instanzname>
- Beim Wechsel zu einer vorhandenen OfficeScan SQL-Datenbank: <Host-Name oder IP-Adresse des SQL Servers>,<Portnummer>\<Instanzname>

**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.
-

**Wichtig**

Wenn Sie das **Windows-Konto** für die Anmeldung auf dem Server verwenden:

- Für ein standardmäßiges Domänen-Administratorkonto:
 - **Format von Benutzernamen:** domain_name\administrator
 - Das Konto benötigt Folgendes:
 - Gruppen: „Administratorgruppe“
 - Benutzerrollen: „Als Dienst anmelden“ und „Als Batchauftrag anmelden“
 - Datenbank-Rollen: „dbcreator“, „bulkadmin“ und „db_owner“
 - Für ein Domänen-Benutzerkonto:
 - **Format von Benutzernamen:** domain_name\user_name
 - Das Konto benötigt Folgendes:
 - Gruppen: „Administratorgruppe“ und „Domänen-Administratoren“
 - Benutzerrollen: „Als Dienst anmelden“ und „Als Batchauftrag anmelden“
 - Database roles: „dbcreator“, „bulkadmin“, and „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: 6 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 13-52.*](#)

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 13-21. 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 (IIS oder Apache Webserver) ein, damit die Netzwerkcomputer sich mit dem OfficeScan Server verbinden können. Konfigurieren Sie den Webserver, mit dem sich die Endpunkt-agents 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!

Wenn die Verbindungseinstellungen geändert werden, ist es möglich, dass die Verbindung zwischen dem Server und den agents dauerhaft getrennt wird und eine Neuverteilung 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 13-55*
- *Erweiterte Verschlüsselung der Kommunikation zwischen Server und Agent auf Seite 13-60*

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 13-57](#).

Authentifizierung der vom Server gestarteten Kommunikation konfigurieren

Prozedur

1. Navigieren Sie auf dem OfficeScan Server zum Ordner <Server_installation_folder> \PCCSRV und öffnen Sie die Datei ofcscan.ini mit einem Texteditor.
2. Fügen Sie die Zeichenfolge SGNF im Abschnitt [Global Settings] hinzu, oder bearbeiten Sie diese Zeichenfolge.

Authentifizierung aktivieren: SGNF=1

Authentifizierung deaktivieren: SGNF=0

**Hinweis**

Die Authentifizierung wird von OfficeScan standardmäßig aktiviert. Fügen Sie den Schlüssel `SGNF` in der Datei `ofscan.ini` nur hinzu, wenn Sie diese Funktion deaktivieren möchten.

3. Wechseln Sie auf der Webkonsole zu **Agents > Globale Agent-Einstellungen** und klicken Sie auf **Speichern**, um diese Einstellung an die Agents zu verteilen.
-

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
-

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_Passwort]	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]	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 Das Zertifikat liegt im ZIP-Format vor.		 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]]	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.
 Hinweis Das Zertifikat liegt im ZIP-Format vor.		
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] [Zertifikatspfad]]	CertificateManager.exe -i strongpassword D:\Test \OfcNTCer.pfx	Importiert ein Trend Micro-Zertifikat in den Zertifikatspeicher
 Hinweis Der Standardname des Zertifikats ist: OfcNTCer.pfx		
CertificateManager.exe -l [CSV-Pfad]	CertificateManager.exe -l D: \Test \MismatchedAgentsList.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. Navigieren Sie zum Abschnitt **Kommunikation zwischen Server und Agent**.
3. Klicken Sie auf die Schaltfläche **Ändern** neben **AES-256-Verschlüsselung für Kommunikation zwischen dem OfficeScan Server und OfficeScan Agents**.

Eine Meldung wird angezeigt.

4. Klicken Sie auf **Versionen überprüfen**, um zu bestätigen, dass Sie alle Agents auf OfficeScan 11.0 SP1 oder höher aktualisiert haben.
5. 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

Über das Fenster **Einstellungen der Webkonsole** können Sie folgende Aktionen ausführen:

- Konfigurieren Sie den OfficeScan Server, um das Übersichts-Dashboard in regelmäßigen Abständen zu erneuern. Standardmäßig erneuert der Server das Dashboard alle 30 Sekunden. Die Anzahl der Sekunden kann 10 bis 300 betragen.
- Die Zeitüberschreitungseinstellungen der Webkonsole angeben. Standardmäßig wird ein Benutzer nach 30 Minuten Inaktivität automatisch von der Webkonsole abgemeldet. Der Wert für die Anzahl der Minuten kann 10 bis 60 betragen.

Einstellungen der Webkonsole konfigurieren

Prozedur

1. Navigieren Sie zu **Administration > Einstellungen > Webkonsole**.
 2. Wählen Sie **Automatische Aktualisierung aktivieren**, und wählen Sie anschließend das Intervall für die Aktualisierung.
 3. Wählen Sie **Automatische Abmeldung von der Webkonsole aktivieren** und wählen Sie anschließend das Intervall für die Zeitüberschreitung aus.
 4. 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 Ordner *<Installationsordner des Agents>* \SUSPECT 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 7-43*.

Wenn sich der vorgesehene Quarantäne-Ordner auf dem OfficeScan Server-Computer befindet, ändern Sie die Einstellungen für den Quarantäne-Ordner des Servers von der Webkonsole aus. Der Server speichert die unter Quarantäne gestellten Dateien im Ordner *<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 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 14

OfficeScan Agent verwalten

In diesem Kapitel werden die Verwaltung und Konfiguration von OfficeScan Agent beschrieben.

Es werden folgende Themen behandelt:

- *Endpunktspeicherort auf Seite 14-2*
- *OfficeScan Agent Programmverwaltung auf Seite 14-6*
- *Agent-Server-Verbindung auf Seite 14-27*
- *OfficeScan Agent Proxy-Einstellungen auf Seite 14-52*
- *OfficeScan Agent-Informationen anzeigen auf Seite 14-57*
- *Agent-Einstellungen importieren und exportieren auf Seite 14-57*
- *Einhaltung von Sicherheitsrichtlinien auf Seite 14-59*
- *Unterstützung für Trend Micro Virtual Desktop auf Seite 14-79*
- *Globale Agent-Einstellungen auf Seite 14-94*
- *Agent-Berechtigungen und weitere Einstellungen konfigurieren auf Seite 14-96*

Endpunktspeicherort

OfficeScan unterstützt die Funktion Location Awareness, mit der festgestellt wird, ob sich der OfficeScan Agent an einem lokalen oder an einem externen Standort befindet. Location Awareness wird in folgenden OfficeScan Funktionen und Services genutzt:

TABELLE 14-1. Funktionen und Services mit Location Awareness

FUNKTION/SERVICE	BESCHREIBUNG
Web-Reputation-Dienste	Der Standort des OfficeScan Agents legt fest, welche Web-Reputation-Richtlinie der OfficeScan Agent anwendet. Bei externen agents setzen Administratoren normalerweise eine strengere Richtlinie durch. Weitere Informationen zu Web-Reputation-Richtlinien finden Sie unter Web-Reputation-Richtlinien auf Seite 11-5.
File-Reputation-Dienste	Bei agents, die die intelligente Suche verwenden, bestimmt der Standort des OfficeScan Agents die Smart Protection Quelle, an welche die agents Anfragen senden. Externe OfficeScan Agents senden Anfragen an das Smart Protection Network, während interne agents ihre Anfragen an die Quellen senden, die in der Liste der Smart Protection Quelle angegeben ist. Weitere Informationen zu Smart Protection Quellen finden Sie unter Smart Protection Quellen auf Seite 4-6.
Prävention vor Datenverlust	Der Standort des OfficeScan Agent legt fest, welche Richtlinie zur Prävention vor Datenverlust der agent anwendet. Bei externen agents setzen Administratoren normalerweise eine strengere Richtlinie durch. Weitere Informationen über Richtlinien zur Prävention vor Datenverlust finden Sie unter Richtlinien für 'Prävention vor Datenverlust' auf Seite 10-3.

FUNKTION/SERVICE	BESCHREIBUNG
Gerätesteuerung	Der Standort des OfficeScan Agents legt fest, welche Gerätesteuerungsrichtlinie der agent anwendet. Bei externen agents setzen Administratoren normalerweise eine strengere Richtlinie durch. Weitere Informationen zu Gerätesteuerungsrichtlinien finden Sie unter Gerätesteuerung auf Seite 9-2.

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 13-34*.

- 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 Roaming- 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 entdeckt eine IP-Adressänderung auf dem Endpunkt.
 - Der OfficeScan Agent wird neu gestartet.
 - Der Server startet eine Verbindungsüberprüfung. Weitere Informationen finden Sie unter *OfficeScan Agent Symbole auf Seite 14-28*.
 - 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 Gateway Settings Importer Tool, um eine Liste mit Gateway-Einstellungen in dieses Fenster zu importieren.

Weitere Informationen finden Sie unter [Import von Gateway-Einstellungen auf Seite 14-5](#).

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. Wechseln Sie auf dem Servercomputer in den Ordner *<Installationsordner des Servers>* \PCCSRV\Admin\Utility\GatewaySettingsImporter, und doppelklicken Sie auf GSImporter.exe.



Hinweis

Der Gateway Settings Importer kann nicht über Terminal Services ausgeführt werden.

3. Navigieren Sie im Fenster **Import von Gateway-Einstellungen** zu der Datei, die Sie in Schritt 1 erstellt haben, und klicken Sie auf **Importieren**.

4. Klicken Sie auf **OK**.

Die Gateway-Einstellungen werden im Fenster **Endpunktspeicherort** angezeigt, und der OfficeScan Server verteilt die Einstellungen an die OfficeScan Agents.

5. 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**.

6. 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 14-7*
- *Neustart des OfficeScan Agent Dienstes auf Seite 14-12*
- *OfficeScan Agent Eigenschutz auf Seite 14-13*
- *Einschränkung des Zugriffs auf die OfficeScan Agent-Konsole auf Seite 14-18*

- *OfficeScan Agent Beenden und entsperren auf Seite 14-19*
- *OfficeScan AgentRoaming-Berechtigungen auf Seite 14-20*
- *Agent Mover auf Seite 14-24*
- *Inaktive OfficeScan Agents auf Seite 14-26*

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.

TABELLE 14-2. OfficeScan Agent-Dienste

DIENT	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 Echtzeitsuche (ntrtscan.exe)	• Echtzeitsuche • Zeitgesteuerte Suche • Manuelle Suche/Sofort durchsuchen

DIENT	KONTROLLIERTE FUNKTIONSMERKMALE
Gemeinsames Client Solution Framework für OfficeScan (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 14-10](#).

Bei Desktop-Plattformen deaktivieren Sie die Dienste nur, wenn Sie einen deutlichen Leistungsabfall verzeichnen.

Die Agent-Dienste von der Webkonsole aus aktivieren bzw. deaktivieren

Prozedur

1. Navigieren Sie zu **Agents > Agent-Verwaltung**.
2. Für OfficeScan Agents unter Windows XP, Vista, 7, 8 oder 8.1:

- a. Klicken Sie in der agent-Hierarchie auf das Stammsymbol , 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 unter Window XP, Vista, 7, 8 oder 8.1. Diese Einstellung gilt nicht für agents unter einer Windows Server-Plattform, selbst wenn sie zu den Domänen gehören.

- b. Klicken Sie auf **Einstellungen > Zusätzliche Diensteinstellungen**.
- c. Aktivieren oder deaktivieren Sie das Kontrollkästchen unter den folgenden Abschnitten:
- **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 XP/Vista/7/8/8.1 agents und auf solche agents an, die neu zu einer vorhandenen/künftigen Domäne hinzukommen. 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 XP/Vista/7/8/8.1 agents an, die zu zukünftigen Domänen hinzukommen. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
3. Für OfficeScan Agents unter Windows Server 2003, Windows Server 2008 oder Windows Server 2012:

- a. Wählen Sie einen einzelnen agent in der agent-Hierarchie aus.
 - b. Klicken Sie auf **Einstellungen > Zusätzliche Diensteinstellungen**.
 - c. Aktivieren oder deaktivieren Sie das Kontrollkästchen unter den folgenden Abschnitten:
 - **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 TMBMCLL.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**.

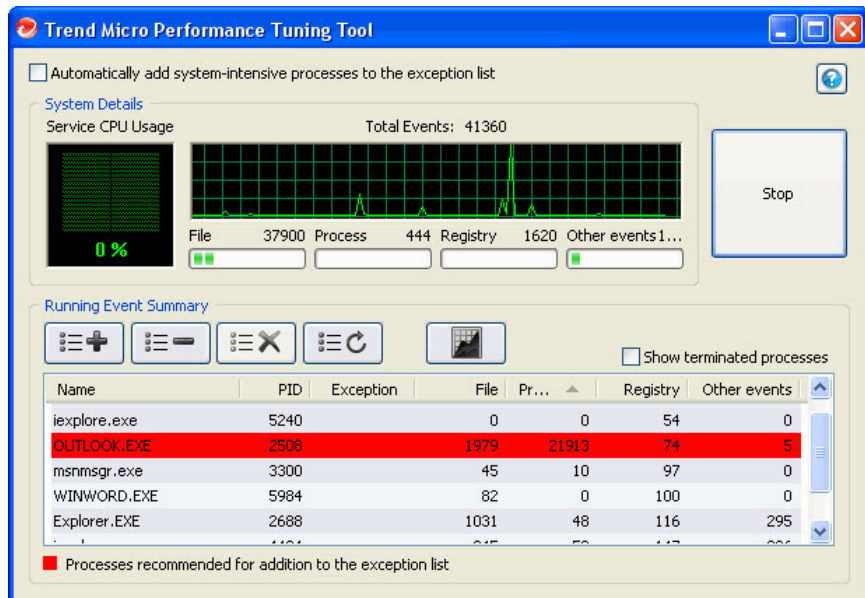


ABBILDUNG 14-1. Markierter systemintensiver Prozess

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 8-7.*](#)

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 14-7.*](#)

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. Gehen Sie zum Abschnitt **Neustart des OfficeScan Dienstes**.
3. Wählen Sie **OfficeScan Agent-Dienst beim unerwarteten Beenden des Diensts automatisch neu starten**.
4. 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.
 - **Wenn der erste Neustartversuch fehlschlägt, noch __ Mal versuchen:**
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 14-14](#)*
- *[Dateien im OfficeScan Agent-Installationsordner schützen auf Seite 14-15](#)*
- *[OfficeScan Agent-Registrierungsschlüssel schützen auf Seite 14-16](#)*
- *[OfficeScan Agent-Prozesse schützen auf Seite 14-17](#)*

Eigenschutzeinstellungen des OfficeScan Agents konfigurieren

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. 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 14-14*
 - *Dateien im OfficeScan Agent-Installationsordner schützen auf Seite 14-15*
 - *OfficeScan Agent-Registrierungsschlüssel schützen auf Seite 14-16*
 - *OfficeScan Agent-Prozesse schützen auf Seite 14-17*
6. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

OfficeScan Agent-Dienste schützen

OfficeScan blockiert alle Versuche, die folgenden OfficeScan Agent-Dienste zu beenden:

- OfficeScan NT Listener (TmListen.exe)
- OfficeScan NT Echtzeitsuche (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 OfficeScan möglicherweise, dass sich Produkte anderer Hersteller erfolgreich auf den Endpunkten installieren. 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
 - msvcpl80.dll
 - msver80.dll
 - OfceSCV.dll
 - OFCESCVPack.exe
 - patchbld.dll
 - patchw32.dll
 - patchw64.dll
 - PiReg.exe
 - sslay32.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

OfficeScan sperrt alle Versuche, unter den folgenden Registrierungsschlüsseln und Unterschlüsseln Einträge zu ändern, zu löschen oder neue 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

OfficeScan blockiert alle Versuche, die Prozesse in der folgenden Tabelle zu beenden.

PROZESS	BESCHREIBUNG
TmListen.exe:	Empfängt Befehle und Benachrichtigungen vom OfficeScan Server und ermöglicht die Kommunikation zwischen OfficeScan Agent und 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, Netzwerkvirusuche 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.

OfficeScan kann auch vor dem Hinzufügen von Prozessen in den Microsoft 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 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 bzw. deaktivieren auf Seite 14-8*.

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 Stammsymbol () , 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

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 Stammsymbol () , 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. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen

Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

OfficeScan AgentRoaming-Berechtigungen

Gewähren Sie bestimmten Benutzern die Roaming-Berechtigung für OfficeScan Agents, wenn agent-Server-Ereignisse die Aufgaben des Benutzers behindern. Wenn ein Benutzer beispielsweise häufig Präsentationen zeigt, kann er vor Beginn der Präsentation den Roaming-Modus aktivieren und so verhindern, dass der OfficeScan Server OfficeScan Agent-Einstellungen verteilt und Suchen auf dem OfficeScan Agent startet.

Wenn für OfficeScan Agents der Roaming-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 Roaming-agents aus:

- Der Benutzer führt ein manuelles Update aus.
- Das automatische agent-Update wird ausgeführt. Sie können automatische agent-Updates auf Roaming-agents deaktivieren.

Weitere Informationen finden Sie unter *[Automatische Agent-Updates auf Roaming-Agents deaktivieren auf Seite 14-22](#)*.

- 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 [Die Berechtigung für zeitgesteuerte Updates auf Roaming-OfficeScan Agents widerrufen OfficeScan Agents auf Seite 14-22](#).

Die Berechtigung zum Roaming des Agents 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. Wechseln Sie auf der Registerkarte **Berechtigungen** zum Abschnitt **Roaming**.
 5. Wählen Sie die Option **Roaming-Modus aktivieren**.
 6. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.
-

Automatische Agent-Updates auf Roaming-Agents deaktivieren

Prozedur

1. Navigieren Sie zu **Updates > Agents > Automatisches Update**.
2. Navigieren Sie zum Abschnitt **Ereignisbedingtes Update**.
3. Deaktivieren Sie die Option **Auch auf Roaming- und Offline-Agents verteilen**.



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.

Die Berechtigung für zeitgesteuerte Updates auf Roaming-OfficeScan Agents widerrufen OfficeScan 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. Gehen Sie zum Abschnitt **Sprachkonfiguration für Agent**.
3. 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.

4. 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. Öffnen Sie auf dem OfficeScan Server den Ordner *<Installationsordner des Servers>* \PCCSRV\Admin\Utility\IpXfer.
2. Kopieren Sie IpXfer.exe auf den OfficeScan Agent Endpunkt. Wenn der OfficeScan Agent Endpunkt auf einer x64-Plattform ausgeführt wird, kopieren Sie stattdessen 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 <Speicherort des Zertifikats und Dateiname>

TABELLE 14-3. Agent Mover-Parameter

PARAMETER	ERKLÄRUNG
<Name der ausführbaren Datei>	IpXfer.exe oder IpXfer_x64.exe
-s <server name>	Der Name des OfficeScan Zielservers (der Server, dem der OfficeScan Agent zugeordnet werden soll)
-p <Server-Listening-Port>	Der Listening Port (oder der vertrauenswürdige Port) des OfficeScan Zielservers. Klicken Sie im Hauptmenü auf Administration > Einstellungen > Agent-Verbindung , um den Listening-Port auf der OfficeScan Webkonsole anzuzeigen.
-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.
-e <Speicherort des Zertifikats und Dateiname>	Importiert ein neues Authentifizierungszertifikat für den OfficeScan Agent während des Verschiebungsprozesses. 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\Pcnet\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.

Beispiele:

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

```
ipXfer_x64.exe -s Server02 -p 8080 -c 21112 -d Workgroup  
\Gruppe01
```

5. Bestätigen Sie, dass der OfficeScan Agent ab jetzt an den anderen Server berichtet. Gehen Sie dazu folgendermaßen vor:
 - a. Klicken Sie in der Taskleiste auf dem OfficeScan Agent-Endpunkt mit der rechten Maustaste auf das Symbol des OfficeScan Agent-Programms.
 - 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, sollten Sie den Master Service (ofservice.exe) des neuen Servers neu starten.

Inaktive OfficeScan Agents

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 5-9*
- *OfficeScan Agent Symbole auf Seite 14-28*
- *Verbindung des Agents zum Server überprüfen auf Seite 14-45*
- *Verbindungsüberprüfungsprotokolle auf Seite 14-46*
- *Nicht erreichbar Agents auf Seite 14-47*

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 14-4. 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 14-42.
	Roaming-agents können möglicherweise nicht 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 Roaming-agents finden Sie unter OfficeScan AgentRoaming-Berechtigungen auf Seite 14-20.

AGENT-STATUS	BESCHREIBUNG	VISUELLER HINWEIS
Verfügbare it von Smart Protection Quellen	Zu den Smart Protection Quellen zählen Smart Protection Server und Trend Micro Smart Protection Network.	Das Symbol zeigt ein Häkchen, wenn eine Smart Protection Quelle verfügbar ist. 
	agents der herkömmlichen Suche verbinden sich für Web-Reputation-Abfragen mit Smart Protection Quellen.	Das Symbol zeigt einen Fortschrittsbalken, wenn keine Smart Protection Quelle verfügbar ist und der agent versucht, eine Verbindung zu den Quellen herzustellen. 
	agents der intelligenten Suche verbinden sich für Such- und Web- Reputation-Abfragen mit Smart Protection Quellen.	Weitere Informationen zu diesem Problem finden Sie unter Lösungen für Probleme, die durch OfficeScan Agent-Symbole angezeigt werden auf Seite 14-42. 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. Für die 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. Für die 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 14-42.

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 14-42.
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 6-30.

Intelligente Suchsymbole

Wenn OfficeScan Agents die intelligente Suche verwenden, werden entsprechend die nachfolgenden Symbole angezeigt.

TABELLE 14-5. 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
	Offline	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert

SYMBOL	VERBINDUNG MIT OFFICESCAN SERVER	VERFÜGBARKEIT VON SMART PROTECTION QUELLEN	ECHTZEITSUCHDIENST	ECHTZEITSUCHE
	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
	Roaming	Verfügbar	Funktioniert	Aktiviert
	Roaming	Verfügbar	Funktioniert	Deaktiviert
	Roaming	Verfügbar	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig
	Roaming	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert
	Roaming	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Deaktiviert
	Roaming	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 14-6. Herkömmliche Suchsymbole

SYM BOL	VERBINDUNG MIT OFFICESCAN SERVER	WEB-REPUTATION- DIENSTE ZUR VERFÜGUNG GESTELLT VON SMART PROTECTION QUELLEN	ECHTZEITSUCH DIENST	ECHTZEITSUCH E	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
	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

SYM BOL	VERBINDUNG MIT OFFICESCAN SERVER	WEB-REPUTATION- DIENSTE ZUR VERFÜGUNG GESTELLT VON SMART PROTECTION QUELLEN	ECHTZEITSUCH DIENST	ECHTZEITSUCH E	VIREN- PATTERN
	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
	Offline	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert	Stark veraltet
	Offline	Verfügbar	Funktioniert	Deaktiviert	Aktuell oder leicht veraltet

SYM BOL	VERBINDUNG MIT OFFICESCAN SERVER	WEB-REPUTATION- DIENSTE ZUR VERFÜGUNG GESTELLT VON SMART PROTECTION QUELLEN	ECHTZEITSUCH DIENST	ECHTZEITSUCH E	VIREN- PATTERN
	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
	Offline	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Stark veraltet
	Roaming	Verfügbar	Funktioniert	Aktiviert	Aktuell oder leicht veraltet

SYM BOL	VERBINDUNG MIT OFFICESCAN SERVER	WEB-REPUTATION- DIENSTE ZUR VERFÜGUNG GESTELLT VON SMART PROTECTION QUELLEN	ECHTZEITSUCH DIENST	ECHTZEITSUCH E	VIREN- PATTERN
	Roaming	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert	Aktuell oder leicht veraltet
	Roaming	Verfügbar	Funktioniert	Aktiviert	Stark veraltet
	Roaming	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Aktiviert	Stark veraltet
	Roaming	Verfügbar	Funktioniert	Deaktiviert	Aktuell oder leicht veraltet
	Roaming	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Deaktiviert	Aktuell oder leicht veraltet
	Roaming	Verfügbar	Funktioniert	Deaktiviert	Stark veraltet
	Roaming	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Funktioniert	Deaktiviert	Stark veraltet
	Roaming	Verfügbar	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Aktuell oder leicht veraltet

SYM BOL	VERBINDUNG MIT OFFICESCAN SERVER	WEB-REPUTATION- DIENSTE ZUR VERFÜGUNG GESTELLT VON SMART PROTECTION QUELLEN	ECHTZEITSUCH DIENST	ECHTZEITSUCH E	VIREN- PATTERN
	Roaming	Nicht verfügbar, Verbindung zu Quellen wird wiederhergestellt	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Aktuell oder leicht veraltet
	Roaming	Verfügbar	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Stark veraltet
	Roaming	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
	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

SYM BOL	VERBINDUNG MIT OFFICESCAN SERVER	WEB-REPUTATION- DIENSTE ZUR VERFÜGUNG GESTELLT VON SMART PROTECTION QUELLEN	ECHTZEITSUCH DIENST	ECHTZEITSUCH E	VIREN- PATTERN
	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
	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

SYM BOL	VERBINDUNG MIT OFFICESCAN SERVER	WEB-REPUTATION- DIENSTE ZUR VERFÜGUNG GESTELLT VON SMART PROTECTION QUELLEN	ECHTZEITSUCH DIENST	ECHTZEITSUCH E	VIREN- PATTERN
	Offline	Nicht zutreffend (Web-Reputation- Funktion auf agent deaktiviert)	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Stark veraltet
	Roaming	Nicht zutreffend (Web-Reputation- Funktion auf agent deaktiviert)	Funktioniert	Aktiviert	Aktuell oder leicht veraltet
	Roaming	Nicht zutreffend (Web-Reputation- Funktion auf agent deaktiviert)	Funktioniert	Aktiviert	Stark veraltet
	Roaming	Nicht zutreffend (Web-Reputation- Funktion auf agent deaktiviert)	Funktioniert	Deaktiviert	Aktuell oder leicht veraltet
	Roaming	Nicht zutreffend (Web-Reputation- Funktion auf agent deaktiviert)	Funktioniert	Deaktiviert	Stark veraltet
	Roaming	Nicht zutreffend (Web-Reputation- Funktion auf agent deaktiviert)	Deaktiviert oder nicht funktionsfähig	Deaktiviert oder nicht funktionsfähig	Aktuell oder leicht veraltet
	Roaming	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 Update erteilen.
Der Echtzeitsuchdienst wurde deaktiviert oder funktioniert nicht	Wenn der Echtzeitsuchdienst (OfficeScan NT Echtzeitsuche) deaktiviert wurde oder nicht funktioniert, müssen Benutzer den Dienst manuell über die Microsoft Management-Konsole starten.
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 Roaming-Modus.	Benutzer müssen zuerst den Roaming-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.

BEDINGUNG:	BESCHREIBUNG
	2. Lautet der Verbindungsstatus auf dem OfficeScan Agent „offline“, aber auf dem Server „online“, und verbindet sich der OfficeScan Agent gemäß der Auswahl während der Serverinstallation über den Domännennamen mit dem Server, hat sich möglicherweise dessen Domänenname geändert. Registrieren Sie den Domännennamen des OfficeScan am DNS oder WINS Server, oder fügen Sie den Domännennamen und die IP-Angaben zur Hosts-Datei im Ordner <Windows-Ordner>\system32\drivers\etc auf dem agent Endpunkt hinzu. 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 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 agent 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.

BEDINGUNG:	BESCHREIBUNG
	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: • <code>sscfcfg.ini</code> • <code>ssnotify.ini</code> 4. Öffnen Sie den Registrierungseditor, und überprüfen Sie, ob der agent mit dem Unternehmensnetzwerk verbunden ist. Schlüssel: <pre>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\iCRC Scan\Scan Server</pre> • Bei <code>LocationProfile=1</code> ist der OfficeScan Agent mit dem Netzwerk verbunden und sollte mit einem Smart Protection Server eine Verbindung herstellen können. • Bei <code>LocationProfile=2</code> 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 vom OfficeScan Agent Endpunkt aus Webseiten im Internet aufgerufen werden können. 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 Interner Proxy für OfficeScan Agents auf Seite 14-52 und Externer Proxy für OfficeScan Agents auf Seite 14-53. 6. Stellen Sie für agents der herkömmlichen Suche, auf denen Windows XP, Vista, Server 2003 und Server 2008 ausgeführt werden, sicher, dass der OfficeScan NT Proxy-Dienst (TmProxy.exe) ausgeführt wird. Wenn dieser Dienst angehalten wird, können sich agents nicht mit Smart Protection Quellen für Web Reputation verbinden.

BEDINGUNG:	BESCHREIBUNG
	Stellen Sie für agents der herkömmlichen Suche, auf denen Windows 7, Server 2012 und neuere Versionen ausgeführt werden, 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.

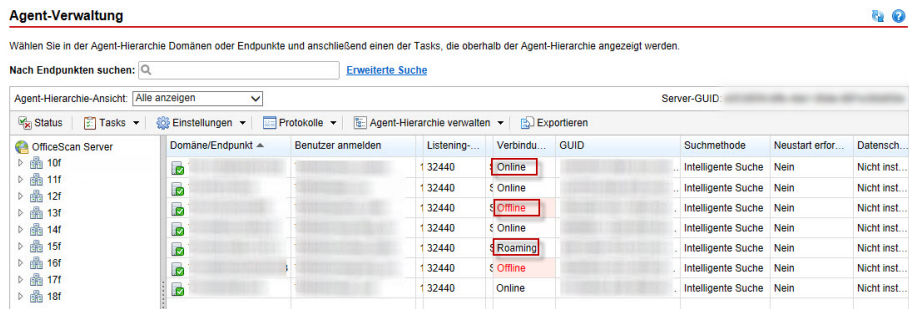


ABBILDUNG 14-2. Agent-Hierarchie mit der Anzeige des Verbindungsstatus des agents mit dem OfficeScan Server

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 13-40](#)*.

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 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 6-30*). 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 14-7. 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. Gehen Sie zum Abschnitt **Nicht erreichbares Netzwerk**.
3. Konfigurieren Sie die Server-Abfrage-Einstellungen.

Weitere Informationen zum Abfragen des Servers finden Sie unter [Serverabfrage auf Seite 14-49](#).

- 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 mit einem Dual-Stack-OfficeScan Server verbinden.

Agents mit einer IPv6-Adresse können sich mit einem reinen IPv6- oder mit einem Dual-Stack-OfficeScan Server verbinden.

Dual-Stack-agents können sich mit einem Dual-Stack-, einem reinen IPv4- bzw. einem reinen 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.

4. Konfigurieren Sie die Rückmeldungseinstellungen.

Weitere Informationen über die Rückmeldungsfunktion finden Sie unter [Rückmeldung auf Seite 14-48](#).

- 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 die 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**, wieviel Zeit vergehen muss, bis der OfficeScan Server einen agent als offline einstuft. Geben Sie einen Wert zwischen 1 und 129600 Minuten ein.

5. Klicken Sie auf **Speichern**.
-

OfficeScan Agent Proxy-Einstellungen

Konfigurieren Sie die OfficeScan Agents, sodass diese die Proxy-Einstellungen beim Verbindungsaufbau mit internen und externen Servern verwenden.

Interner Proxy für OfficeScan Agents

OfficeScan Agents können mit Hilfe der Einstellungen für interne Proxy-Server eine Verbindung zu den folgenden Servern im Netzwerk aufbauen:

- OfficeScan Server

Auf dem Servercomputer befinden sich der OfficeScan 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 beinhalten alle eigenständigen Smart Protection Server und den integrierten Smart Protection Server der anderen OfficeScan Server. OfficeScan Agents stellen eine Verbindung zu den Servern her, um Such- und Web-Reputation-Abfragen zu senden.

Einstellungen für internen Proxy konfigurieren

Prozedur

1. Navigieren Sie zu **Administration > Einstellungen > Proxy**.
2. Klicken Sie auf die Registerkarte **Interner Proxy**.
3. Navigieren Sie zum Abschnitt **Agent-Verbindung mit dem OfficeScan Server**.

- a. Wählen Sie **Die folgenden Proxy-Einstellungen für Agent-Verbindungen mit dem OfficeScan Server verwenden**.
- b. Geben Sie den Namen des Proxy-Servers oder eine IPv4-/IPv6-Adresse und eine Portnummer an.

**Hinweis**

Geben Sie den Host-Namen eines Dual-Stack-Proxy-Servers an, wenn Sie IPv4- und IPv6-agents haben. Der Grund hierfür ist, dass die internen Proxy-Einstellungen globale Einstellungen sind. Wenn Sie eine IPv4-Adresse angeben, können IPv6-agents keine Verbindung zum Proxy-Server herstellen. Dasselbe trifft für IPv4-agents zu.

- c. Wenn der Proxy-Server eine Authentifizierung voraussetzt, geben Sie den Benutzernamen und das Kennwort ein. Anschließend bestätigen Sie das Kennwort.
4. Navigieren Sie zum Abschnitt **Agent-Verbindung mit eigenständigen Smart Protection Servern**.
 - a. Wählen Sie **Die folgenden Proxy-Einstellungen für Agent-Verbindungen mit eigenständigen Smart Protection Servern verwenden**.
 - b. Geben Sie den Namen des Proxy-Servers oder eine IPv4-/IPv6-Adresse und eine Portnummer an.
 - c. Wenn der Proxy-Server eine Authentifizierung voraussetzt, geben Sie den Benutzernamen und das Kennwort ein. Anschließend bestätigen Sie das Kennwort.
 5. Klicken Sie auf **Speichern**.
-

Externer Proxy für OfficeScan Agents

Der OfficeScan Server und OfficeScan Agent können beim Verbindungsaufbau mit Servern, die von Trend Micro gehostet werden, Einstellungen für externe Proxy-Server verwenden. In diesem Thema werden die Einstellungen für externe Proxy-Server für agents behandelt. Informationen zu den externen Proxy-Einstellungen für den Server finden Sie unter [Proxy für Updates von OfficeScan Server auf Seite 6-21](#).

OfficeScan Agents verwenden die Proxy-Einstellungen, die in Internet Explorer oder Chrome konfiguriert wurden, um eine Verbindung zum Trend Micro Smart Protection Network herzustellen. Wenn eine Proxy-Server-Authentifizierung erforderlich ist, verwenden die Agents die Anmeldedaten für die Proxy-Server-Authentifizierung (Benutzer-ID und Kennwort).

Anmeldedaten für die Proxy-Server-Authentifizierung konfigurieren

Prozedur

1. Navigieren Sie zu **Administration > Einstellungen > Proxy**.
 2. Klicken Sie auf die Registerkarte **Externer Proxy**.
 3. Navigieren Sie zum Abschnitt **OfficeScan Agent-Verbindung mit Trend Micro Servern**.
 4. Geben Sie die Benutzer-ID und das Kennwort für die Authentifizierung am Proxy-Server ein. Die folgenden Proxy-Authentifizierungsprotokolle werden unterstützt:
 - Allgemeine Zugriffsauthentifizierung
 - Authentifizierung für den zusammenfassenden Zugriff
 - Integrierte Windows Authentifizierung
 5. Klicken Sie auf **Speichern**.
-

Proxy-Konfiguration – Berechtigungen für Agents

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.

Weitere Informationen finden Sie unter *Automatische Proxy-Einstellungen für OfficeScan Agent auf Seite 14-56*.



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.

Proxy-Konfiguration, 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. Navigieren Sie auf der Registerkarte **Berechtigungen** zum Abschnitt **Proxy-Einstellungen**.
5. Wählen Sie **Benutzern die Konfiguration der Proxy-Einstellungen erlauben** aus.
6. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie 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 alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser

Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

Automatische Proxy-Einstellungen für OfficeScan Agent

Die manuelle Konfiguration der Proxy-Einstellungen kann sich für viele Endbenutzer als schwierig gestalten. Verwenden Sie die automatischen Proxy-Einstellungen. Dadurch werden die korrekten Proxy-Einstellungen ohne Eingreifen des Benutzers angewendet.

Bei aktivierter Option haben die automatischen Proxy-Einstellungen Vorrang beim automatischen Update oder bei "Jetzt aktualisieren" auf dem OfficeScan Agents. Informationen über das automatische Update und die Funktion "Jetzt aktualisieren" finden Sie unter [OfficeScan Agent Update-Methoden auf Seite 6-40](#).

Kann die OfficeScan Agents mit den automatischen Proxy-Einstellungen keine Verbindung aufbauen, können entsprechend berechtigte agent-Benutzer die Einstellungen selbst konfigurieren. Andernfalls schlägt der Verbindungsaufbau über die automatischen Proxy-Einstellungen fehl.



Hinweis

Die Proxy-Authentifizierung wird nicht unterstützt.

Automatische Proxy-Einstellungen konfigurieren

Prozedur

1. Navigieren Sie zu **Agents > Globale Agent-Einstellungen**.
2. Gehen Sie zum Abschnitt **Proxy-Konfiguration**.
3. Wählen Sie **Einstellungen automatisch erkennen**, wenn Sie möchten, dass OfficeScan die vom Administrator konfigurierten Proxy-Einstellungen automatisch über DHCP oder DNS erkennt.
4. Wenn Sie möchten, dass OfficeScan das vom Netzwerkadministrator erstellte PAC-Skript (Proxy Auto-Configuration) verwendet, um den zuständigen Proxy-Server zu ermitteln:

- a. Wählen Sie **Automatisches Konfigurationsskript verwenden**.
 - b. Geben Sie die Adresse für das PAC-Skript ein.
5. Klicken Sie auf **Speichern**.
-

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 Endpunkttypen 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 14-60](#).
- **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 14-74](#)*.

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 14-61](#)*.
- **Komponenten:** Verwenden Sie diese Registerkarte, um zu überprüfen, ob die OfficeScan Agents über Update-Komponenten verfügen. Weitere Informationen finden Sie unter *[Komponenten auf Seite 14-62](#)*.
- **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 14-64](#)*.
- **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 14-67](#)*.



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.

Hinweise zum Bericht zur Einhaltung von Richtlinien

- Die Einhaltung der Sicherheitsrichtlinien fragt den Verbindungsstatus des OfficeScan Agents ab, bevor sie einen Bericht zur Einhaltung von Richtlinien erstellt. Der Bericht umfasst Online- und Offline-agents, jedoch keine Roaming-agents.
- Bei rollenbasierten Benutzerkonten:
 - Für jedes Webkonsolen-Benutzerkonto gelten völlig unterschiedliche Einstellungen für den Bericht zur Einhaltung von Richtlinien. Änderungen dieser Einstellungen haben keine Auswirkung auf die Einstellungen der anderen Benutzerkontos.
 - Der Umfang des Berichts ist abhängig von den Berechtigungen der agent-Domäne für dieses Benutzerkonto. Wenn beispielsweise das Dashboard eines Benutzerkontos die Berechtigung hat, die Domänen A und B zu verwalten, zeigen die Berichte 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 13-3*](#).

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.

Dienste	Komponenten	Einhaltung von Suchrichtlinien	Einstellungen
Endpunkte mit nicht kompatiblen Diensten			
<u>Dienste</u>	<u>Endpunkte</u>		
Virenschutz	0		
Anti-Spyware	0		
Firewall	0		
Web Reputation	0		
Verhaltensüberwachung/Gerätesteuerung	0		
Verdächtige Verbindung	0		
Endpunkte mit nicht kompatiblen Diensten	0		

ABBILDUNG 14-3. 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 einer Komponente auf dem agent neuer ist als die Version auf dem Server.

Die Einhaltung der Sicherheitsrichtlinien überprüft folgende Komponenten:

- Agent-Pattern der intelligenten Suche
- Viren-Pattern
- IntelliTrap Pattern
- IntelliTrap Ausnahme-Pattern
- Viren-Scan-Engine
- Spyware-Pattern
- Spyware-Aktivmonitor-Pattern
- Spyware-Scan-Engine
- Viren-Cleanup-Template
- Viren-Cleanup-Engine
- Pattern der allgemeinen Firewall
- Treiber für die allgemeine Firewall
- Treiber der Verhaltensüberwachung
- Kerndienst der Verhaltensüberwachung
- Pattern zur Konfiguration der Verhaltensüberwachung
- Pattern für digitale Signaturen
- Pattern der Richtliniendurchsetzung
- Erkennungs-Pattern der Verhaltensüberwachung
- Globale C&C-IP-Liste
- Pattern der Relevanzregel
- Early Boot Cleanup Driver
- Pattern zum Auslösen der Arbeitsspeichersuche
- Pattern der Arbeitsspeicherprüfung
- Pattern zur Erkennung von Browser-Schwachstellen
- Pattern der Skriptanalyse
- Programmversion

Ein nicht richtlinienkonformer agent wird im Bericht zur Einhaltung von Richtlinien mindestens zwei Mal gezählt.

Dienste	Komponenten	Einhaltung von Suchrichtlinien	Einstellungen
Endpunkte mit inkonsistenten Komponentenversionen			
<u>Komponenten</u>	<u>Endpunkte</u>		
Agent-Pattern der intelligenten Suche	0		
Viren-Pattern	0		
IntelliTrap Pattern	0		
IntelliTrap Ausnahme-Pattern	0		
Viren Scan Engine	0		
Spyware-Pattern	0		
Spyware-Aktivmonitor-Pattern	0		
Spyware-Scan-Engine	0		

ABBILDUNG 14-4. 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 zum Beispiel die Version des agent-Pattern der intelligenten Suche nicht mit der Version auf dem Server übereinstimmt, wird der agent in der Kategorie **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.

Dienste	Komponenten	Einhaltung von Suchrichtlinien	Einstellungen
Endpunkte mit veralteten Virensuchfunktionen			
<u>Suchkriterien</u>		<u>Endpunkte</u>	
Es wurde weder 'Jetzt durchsuchen' noch eine zeitgesteuerte Suche durchgeführt in den letzten 10 Tagen		0	
'Jetzt durchsuchen' oder zeitgesteuerte Suche überschritten um 5 Stunden		0	
Endpunkte mit veralteten Virensuchfunktionen		0	

ABBILDUNG 14-5. 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 verschieben, für die andere Einstellungen gelten, 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 zulässigen Spyware/Grayware
- Einstellungen für 'Prävention vor Datenverlust'
- Verdächtige Verbindung
- Liste der vertrauenswürdigen Programme

Ein nicht richtlinienkonformer agent wird im Bericht zur Einhaltung von Richtlinien mindestens zwei Mal gezählt.

Dienste	Komponenten	Einhaltung von Suchrichtlinien	Einstellungen
Endpunkte mit inkonsistenten Konfigurationseinstellungen			
<u>Einstellungen</u>		<u>Endpunkte</u>	^
Suchmethode		0	
Manuelle Suche – Einstellungen		0	
Echtzeitsuche – Einstellungen		0	
Zeitgesteuerte Suche – Einstellungen		0	
Jetzt durchsuchen – Einstellungen		0	
Berechtigungen und andere Einstellungen		0	
Zusätzliche Diensteinstellungen		0	
Web Reputation		0	v

ABBILDUNG 14-6. 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 der 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 Sicherheitsrichtlinien 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 14-60](#)*.

Einen bedarfsgesteuerten Bericht zur Einhaltung von Richtlinien 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. Bericht zur Einhaltung von Richtlinien für agent-Dienste anzeigen.

Weitere Informationen zu agent Diensten finden Sie unter *[Dienste auf Seite 14-61](#)*.

- 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 agents aus dem Ergebnis der Abfrage 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. Um die Liste der agents in einer Datei zu speichern, klicken Sie auf **Exportieren**.

5. Bericht zur Einhaltung von Richtlinien für agent-Komponenten anzeigen.

Weitere Informationen zu agent-Komponenten finden Sie unter *[Komponenten auf Seite 14-62](#)*.

- 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 agent über eine aktuellere Komponente als der OfficeScan Server verfügt, aktualisieren Sie den OfficeScan Server manuell.

- d. Wählen Sie agents aus dem Ergebnis der Abfrage aus.
- e. Klicken Sie auf **Jetzt aktualisieren**, um durchzusetzen, dass die agents die Komponenten herunterladen.

**Hinweis**

- Um sicherzustellen, dass die agents das agent-Programm upgraden können, deaktivieren Sie die Option **OfficeScan Agents können Komponenten aktualisieren, aber kein Upgrade des Agent-Programms durchführen oder Hotfixes verteilen** unter **Agents > Agent-Verwaltung > Einstellungen > Berechtigungen** oder andere Einstellungen.
- Starten Sie den Endpunkt neu und klicken Sie nicht auf **Jetzt aktualisieren**, um den Treiber für die allgemeine Firewall zu aktualisieren.

- f. Um die Liste der agents in einer Datei zu speichern, klicken Sie auf **Exportieren**.

6. Berichte zur Richtlinieneinhaltung für Suchvorgänge anzeigen.

Weitere Informationen zu Suchvorgängen finden Sie unter [Einhaltung von Suchrichtlinien auf Seite 14-64](#).

- 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 "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, welche die Suchkriterien erfüllen.
- e. Klicken Sie auf eine verlinkte Zahl, um alle in der agent-Hierarchie betroffenen agents anzuzeigen.

- f. Wählen Sie agents aus dem Ergebnis der Abfrage 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. Um die Liste der agents in einer Datei zu speichern, klicken Sie auf **Exportieren**.
7. Berichte zur Richtlinieneinhaltung für Einstellungen anzeigen.
- Weitere Informationen zu Einstellungen finden Sie unter [Einstellungen auf Seite 14-67](#).
- a. Klicken Sie auf die Registerkarte **Einstellungen**.
 - b. Überprüfen Sie unter **Computer mit inkonsistenten Konfigurationseinstellungen** die Anzahl der agents mit Einstellungen, die mit den Domänen-Einstellungen in der agent-Hierarchie nicht übereinstimmen.
 - c. Klicken Sie auf eine verlinkte Zahl, um alle in der agent-Hierarchie betroffenen agents anzuzeigen.
 - d. Wählen Sie agents aus dem Ergebnis der Abfrage aus.
 - e. Klicken Sie auf **Domäneneinstellungen übernehmen**.
 - f. Um die Liste der agents in einer Datei zu speichern, klicken Sie auf **Exportieren**.
-

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 14-60](#)*.

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 14-61](#)*
 - *[Komponenten auf Seite 14-62](#)*
 - *[Einhaltung von Suchrichtlinien auf Seite 14-64](#)*
 - *[Einstellungen auf Seite 14-67](#)*
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 13-36](#)*.

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 14-8. 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.
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 14-75*.

2. Überprüfen Sie ungeschützte Computer anhand der Suchabfrageergebnisse. Weitere Informationen finden Sie unter *Abfrageergebnisse anzeigen auf Seite 14-77*.
3. Installieren Sie den OfficeScan Agent. Weitere Informationen finden Sie unter *Installation bei Einhaltung von Sicherheitsrichtlinien auf Seite 5-66*.
4. Konfigurieren Sie zeitgesteuerte Abfragen. Weitere Informationen finden Sie unter *Bewertung zeitgesteuerter Abfragen konfigurieren auf Seite 14-79*.

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 2-38*.

Prozedur

1. Navigieren Sie zu **Bewertung > Nicht verwaltete Endpunkte**.
2. Klicken Sie im Abschnitt **Active Directory/IP-Adressenbereich** auf **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 14-9. 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 Verbindung 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, behandelt OfficeScan den Endpunkt sofort als nicht erreichbar. Die Standardportnummer lautet 135.

Wenn Sie diese Einstellung aktivieren, wird die Abfrage beschleunigt. Wenn die Verbindung zu Endpunkte nicht aufgebaut werden kann, muss der OfficeScan Server nicht mehr all die 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 14-24*.

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 **Einstellungen**.
 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 "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 15-12* 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 **Plugins > 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 **Plugins > 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 14-88](#).

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. Wechseln Sie auf dem OfficeScan Server-Computer zu *<Installationsordner des Servers>*PCCSRV\Private\vd.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 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 `vd.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**.

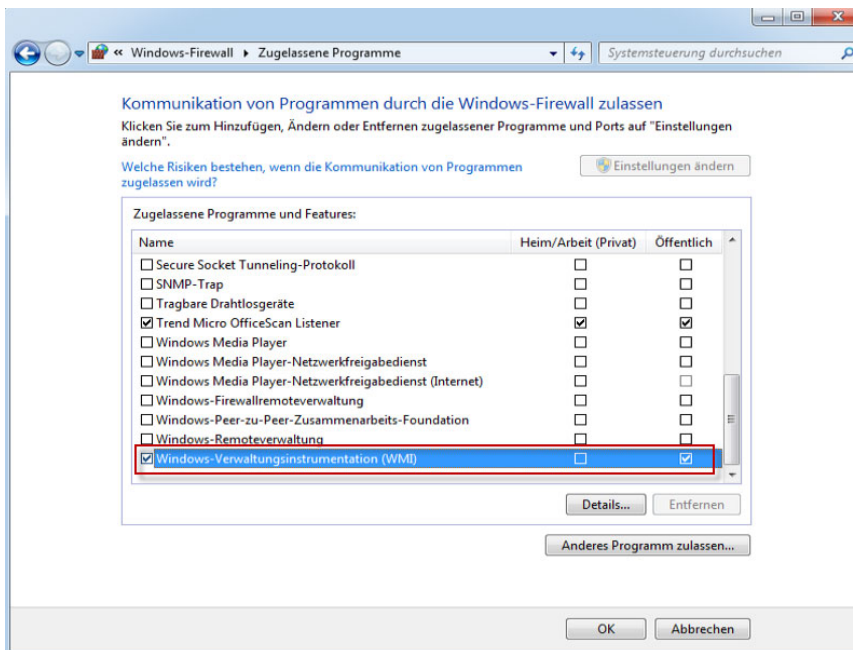


ABBILDUNG 14-7. Fenster "Windows-Firewall - Zugelassene Programme"

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](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 14-10. 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 **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 14-11. 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 14-12. Globale Agent-Einstellungen

EINSTELLUNG	NACHSCHLAGEWERKE
Sucheinstellungen	<i>Allgemeine Sucheinstellungen auf Seite 7-76</i>
Einstellungen für die zeitgesteuerte Suche	<i>Allgemeine Sucheinstellungen auf Seite 7-76</i>

EINSTELLUNG	NACHSCHLAGEWERKE
Bandbreiteneinstellungen des Viren-/Malware-Protokolls	<i>Allgemeine Sucheinstellungen auf Seite 7-76</i>
Firewall-Einstellungen	<i>Allgemeine Firewall-Einstellungen auf Seite 12-27</i>
Einstellungen der Verhaltensüberwachung	<i>Verhaltensüberwachung auf Seite 8-2</i>
Einstellungen für Certified Safe Software Service	<i>Certified Safe Software Service für Verhaltensüberwachung, Firewall und Virensuchen aktivieren auf Seite 7-87</i>
Verdächtige Verbindungseinstellungen	<i>Globale Einstellungen für die benutzerdefinierte IP-Liste konfigurieren auf Seite 11-14</i>
Updates	<i>ActiveUpdate Server als OfficeScan Agent-Update-Adresse auf Seite 6-40</i>
Reservierter Festplattenspeicher	<i>Reservierten Festplattenspeicher für OfficeScan Agents-Updates konfigurieren auf Seite 6-52</i>
Nicht erreichbares Netzwerk	<i>Nicht erreichbar Agents auf Seite 14-47</i>
Warneinstellungen	<i>OfficeScan Agent-Update-Benachrichtigungen konfigurieren auf Seite 6-54</i>
Sprachkonfiguration für Agent	<i>Sprachkonfiguration für OfficeScan Agent auf Seite 14-23</i>
Kommunikation zwischen Server und Agents	<i>Erweiterte Verschlüsselung der Kommunikation zwischen Server und Agent auf Seite 13-60</i>
Neustart des OfficeScan Diensts	<i>Neustart des OfficeScan Agent Dienstes auf Seite 14-12</i>
Proxy-Konfiguration	<i>Automatische Proxy-Einstellungen für OfficeScan Agent auf Seite 14-56</i>
Bevorzugte IP-Adresse	<i>Agent IP-Adressen auf Seite 5-9</i>

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 Stammsymbol () , 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 14-13. Agent-Berechtigungen

AGENT-BERECHTIGUNGEN	NACHSCHLAGEWERKE
Roaming-Berechtigungen	<i>OfficeScan AgentRoaming-Berechtigungen auf Seite 14-20</i>
Suchberechtigungen	<i>Berechtigungen für die Sucharten auf Seite 7-60</i>

AGENT-BERECHTIGUNGEN	NACHSCHLAGEWERKE
Berechtigungen für die zeitgesteuerte Suche	<i>Zeitgesteuerte Suchberechtigungen und andere Einstellungen auf Seite 7-62</i>
Firewall-Berechtigungen	<i>Firewall-Berechtigungen auf Seite 12-25</i>
Verhaltensüberwachungsberechtigungen	<i>Verhaltensüberwachungsberechtigungen auf Seite 8-13</i>
Liste der vertrauenswürdigen Programme	<i>Berechtigung für die Liste der vertrauenswürdigen Programme auf Seite 7-74</i>
Mail Scan Berechtigungen	<i>Mail-Scan-Berechtigungen und andere Einstellungen auf Seite 7-68</i>
Berechtigungen für die Proxy-Einstellungen	<i>Proxy-Konfiguration – Berechtigungen für Agents auf Seite 14-54</i>
Berechtigungen für Komponenten-Updates	<i>Update-Berechtigungen und weitere Einstellungen konfigurieren auf Seite 6-49</i>
Beenden und entsperren	<i>Die Berechtigung zum Beenden und Entsperren des Agents gewähren auf Seite 14-19</i>
Deinstallation	<i>Gewähren der Berechtigung zum Deinstallieren von OfficeScan Agent auf Seite 5-77</i>

5. Klicken Sie auf die Registerkarte **Weitere Einstellungen**, und konfigurieren Sie die folgenden Einstellungen:

TABELLE 14-14. Andere Agent-Einstellungen

EINSTELLUNG	NACHSCHLAGEWERKE
Update-Einstellungen	<i>Update-Berechtigungen und weitere Einstellungen konfigurieren auf Seite 6-49</i>
Web-Reputation-Einstellungen	<i>Benachrichtigungen über Internet-Bedrohungen für Agent-Benutzer auf Seite 11-17</i>

EINSTELLUNG	NACHSCHLAGEWERKE
Einstellungen der Verhaltensüberwachung	Verhaltensüberwachungsberechtigungen auf Seite 8-13
C&C-Kontakt – Alarmeinstellungen	C&C-Kontaktalarmbenachrichtigungen für Agent-Benutzer auf Seite 11-22
Warneinstellungen der zentralen Quarantänewiederherstellung	Zeigt nach der Wiederherstellung einer unter Quarantäne gestellten Datei eine Benachrichtigung auf dem Endpunkt an
Eigenschutz des OfficeScan Agents	OfficeScan Agent Eigenschutz auf Seite 14-13
Einstellungen für die zeitgesteuerte Suche	Berechtigungen für die zeitgesteuerte Suche gewähren und die Berechtigungsbenachrichtigung anzeigen auf Seite 7-63
Cache-Einstellungen für die Suche	Cache-Einstellungen für die Suche auf Seite 7-70
Einstellungen für die Suche in POP3-Mails	Mail Scan-Berechtigungen gewähren und POP3 Mail Scan aktivieren auf Seite 7-69
Einschränkung des Zugriffs auf OfficeScan Agent	Einschränkung des Zugriffs auf die OfficeScan Agent-Konsole auf Seite 14-18
Aufforderung zum Neustart	Benachrichtigungen bei Sicherheitsrisiken für OfficeScan Agent Benutzer auf Seite 7-94

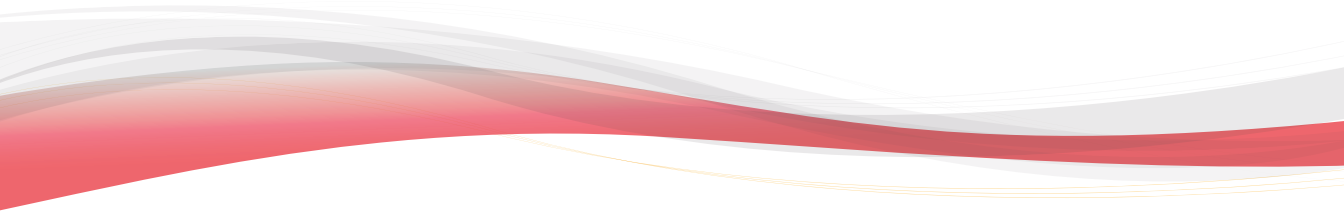
6. Wenn Sie Domäne(n) oder agent(s) in der agent-Hierarchie ausgewählt haben, klicken Sie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, können Sie aus folgenden Optionen auswählen:

- **Auf alle Agents anwenden:** Wendet die Einstellungen auf alle vorhandenen agents und auf alle neuen agent an, die einer vorhandenen/zukünftigen Domäne hinzugefügt werden. 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 zukünftigen Domänen hinzugefügt werden. Bei dieser

Option werden die Einstellungen nicht auf agents angewendet, die einer vorhandenen Domäne hinzugefügt werden.

Teil IV

Zusätzlichen Schutz bereitstellen



Kapitel 15

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 15-2*
- *Plug-in Manager Installation auf Seite 15-3*
- *Verwaltung nativer OfficeScan Funktionen auf Seite 15-4*
- *Plug-in-Programme verwalten auf Seite 15-4*
- *Plug-in Manager deinstallieren auf Seite 15-12*
- *Fehlersuche in Plug-in Manager auf Seite 15-12*

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.

Plug-in Manager liefert zwei verschiedene Lösungen:

- **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 Datenschutz**.

- **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. Beispiele für Plug-in-Programme sind **Intrusion Defense Firewall** und **Trend Micro Security (für Mac)**.

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 Endpunkte

Einige Plug-in-Programme (wie etwa Intrusion Defense Firewall) verfügen über Agents, die unter 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 Installationspaket von Plug-in Manager vom Trend Micro ActiveUpdate Server heruntergeladen und dann auf dem Endpunkt installiert, auf dem sich der OfficeScan Server befindet. In dieser Version ist das Installationspaket im Installationspaket des OfficeScan Servers enthalten.

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 Programme 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.

OPTION	BEZEICHNUNG
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**.

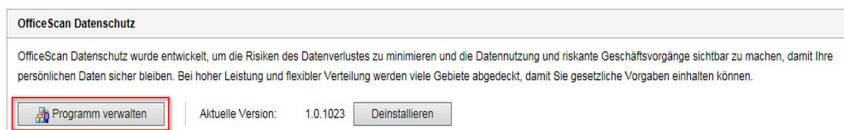


ABBILDUNG 15-1. Schaltfläche "Programm verwalten"

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.
-

Die Version des Apache Webserver wird nicht unterstützt.

Der Plug-in Manager verarbeitet einige der Webanfragen über die ISAPI (Internet Server Application Programming Interface). Diese ist nicht kompatibel mit den Apache-Webserver-Versionen 2.0.56 bis 2.0.59 und 2.2.3 bis 2.2.4.

Wenn auf Ihrem Apache-Webserver solche inkompatiblen Versionen laufen, können Sie sie durch die Version 2.2.25 ersetzen, das heißt mit der Version, die von OfficeScan und Plug-in Manager verwendet wird. Diese Version ist auch mit der ISAPI kompatibel.

Prozedur

1. Führen Sie ein Upgrade des OfficeScan Servers auf die aktuelle Version durch.

2. Sichern Sie die folgenden Dateien in den Ordner "Apache2" im <Installationsordner des Servers>:
 - httpd.conf
 - httpd.conf.tmbackup
 - httpd.default.conf
 3. Deinstallieren Sie die inkompatible Version von Apache Webserver im Fenster **Programme hinzufügen/entfernen**.
 4. Installieren Sie Apache Webserver 2.2.25.
 - a. Starten Sie apache.msi aus <Installationsordner des Servers>\Admin\Utility\Apache.
 - b. Geben Sie im Fenster Serverinformationen die erforderlichen Daten ein.
 - c. Ändern Sie im Fenster Zielordner den Zielordner, indem Sie auf **Ändern** klicken und dann zum Ordner <Installationsordner des Servers> navigieren.
 - d. Schließen Sie die Installation ab.
 5. Kopieren Sie die Sicherungsdateien zurück in den Apache2 Ordner.
 6. Starten Sie den Dienst für den Apache Webserver neu.
-

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 ofscan.ini.

- a. Öffnen Sie mit einem Texteditor die Datei ofscan.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 15-1. Plug-in Manager Fehlercodes

FEHLE RCODE	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.
002	Es ist ein Systemfehler aufgetreten. Das Plug-in Manager Update-Modul kann den Registrierungsschlüssel <code>SOFTWARE\TrendMicro\OfficeScan\service\AoS</code> nicht öffnen, da er möglicherweise gelöscht wurde. Führen Sie folgende Schritte durch: 1. Öffnen Sie den Registrierungseditor, und navigieren Sie zu <code>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_ComList_Version</code>. 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.

FEHLE RCODE	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 <code>\PCCSRV\Web\Service\AU_Data\AU_Log</code>. Führen Sie folgende Schritte durch: 1. Öffnen Sie den Registrierungseditor, und navigieren Sie zu <code>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version</code>. Setzen Sie den Wert auf 1.0.1000 zurück. 2. Löschen Sie den Registrierungsschlüssel des Plug-in-Programms unter <code>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_XXX</code>. 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.

FEHLE RCODE	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 Fehler codes	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 16

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 16-2*
- *Case Diagnostic Tool auf Seite 16-2*
- *Trend Micro Performance Tuning Tool auf Seite 16-2*
- *OfficeScan Serverprotokolle auf Seite 16-3*
- *OfficeScan Agent Protokolle auf Seite 16-15*

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 16-2*.
- Sammeln Sie die folgenden Protokolle:
 - Alle Dateien im Ordner <*Installationsordner des Servers*>\PCCSRV\Private\AuthorStore.
 - *OfficeScan Serverprotokolle auf Seite 16-3*

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 aufcg.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 aufg.ini.
 2. Starten Sie den OfficeScan Master Service neu.
-

Apache Server Protokolle

Dateinamen:

- install.log
- error.log
- access.log

Speicherort: *<Installationsordner des Servers>*\PCCSRV\Apache2

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\AgentPackager 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 16-3*

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

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.
-

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.

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\
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 16-3](#).

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: jjjmmmtt.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 aufg.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 aufcg.ini löschen und den OfficeScan Agent neu laden.

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>*\

OfficeScan Firewall-Protokolle

Debug-Protokollierung für den allgemeinen Firewall-Treiber auf Computern mit Windows Vista/Server 2008/7/Server 2012/8/8.1 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\tmlcfw\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

1. Bearbeiten Sie TmProxy.ini im Ordner *<Installationsordner des Agents>* wie folgt:


```
[ServiceSession]  
  
Enable=1  
  
LogFolder=C:\temp
```
 2. Laden Sie den OfficeScan Agent neu.
 3. Überprüfen Sie die Datei ddmmyyyy_NSC_TmProxy.log unter C:\temp.
-

Debug-Protokollierung des Web-Reputation-Moduls und POP3 Mail Scan deaktivieren

Prozedur

1. Öffnen Sie die Datei TmProxy.ini, und ändern Sie den Wert "Enable" von 1 in 0.

2. 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)
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 17

Technischer Support

In diesem Kapitel wird beschrieben, wie Sie online nach Lösungen suchen, das Support-Portal verwenden und Kontakt zu Trend Micro aufnehmen.

Es werden folgende Themen behandelt:

- *Ressourcen zur Fehlerbehebung auf Seite 17-2*
- *Kontaktaufnahme mit Trend Micro auf Seite 17-4*
- *Verdächtige Inhalte an Trend Micro senden auf Seite 17-5*
- *Sonstige Ressourcen auf Seite 17-6*

Ressourcen zur Fehlerbehebung

Vor der Kontaktaufnahme mit dem technischen Support sollten Sie die folgenden Online-Ressourcen zu Trend Micro heranziehen.

Trend Micro-Community

Um Hilfe anzufordern, Erfahrungen auszutauschen, Fragen zu stellen und Sicherheitsprobleme mit anderen Benutzern, Fans und Sicherheitsexperten zu diskutieren, navigieren Sie zu:

<http://community.trendmicro.com/>

Support-Portal verwenden

Das Trend Micro Support-Portal ist täglich rund um die Uhr online verfügbar und enthält die aktuellsten Informationen zu häufig auftretenden und ungewöhnlichen Problemen.

Prozedur

1. Navigieren Sie zu <http://esupport.trendmicro.com>.
2. Wählen Sie ein Produkt oder einen Dienst aus, oder klicken Sie auf eine Schaltfläche, um weitere Produkte bzw. Dienste zu suchen.
3. Verwenden Sie das Feld **Search Support** (Support durchsuchen), um nach verfügbaren Lösungen zu suchen.
4. Falls keine Lösung gefunden wird, klicken Sie auf **Contact Support** (Support kontaktieren) oder reichen Sie eine Support-Anfrage auf der folgenden Seite ein:

<http://esupport.trendmicro.com/srf/SRFMain.aspx>

Ein Support-Mitarbeiter von Trend Micro analysiert Ihre Anfrage und antwortet innerhalb von maximal 24 Stunden.

Community für Sicherheitsinformationen

Bei den Internet-Sicherheitsexperten von Trend Micro handelt es sich um ein Eliteteam für Sicherheitsinformationen, das sich auf die Erkennung und Analyse von Bedrohungen, die Sicherheit bei der Cloud- und Virtualisierungstechnologie sowie die Datenverschlüsselung spezialisiert hat.

Auf <http://www.trendmicro.com/us/security-intelligence/index.html> finden Sie weitere Informationen zu folgenden Themen:

- Trend Micro-Blogs, Twitter, Facebook, YouTube und sonstige soziale Medien
- Berichte zu Internet-Bedrohungen, Forschungsarbeiten und Artikel
- Lösungen, Podcasts und Newsletter von Sicherheitsexperten weltweit
- Kostenlose Tools, Apps und Widgets

Bedrohungszyklopädie

Der Großteil der Malware besteht heutzutage aus "kombinierten Bedrohungen", also einer Kombination aus mindestens zwei Technologien zur Umgehung der Sicherheitsprotokolle des Computers. Trend Micro bekämpft diese komplexe Malware mit Produkten, die eine benutzerdefinierte Verteidigungsstrategie verfolgen. Die Bedrohungszyklopädie 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

In Deutschland erreichen Sie unsere Trend Micro Vertriebspartner telefonisch oder per E-Mail:

Adresse	Trend Micro, Incorporated Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland
Telefon	Tel.: +49 (0) 811 88990-700
Website	http://www.trendmicro.com
E-Mail-Adresse	sales@trendmicro.de

- Weltweite Support-Büros:
<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 zusätzliche Hardware, die an den Endpunkt angeschlossen ist
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Betriebssystem- und Service Pack-Version

- Client-Version des Endpunkts
- 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.

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.

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/1055473.aspx>

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.

TrendEdge

Hier finden Sie Informationen zu nicht unterstützten, innovativen Techniken, Tools und bewährten Methoden für Produkte und Services von Trend Micro. Die TrendEdge Datenbank enthält zahlreiche Dokumente zu vielen Themen für Partner und Mitarbeiter von Trend Micro sowie andere Interessierte.

Die neuesten Informationen in der TrendEdge Datenbank finden Sie unter:

<http://trendedge.trendmicro.com/>

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://www.trendmicro.com/download/emca/?lng=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.

TrendLabs

Bei TrendLabsSM handelt es sich um ein globales Netzwerk aus Forschungs-, Entwicklungs- und Wartungszentren, die täglich rund um die Uhr nach Sicherheitsbedrohungen suchen, Angriffe verhindern und schnell und problemlos Lösungen bereitstellen. TrendLabs dient als Backbone der Trend Micro Service-Infrastruktur und beschäftigt mehrere hundert Mitarbeiter und zertifizierte Support-Experten, die sich um die vielfältigen Anfragen zu Produkten und technischem Support kümmern.

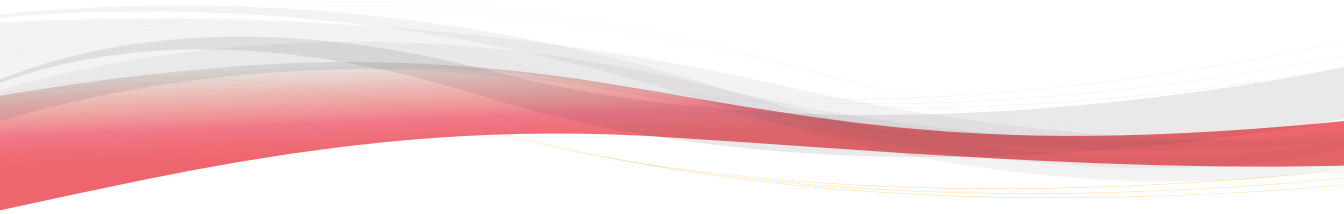
TrendLabs überwacht die weltweite Bedrohungslage, um effektive Sicherheitsmaßnahmen anzubieten, mit denen Angriffe erkannt, vermieden und beseitigt werden können. Die Kunden profitieren von diesen täglichen Bemühungen in Form von häufigen Viren-Pattern-Updates und Erweiterungen der Scan Engine.

Weitere Informationen zu TrendLabs finden Sie unter:

<http://www.trendmicro.de/newsroom/faces/index.html>

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 oder Windows Server 2012 installiert sein. Er darf nicht unter Windows Server 2003 installiert sein, da dieses Betriebssystem die IPv6-Adressierung nur teilweise unterstützt.
- Der Server muss einen IIS Webserver verwenden. Der Apache Webserver unterstützt keine IPv6-Adressierung.
- 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 Vista
- Windows 8
- Windows 8.1
- Windows Server 2012

Er darf nicht auf Windows Server 2003 und Windows XP installiert sein, da diese Betriebssysteme die IPv6-Adressierung nur teilweise unterstützen.

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
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.
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 Beispiel 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.

- 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 am Server verwenden, können über **Agents > Globale Agent-Einstellungen > 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

Weitere Informationen über die agent 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.

- 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

Die folgende Tabelle enthält eine Liste der IP-Adressen des OfficeScan Servers und der OfficeScan Agents, die auf der Control Manager-Konsole angezeigt werden.

TABELLE A-3. OfficeScan Die IP-Adressen des Servers und der OfficeScan Agent, die auf der Control Manager-Konsole angezeigt werden

OFFICESCAN	CONTROL MANAGER VERSION	
	6.0 ODER HÖHER	5.5 SP1
Dual-Stack-Server	IPv4 und IPv6	IPv4 und IPv6
Reine IPv4-Server	IPv4	IPv4
Reine IPv6-Server	IPv6	IPv6
Dual-stack OfficeScan Agent	Die IP-Adresse, mit der sich der OfficeScan Agent am OfficeScan Server registriert hat	Die IP-Adresse, mit der sich der OfficeScan Agent am OfficeScan Server registriert hat
Reines IPv4 OfficeScan Agent	IPv4	IPv4
Reines IPv6 OfficeScan Agent	IPv6	IPv6

Anhang B

Unterstützung für Windows Server Core 2008/2012

Im Anhang wird die OfficeScan-Unterstützung für Windows Server Core 2008/2012 behandelt.

Unterstützung für Windows Server Core 2008/2012

Windows Server Core 2008/2012 ist eine "minimale" Installation von Windows Server 2008/2012. In einer Server Core Installation:

- Sind viele Optionen von Windows Server 2008/2012 nicht verfügbar.
- 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.

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 über keinen Internet Explorer verfügt.
- 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 5-20](#)*.
- Anmeldeskript-Setup

- Agent Packager

OfficeScan Agent mit dem Anmeldeskript-Setup installieren

Prozedur

1. Öffnen Sie ein Eingabeaufforderungsfenster.
2. Ordnen Sie den Speicherort der Datei AutoPcc.exe zu, indem Sie den folgenden Befehl eingeben:

```
net use <zugeordneter Laufwerksbuchstabe> \\<Host-Name oder  
IP-Adresse des OfficeScan Servers>\ofcscan
```

Beispiel:

```
net use P: \\10.1.1.1\ofcscan
```

Eine Meldung wird angezeigt, die Sie darüber informiert, ob der Speicherort von AutoPcc.exe erfolgreich zugeordnet wurde.

3. Ändern Sie den Speicherort von AutoPcc.exe, indem Sie den zugeordneten Laufwerksbuchstaben und einen Doppelpunkt eingeben. Beispiel:

```
P:
```

4. Geben Sie zum Starten der Installation Folgendes ein:

```
AutoPcc.exe
```

Im folgenden Bild werden die Befehle und Ergebnisse in der Eingabeaufforderung angezeigt.

```
C:\Windows>net use P: \\172.16.9.24\ofcscan
Der Befehl wurde erfolgreich ausgeführt.
```

```
C:\Windows>P:
```

```
P:\>AutoPcc.exe
AutoPcc.exe
```

```
-----
Trend Micro OfficeScan
Automatisches Setup-Programm V11.0
Copyright Trend Micro, Inc.
1998-2014
-----
```

```
P:\>_
```

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 5-27](#)*.

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 verfügbaren OfficeScan Agent-Funktionen werden auch unter Server Core unterstützt. Der Roaming-Modus wird als einzige Funktion nicht unterstützt.

Eine Liste der unter Windows Server 2008/2012 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 über keinen Browser verfügen, kann diese Hilfe dort nicht aufgerufen werden. Um die Hilfe anzuzeigen, muss der Benutzer einen Browser installieren.

Windows Server Core Befehle

Führen Sie OfficeScan Agent-Tasks mit Befehlen über die Befehlszeilenschnittstelle aus.

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 Verzeichnispfad>	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

BEFEHL	AKTION
<code>pccntmon -r</code>	Öffnet den Echtzeitmonitor
<code>pccntmon -v</code>	Führt die agent-Komponenten und deren Versionen auf.
<code>pccntmon -u</code>	Aktualisiert die OfficeScan Agent-Komponenten.
<code>pccntmon -n</code> <code><unload_password></code>	Entlädt den OfficeScan Agent. Geben Sie den folgenden Befehl ein, um den OfficeScan Agent erneut zu laden: <code>pccntmon</code>
<code>pccntmon -m</code> <code><uninstall_password></code>	Deinstalliert den OfficeScan Agent.

BEFEHL	AKTION
<code>pccntmon -c</code>	Zeigt die folgenden Informationen in der Befehlszeile: • Suchmethode • Intelligente Suche • Herkömmliche Suche • Pattern-Status • Aktualisiert • Nicht aktuell • Echtzeitsuchdienst • Funktioniert • Deaktiviert oder nicht funktionsfähig • Agent-Verbindungsstatus • Online • Roaming • Offline • Web-Reputation-Dienste • Verfügbar • Die Verbindung wird wiederhergestellt • File-Reputation-Dienste • Verfügbar • Die Verbindung wird wiederhergestellt
<code>pccntmon -h</code>	Zeigt alle verfügbaren Befehle

Anhang C

Unterstützung für Windows 8/8.1 und Windows Server 2012

In diesem Anhang wird die OfficeScan Unterstützung für Windows 8/8.1 und Windows Server 2012 behandelt.

Informationen zu Windows 8/8.1 und Windows Server 2012

Windows 8/8.1 und Windows Server 2012 stellen Benutzern zwei verschiedene Betriebsmodi bereit: den Desktop-Modus und den Windows-Benutzeroberflächenmodus. 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
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 ob 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 im Windows-Benutzeroberflächenmodus

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.
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

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)
-

Internet Explorer 10/11

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.

Internet Explorer 10 oder höher für den Windows-Benutzeroberflächenmodus bietet eine Plug-In-freie Browserumgebung. Plug-In-Programme für das Webbrowser 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-3. 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
Netzwerkcommunication, 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.

OfficeScan Funktionsunterstützung in Internet Explorer 10/11

Der Modus, in dem Benutzer Windows 8/8.1 oder Windows Server 2012 verwenden, hat Einfluss auf die verwendete Internet Explorer 10-Version oder höher 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-4. OfficeScan Funktionsunterstützung im Benutzeroberflächenmodus

FUNKTION	DESKTOP-MODUS	WINDOWS-BENUTZEROBERFLÄCHENMODUS
Webserverkonsole	Vollständige Unterstützung	Nicht unterstützt
Web reputation	Vollständige Unterstützung	Eingeschränkte Unterstützung • HTTPS-Suchfunktion deaktiviert
Firewall	Vollständige Unterstützung	Eingeschränkte Unterstützung • Anwendungsfilter deaktiviert

Anhang D

OfficeScan Rollback

In diesem Anhang werden der OfficeScan Server und die Unterstützung des OfficeScan Agent-Rollbacks behandelt.

Rollback des OfficeScan Servers und der OfficeScan Agents

Der Vorgang des OfficeScan Rollbacks umfasst das Rollback von OfficeScan Agents und anschließend das Rollback des OfficeScan Servers.



Wichtig

- Administratoren können das Rollback von OfficeScan Server und OfficeScan Agents nur durchführen, indem sie folgendermaßen vorgehen, wenn die Administratoren den Server während des Installationsvorgangs sichern möchten. Wenn die Server-Sicherungsdateien nicht verfügbar sind, finden Sie im *Installations- und Upgrade-Handbuch* für OfficeScan 11.0 weitere Informationen zum manuellen Rollback.
 - Diese Version von OfficeScan unterstützt Rollbacks nur für die folgenden OfficeScan Versionen:
 - OfficeScan 11.0
-

Rollback der OfficeScan Agents

Prozedur

1. Stellen Sie sicher, dass OfficeScan Agents ein Upgrade des agent-Programms durchführen können.
 - a. Navigieren Sie auf der OfficeScan 11.0 SP1 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. Aktivieren Sie die Option **Agents können Komponenten aktualisieren, aber kein Upgrade des OfficeScan Agent-Programms durchführen oder Hotfixes verteilen**.

2. Navigieren Sie auf der OfficeScan 11.0 SP1 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 eine manuelle Aktualisierung auf den Clients einleiten. Weitere Informationen finden Sie unter *OfficeScan Agents manuell aktualisieren auf Seite 6-48*.

9. Fordern Sie den Benutzer nach der Installation der vorherigen Version des OfficeScan Agents auf, den Computer 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.

Rollback des OfficeScan Servers durchführen

Für den Vorgang des Rollbacks für OfficeScan Server müssen die Administratoren Windows Dienste manuell beenden, die Systemregistrierung aktualisieren und OfficeScan Server-Dateien im OfficeScan Installationsverzeichnis ersetzen.

Prozedur

1. 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
 - Apache 2 (bei Verwendung des Apache Webserver)
 - World Wide Web Publishing Dienst (bei Verwendung des IIS-Webserver)
2. Kopieren und ersetzen Sie alle Dateien und Verzeichnisse aus dem Verzeichnis *<Installationsordner des Servers>* \PCCSRV\Backup\ServicePack1_<Buildnummer> \ in das Verzeichnis *<Installationsordner des Servers>* \PCCSRV\.

3. Klicken Sie auf **Start**, geben Sie **regedit** ein und drücken Sie die Eingabetaste.

Das Fenster **Registrierungseditor** wird angezeigt.

4. 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

5. Wechseln Sie zu **Datei > Importieren....**

6. Wählen Sie die Datei RegBak_ServicePack1_<Buildnummer>.reg im Verzeichnis <Installationsordner des Servers>\PCCSRV\Backup\ aus.

7. Klicken Sie auf **Ja**, um alle vorherigen Versionsschlüssel von OfficeScan wiederherzustellen.

8. Öffnen Sie einen Befehlszeilen-Editor (klicken Sie auf **Start** und geben Sie **cmd.exe** ein) und geben Sie die folgenden Befehle ein, um den Leistungszähler des Local Web Classification Servers zurückzusetzen:

```
cd <Installationsordner des Servers>\PCCSRV\IWCS  
regsvr32.exe /u /s perflWCSPerfMonMgr.dll  
regsvr32.exe /s perflWCSPerfMonMgr.dll
```

9. 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 Webserver)
 - World Wide Web Publishing Dienst (bei Verwendung des IIS-Webserver)
10. 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>.

Der OfficeScan Server wurde auf die vorher installierte Version zurückgesetzt.



Tipp

Administratoren können einen erfolgreichen Rollback bestätigen, indem sie die OfficeScan Versionsnummer im **Info**-Fenster (**Hilfe** > **Info**) überprüfen.

11. Nachdem Sie das erfolgreiche Rollback von OfficeScan bestätigt haben, löschen Sie folgende Elemente im Verzeichnis <Installationsordner des Servers>\PCCSRV\Backup\:
- Ordner: ServicePack1_<SP1_Buildnummer>
 - Datei: RegBak_ServicePack1_<SP1_Buildnummer>.reg
-

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 Systemen 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 Domännennamen, 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 Netzwerkkumgebungen 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.

SOCKS 4

SOCKS 4 ist ein TCP-Protokoll, mit dem Proxy-Server eine Verbindung zwischen agents im internen Netzwerk oder LAN und Endpunkte oder Servern außerhalb des LAN herstellen. Das SOCKS-4-Protokoll sendet Verbindungsanfragen, richtet Proxy-Verbindungen ein und leitet Daten an die Anwendungsschicht des OSI-Schichtenmodells weiter.

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

PORTNUMMER	TROJANER	PORTNUMMER	TROJANISCHES PFERD
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

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 ofscan.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 kann folgende Dateien nicht 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: Die Viren-Cleanup-Engine und die Viren-Cleanup-Template entfernen Trojaner.
Mit Würmern infizierte Dateien	Ein Wurm ist ein eigenständiges Programm (oder eine Gruppe von Programmen), das funktionsfähige Kopien von sich selbst oder seinen Segmenten an andere 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.

NICHT ZU SÄUBERnde DATEI	ERKLÄRUNG UND LÖSUNG
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.
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: <pre>cd \ cd recycled del *.* /S</pre> 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: <pre>cd \</pre>

NICHT ZU SÄUBERENDE DATEI	ERKLÄRUNG UND LÖSUNG
	<pre>cd recycled</pre> <pre>del *.* /S</pre> Mit dem letzten Befehl werden alle Dateien im Papierkorb gelöscht.
Infizierte Dateien im Windows Ordner "Temp" oder im Internet Explorer-Ordner "Temporary Internet Files"	Dateien in diesen Ordnern können möglicherweise nicht gesäubert werden, da sie vom Endpunkt verwendet werden. Möglicherweise handelt es sich bei den Dateien, die gesäubert werden sollen, um temporäre Dateien, die für den Betrieb von Windows benötigt werden. Lösung 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: <pre>cd temp</pre> <pre>attrib -h</pre> <pre>del *.* /S</pre> Mit dem letzten Befehl werden alle Dateien im Windows Temp-Ordner gelöscht. 4. Wenn sich die infizierte Datei im temporären Ordner von Internet Explorer befindet: a. Öffnen Sie die Eingabeaufforderung, und navigieren Sie zum temporären Internet Explorer-Ordner

NICHT ZU SÄUBERNDE DATEI	ERKLÄRUNG UND LÖSUNG
	(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: <pre>cd tempor~1</pre> <pre>attrib -h</pre> <pre>del *.* /S</pre> 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:<pre>cd temp</pre><pre>attrib -h</pre><pre>del *.* /S</pre> 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:

NICHT ZU SÄUBERNDEN DATEIEN	ERKLÄRUNG UND LÖSUNG
	a. Öffnen Sie die Eingabeaufforderung, und navigieren Sie zum temporären Internet Explorer-Ordner (standardmäßig bei Endpunkten 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: <pre>cd tempor~1</pre> <pre>attrib -h</pre> <pre>del *.* /S</pre> 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 Komprimierungstool 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: OfficeScan entfernt Trojaner mit Hilfe der Viren-Cleanup-Engine und des Viren-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 OfficeScan die Datei säubern kann.

Kennwortgeschützte Dateien

Umfasst kennwortgeschützte komprimierte Dateien oder kennwortgeschützte Microsoft Office Dateien.

Lösung: Heben Sie den Kennwortschutz auf, damit OfficeScan diese Dateien säubern kann.

Sicherungsdateien

Bei Dateien mit den Erweiterungen RB0~RB9 handelt es sich um Sicherungskopien infizierter Dateien. OfficeScan erstellt eine Sicherungsdatei der infizierten Datei für den Fall, dass der Virus/die Malware die Datei beim Säubern beschädigt.

Lösung: Wenn die infizierte Datei von OfficeScan gesäubert werden konnte, muss die Sicherungskopie nicht aufbewahrt werden. Wenn der Endpunkt fehlerfrei funktioniert, können Sie die Kopie löschen.

Stichwortverzeichnis

A

ActiveAction, 7-40

Active Directory, 2-38–2-41, 2-56, 2-61, 5-14, 5-32

Adressbereich und Abfrage, 14-75

Agent-Gruppierung, 2-56

Anmeldedaten, 2-40

Ausgelagerte Serververwaltung, 2-39

Benutzerdefinierte Agent-Gruppen,
2-39

integration, 2-38

Rollenbasierte Administration, 2-39

Struktur duplizieren, 2-61

Synchronisierung, 2-41

ActiveSync, 10-40

Agent deinstallieren, 5-75

Agent-Disk-Image, 5-14, 5-39

Agent-Gruppierung, 2-56–2-58, 2-60, 2-61,
2-63–2-65

Active Directory, 2-56, 2-60

Agents verschieben, 2-65

Aufgaben, 2-63

Automatisch, 2-57, 2-58

Benutzerdefinierte Gruppen, 2-57

DNS, 2-56

Domäne oder Agent löschen, 2-64

Hinzufügen einer Domäne, 2-63

IP-Adressen, 2-61

Manuell, 2-56, 2-57

Methoden, 2-56

NetBIOS, 2-56

Umbenennen einer Domäne, 2-65

Agent-Hierarchie, 2-42, 2-44–2-47, 2-51–2-54

Allgemeine Aufgaben, 2-44

Ansichten, 2-45

Erweiterte Suche, 2-45, 2-46

Filter, 2-45

Info über, 2-42

Spezifische Aufgaben, 2-47, 2-51–2-54

Agent-Verwaltung, 2-47

Ausbruchsprävention, 2-51

Manuelle Komponenten-Updates,
2-52

Rollback der Komponenten-
Updates durchführen, 2-53

Sicherheitsrisiko-Protokolle, 2-54

Agent-Installation, 5-2, 5-24

Agent Packager, 5-27

Anmeldeskript-Setup, 5-24

Browserbasiert, 5-19

Nach der Installation, 5-72

Per Agent-Disk-Image, 5-39

Systemvoraussetzungen, 5-2

über die Web-Installationsseite, 5-16

über die Webkonsole, 5-20

Verwenden der Sicherheitsrichtlinien,
5-66

Vulnerability Scanner verwenden, 5-40

Agent-Konsole

Zugriffsbeschränkung, 14-18

agent mover, 14-24

Agent Packager, 5-14, 5-27, 5-30, 5-32, 5-34

Einstellungen, 5-29

Verteilung, 5-27

Agent-Pattern der intelligenten Suche, 4-8, 6-4

Agent-Protokolle

Agent-Update-Protokolle, 16-18

Agent-Verbindungsprotokolle, 16-18

- Datenschutz-Debug-Protokolle, 10-67, 16-23
- Debug-Protokolle, 16-15
- Debug-Protokolle der Ausbruchsprävention, 16-19
- Debug-Protokolle der OfficeScan Firewall, 16-20
- Debug-Protokolle der Web Reputation, 16-22
- Erstinstallations-Protokolle, 16-16
- Mail Scan Protokolle, 16-18
- Protokolle für Damage Cleanup Services, 16-17
- TDI-Debug-Protokolle, 16-24
- Upgrade-/Hotfix-Protokolle, 16-17
- agents, 2-56, 2-64, 2-65, 4-33, 5-2
 - Funktionen, 5-3
 - Gruppierung, 2-56
 - installation, 5-2
 - löschen, 2-64
 - Proxy-Einstellungen, 4-33
 - Standorte, 4-33
 - Verbindung, 4-33
 - verschieben, 2-65
- Agent-Update
 - Automatisch, 6-41
 - Benutzerdefinierte Adresse, 6-35
 - Berechtigungen, 6-49
 - Ereignisbedingt, 6-42
 - Manuell, 6-47
 - Standard-Adresse, 6-34
 - 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, 8-6
- Aktionen
 - Prävention vor Datenverlust, 10-41
- Angaben zum Webserver, 13-54
- Anmeldeskript-Setup, 5-12, 5-13, 5-24, 5-25
- Anwendungsfiler, 12-3
- ARP-Konflikt, 12-5
- Aufgaben vor der Installation, 5-18, 5-21, 5-66
- Ausbruchspräventionsrichtlinie
 - Ausführbare komprimierte Dateien, 7-125
 - Gegenseitige Ausschlüsse, 7-124
 - Mutex-Behandlung, 7-124
 - Ports sperren, 7-121
 - Schreibzugriff verweigern, 7-123
 - Zugriff auf Freigabeordner einschränken/verweigern, 7-120
 - Zugriff auf komprimierte Dateien verweigern, 7-125
- Ausbruchskriterien, 7-114, 11-23, 12-33
- Ausbruchsprävention, 2-20
 - Deaktivieren, 7-126
 - Richtlinien, 7-119
- Ausdrücke, 10-6
 - benutzerdefiniert, 10-7, 10-11
 - Kriterien, 10-8, 10-9
 - vordefiniert, 10-6, 10-7
- Ausgelagerte Serververwaltung, 2-39, 14-74
 - Abfrageergebnisse, 14-77
 - Protokolle, 16-9
 - Zeitgesteuerte Abfrage, 14-79
- Ausschlussliste, 8-7
 - Verhaltensüberwachung, 8-7
- Automatische Agent-Gruppierung, 2-57, 2-58
- AutoPcc.exe, 5-12, 5-13, 5-24, 5-25

B

Bedingungsanweisungen, 10-23

Begriffe, xiv

Benachrichtigungen

Agent-Update, 6-54

C&C-Callback-Erkennungen, 11-22

Erkennung von Internet-Bedrohung,
11-17

Firewall-Verstöße, 12-30

Für Administratoren, 10-57, 13-36

für Agent-Benutzer, 7-94, 10-60

Gerätesteuerung, 9-18

Neustart des Endpunkts, 6-55

Spyware-/Grayware-Fund, 7-53

Veraltetes Viren-Pattern, 6-55

Viren-/Malware-Fund, 7-46

Virenausbrüche, 7-114, 11-23, 12-33

Benutzerdefinierte Agent-Gruppen, 2-39, 2-57

Benutzerdefinierte Ausdrücke, 10-7–10-9, 10-11

Importieren, 10-11

Kriterien, 10-8, 10-9

Benutzerdefinierte Schlüsselwörter, 10-17

Importieren, 10-21

Kriterien, 10-17–10-19

Benutzerdefinierte Vorlagen, 10-23

erstellen, 10-24

Importieren, 10-26

Benutzerkonten, 2-5

dashboard, 2-5

Benutzerrolle

administrator, 13-10

Gastbenutzer, 13-10

Trend Hauptbenutzer, 13-10

Berechtigungen

Beenden, Berechtigung, 14-19

Berechtigungen für die zeitgesteuerte
Suche, 7-62

Erweitert, 9-12

Firewall-Berechtigungen, 12-25, 12-27

Mail Scan Berechtigungen, 7-68

Nicht-Speichergeräte, 9-11

Programmpfad und -name, 9-9

Proxy-Konfiguration, Berechtigungen,
14-54

Roaming-Berechtigungen, 14-20

Speichergeräte, 9-4

Suchberechtigungen, 7-60

Bericht zur Einhaltung von Richtlinien, 14-60

Bewertungsmodus, 7-82

Bootsektorvirus, 7-4

Bösartiger ActiveX-Code, 7-4

Bösartiger Java-Code, 7-4

C

C&C-Callbacks

Allgemeine Einstellungen

Benutzerdefinierte IPO-Listen,
11-14

widgets, 2-29

Cache-Einstellungen für die Suche, 7-70

Cache für die On-Demand-Suche, 7-72

Case Diagnostic Tool, 16-2

Certified Safe Software Liste, 12-3

Certified Safe Software Service, 7-87, 8-11,
12-28

COM-Dateiinfektor, 7-4

Command & Control-Kontaktalarmdienste,
11-2

Global Intelligence-Liste, 11-3

Smart Protection Server, 11-3

Virtual Analyzer, 11-3

Virtual Analyzer Liste, 11-3

community, 17-2

Control Manager

Integration in OfficeScan, 13-25

MCP-Agent-Protokolle, 16-11

Cookies durchsuchen, 7-83

CPU-Auslastung, 7-32

D

Damage Cleanup Services, 1-13, 5-4, 5-6

dashboard, 2-5

Benutzerkonten, 2-5

dashboards

Zusammenfassung, 2-6, 2-7, 2-11

Dashboard Übersicht, 2-6, 2-7, 2-11

Komponenten und Programme, 2-23

Registerkarten, 2-7

Status der Produktlizenz, 2-6

Vordefinierte Registerkarten, 2-11

Vordefinierte Widgets, 2-11

widgets, 2-7

Dateiattribute, 10-6, 10-11, 10-13, 10-14

erstellen, 10-13

Importieren, 10-14

Platzhalter, 10-13

vordefiniert, 10-12

Datenbank, Suche, 7-78

Datenbanksicherung, 13-47

Datenbezeichner, 10-6

Ausdrücke, 10-6

Dateiattribute, 10-6

Schlüsselwörter, 10-6

Datenschutz, 10-2

Deinstallation, 3-15

Installation, 3-2

Lizenz, 3-4

status, 3-8

Verteilung, 3-6

Debug-Protokolle

agents, 16-15

server, 16-3

Deinstallation, 5-75

Datenschutz, 3-15

Plug-in Manager, 15-12

Plug-in-Programm, 15-11

über die Webkonsole, 5-76

Verwenden des

Deinstallationsprogramms, 5-77

Dekomprimierungsregeln, 10-46

Device List, 9-14

DHCP-Einstellungen, 5-49

Dienst neu starten, 14-12

digitaler Signatur-Cache, 7-71

Dokumentation, xii

Domänen, 2-56, 2-63–2-65

Agent-Gruppierung, 2-56

hinzufügen, 2-63

löschen, 2-64

umbenennen, 2-65

DSP, 9-8

E

Early Boot Cleanup Driver, 6-7

Echtzeitsuchdienst, 14-42

Echtzeitsuche, 7-17

EICAR-Testskript, 5-74, 7-3

Eigenschutz des Agents, 14-13

eigenständiger Server, 4-7

Eigenständiger Smart Protection Server, 4-19

ptngrowth.ini, 4-19

Einhaltung von Sicherheitsrichtlinien, 14-59

Ausgelagerte Serververwaltung, 2-39,
14-74

Dienste, 14-61

durchsetzen, 14-74

- Einstellungen, 14-67
- installation, 5-66
- Komponenten, 14-62
- Protokolle, 16-9
- Suche, 14-64
- Update erzwingen, 6-56
- Zeitgesteuerte Bewertungen, 14-72
- Einstellungen exportieren, 14-57
- Einstellungen importieren, 14-57
- E-Mail-Domänen, 10-28
- Endbenutzer-Lizenzvereinbarung (EULA), E-4
- Ereignisüberwachung, 8-4
- Erkennungs-Pattern der Verhaltensüberwachung, 6-10
- Erweiterte Berechtigungen konfigurieren, 9-12
- Speichergeräte, 9-6, 9-7
- EXE-Dateiinfektor, 7-4
- Externe Geräte Zugriff verwalten, 9-11, 9-15
- Externe Geräte, Schutz, 6-10

F

- FakeAV, 7-46
- Fehlerbehebung Plug-in Manager, 15-12
- file reputation, 4-3
- File-Reputation-Dienste, 4-3
- firewall, 5-4, 5-6, 12-2
 - Aufgaben, 12-9
 - Ausbruchsmonitor, 12-6
 - Ausnahmen der Standardrichtlinie, 12-16
 - Berechtigungen, 12-6, 12-25
 - Deaktivieren, 12-7
 - Profile, 12-4, 12-19

- Richtlinien, 12-9
- Richtlinienausnahmen, 12-15
- Testen, 12-35
- Vorteile, 12-2
- Firewall-Protokollzähler, 12-28
- Fragmentiertes IGMP, 12-6
- Fragment zu groß, 12-5
- FTP, 10-29

G

- Gateway-IP-Adresse, 14-3
- Gerätesteuerung, 1-14, 9-2, 9-4, 9-6–9-13, 9-15
 - Benachrichtigungen, 9-18
 - Berechtigungen, 9-4, 9-6, 9-7, 9-9, 9-11
 - Programmpfad und -name, 9-9
 - Erweiterte Berechtigungen, 9-12
 - konfigurieren, 9-12
 - Externe Geräte, 9-11, 9-15
 - Nicht-Speichergeräte, 9-11
 - Platzhalter, 9-10
 - Protokolle, 9-19, 16-10
 - Provider der digitalen Signatur, 9-8
 - Speichergeräte, 9-4, 9-6, 9-7
 - USB-Geräte, 9-13
 - Voraussetzungen, 9-2
 - Zugriff verwalten, 9-11, 9-15
 - Zulässige Liste, 9-13
- Gerätesteuerung;Gerätesteuerungsliste;Gerätsteuerungsliste:Programme hinzufügen, 9-17

H

- Herkömmliche Suche, 7-10, 7-11
 - Wechsel zur intelligenten Suche, 7-11
- Hotfixes, 6-12
- hot fixes, 6-57
- HTML-Virus, 7-4
- HTTP und HTTPS, 10-30

I

- IDS, 12-4
- IM-Anwendungen, 10-30
- Import von Gateway-Einstellungen, 14-5
- Inaktive Agents, 14-26
- Inkrementelles Pattern, 6-23
- installation, 5-2
 - agent, 5-2
 - Einhaltung von Sicherheitsrichtlinien, 5-66
 - Plug-in Manager, 15-3
 - Plug-in-Programm, 15-4
- Installation
 - Datenschutz, 3-2
- Integrierter Server, 4-7
- Integrierter Smart Protection Server, 4-19
 - ptngrowth.ini, 4-19
 - update, 4-20, 4-21
 - Komponenten, 4-21
 - Websperrliste, 4-22
- Intelligente Suche, 6-4, 7-10, 7-11
 - Wechsel von der herkömmlichen Suche, 7-11
- IntelliScan, 7-30
- IntelliTrap Ausnahme-Pattern, 6-6
- IntelliTrap Pattern, 6-6
- Internet-Bedrohungen, 11-2
- intranet, 4-13
- Intrusion Detection System, 12-4
- IPv6, 4-24
 - support, 4-24
- IPv6-Unterstützung, A-2
 - Einschränkungen, A-3, A-4
 - IPv6-Adressen anzeigen, A-7
- IpXfer.exe, 14-24

J

- JavaScript-Virus, 7-4
- Jetzt aktualisieren, 6-51
- Jetzt durchsuchen, 7-25

K

- Kennwort, 13-61
- Kerndienst der Verhaltensüberwachung, 6-10
- Komponenten, 2-23, 5-74, 6-2
 - Aktualisieren der Übersicht, 6-68
 - auf dem Agent, 6-30
 - Auf dem OfficeScan Server, 6-17
 - Auf dem Update-Agent, 6-58
 - Update-Berechtigungen und -Einstellungen, 6-49
- Komponentenduplizierung, 6-23, 6-65
- Komprimierte Dateien, 7-31, 7-79, 7-80
 - Dekomprimierungsregeln, 10-46
- Kontinuität des Schutzes, 4-11
- Kriterien
 - Benutzerdefinierte Ausdrücke, 10-8, 10-9
 - Schlüsselwörter, 10-17–10-19

L

- LAND Attack, 12-6
- Liste der gesperrten Programme, 8-7
- Liste der zulässigen Programme, 8-7
- Lizenzen, 13-44
 - Datenschutz, 3-4
 - status, 2-6
- location awareness, 14-2
- logische Operatoren, 10-23
- LogServer.exe, 16-3, 16-15

M

- MAC-Adresse, 14-3
- mail scan, 7-68

Makrovirus, 7-4
 Manuelle Agent-Gruppierung, 2-56, 2-57
 Manuelle Suche, 7-20
 Verknüpfung, 7-77
 Microsoft Exchange Server, Suche, 7-78
 Microsoft SMS, 5-14, 5-34
 migration
 Von Antiviren-Programmen anderer
 Hersteller, 5-68
 Von ServerProtect Normal Servern,
 5-69
 MSI-Paket, 5-14, 5-32, 5-34

N

NetBIOS, 2-56
 Network VirusWall Enforcer, 4-33
 Netzwerkkanäle, 10-27–10-34, 10-44
 E-Mail-Clients, 10-28
 FTP, 10-29
 HTTP und HTTPS, 10-30
 IM-Anwendungen, 10-30
 Nicht überwachte Ziele, 10-34, 10-44
 SMB-Protokoll, 10-31
 Übertragungsumfang, 10-34
 alle Übertragungen, 10-32
 externe Übertragungen, 10-33
 Konflikte, 10-34
 Übertragungsumfang und Ziele, 10-31
 Überwachte Ziele, 10-34, 10-44
 webmail, 10-31
 Netzwerkvirus, 7-4, 12-4
 Neue Funktionen, 1-2
 Nicht erreichbare Agents, 14-47
 Nicht-Speichergeräte
 Berechtigungen, 9-11
 nicht überwachte E-Mail-Domänen, 10-28
 nicht überwachte Ziele, 10-32, 10-34

O

OfficeScan
 agent, 1-16
 Agent-Dienste, 14-12
 Datenbank, Suche, 7-78
 Datenbanksicherung, 13-47
 Dokumentation, xii
 Info über, 1-2
 Komponenten, 2-23, 6-2
 Komponenten-Update, 5-74
 Lizenzen, 13-44
 Programme, 2-23
 Protokolle, 13-40
 Webkonsole, 2-2
 webserver, 13-54
 Wichtigste Funktionen und Vorteile,
 1-12
 OfficeScan Agent
 Dateien durchsuchen, 14-15
 Deinstallation, 5-75
 Detaillierte Agent-Informationen, 14-57
 Einstellungen importieren und
 exportieren, 14-57
 Inaktive Agents, 14-26
 Installationsmethoden, 5-11
 Prozesse, 14-17
 Registrierungsschlüssel, 14-16
 Reservierter Festplattenspeicher, 6-52
 Verbindung mit OfficeScan Server,
 14-28, 14-42
 Verbindung mit Smart Protection
 Server, 14-43
 OfficeScan server, 1-15
 Funktionen, 1-15
 OfficeScan update, 6-15
 online

community, 17-2

P

packer, 7-2

Patches, 6-12

Pattern-Dateien

Agent-Pattern der intelligenten Suche,
4-8

Pattern der intelligenten Suche, 4-9
smart protection, 4-8

Websperreliste, 4-9

Pattern der intelligenten Suche, 4-9, 6-4

Pattern der Richtliniendurchsetzung, 6-11

Pattern für digitale Signaturen, 6-10, 7-71

Pattern zur Konfiguration der

Verhaltensüberwachung, 6-10

PCRE, 10-8

performance control, 7-32

Performance Tuning Tool, 16-2

Perl Compatible Regular Expressions, 10-8

phishing, E-10

Ping-of-Death, 12-5

Platzhalter, 10-13

Dateiattribute, 10-13

Gerätesteuerung, 9-10

Plug-in Manager, 1-12, 5-5, 5-7, 15-2

Deinstallation, 15-12

Fehlerbehebung, 15-12

installation, 15-3

native Produktfunktionen verwalten,
15-4

Plug-in-Programm

Aktivieren, 3-4, 15-6

deinstallieren, 15-11

installation, 15-4

Ports sperren, 7-121

Prävention gegen Datenverlust

System- und Anwendungskanäle, 10-35,
10-39

Prävention vor Datenverlust, 10-2, 10-3, 10-6

Aktionen, 10-41

Ausdrücke, 10-6–10-9, 10-11

Dateiattribute, 10-11–10-14

Datenbezeichner, 10-6

Dekomprimierungsregeln, 10-46

Kanäle, 10-27

Netzwerkkanäle, 10-27–10-34, 10-44

Richtlinien, 10-3, 10-50

Schlüsselwörter, 10-15–10-19, 10-21

System- und Anwendungskanäle, 10-34,
10-35, 10-38–10-41

Vorlagen, 10-22–10-24, 10-26

widgets, 2-25, 2-27

Programme, 2-23, 6-2

Protokolle, 13-40

Agent-Update-Protokolle, 6-55

Firewall-Protokolle, 12-26, 12-27, 12-31

Protokolle der Gerätesteuerung, 9-19

Protokolle der zentralen

Quarantänewiederherstellung, 7-106

Protokolle zu verdächtigen Dateien,
7-111

Sicherheitsrisiko-Protokolle, 7-98

Spyware-/Grayware-Protokolle, 7-107

Spyware-/Grayware-

Wiederherstellungsprotokolle, 7-111

Suchprotokolle, 7-113

Systemereignisprotokolle, 13-38

über, 13-40

Verbindungsüberprüfungsprotokolle,
14-46

Verhaltensüberwachung, 8-16

Viren-/Malware-Protokolle, 7-86, 7-98

Web-Reputation-Protokolle, 11-25
 Provider der digitalen Signatur, 9-8
 Angeben, 9-8
 Proxy-Einstellungen, 4-33
 agents, 4-33
 Automatische Proxy-Einstellungen, 14-56
 Berechtigungen, 14-54
 Für das Update von Server-Komponenten, 6-21
 Für externe Verbindungen, 14-53
 Für interne Verbindungen, 14-52
 ptngrowth.ini, 4-19

Q

Quarantäne-Manager, 13-62
 Quarantäne-Ordner, 7-43, 7-49

R

Referenzserver, 13-34
 Registerkarten, 2-7
 Remote-Installation, 5-13
 Ressourcen zur Fehlerbehebung, 16-1
 Richtlinien, 10-3
 firewall, 12-4, 12-9
 Prävention vor Datenverlust, 10-50
 web reputation, 11-5
 Roaming-Agents, 5-5, 5-7
 Rollenbasierte Administration, 2-39, 13-3
 Benutzerkonten, 13-14
 Benutzerrollen, 13-4
 rootkit, 7-3
 Rootkit-Erkennung, 6-10

S

Scherzprogramm, 7-2
 Schlüsselwörter, 10-6, 10-15

benutzerdefiniert, 10-17–10-19, 10-21
 vordefiniert, 10-15, 10-16

ServerProtect, 5-69

Serverprotokolle

 Active Directory Protokolle, 16-6
 Agent-Gruppierungsprotokolle, 16-7
 Agent Packager-Protokolle, 16-8
 Apache Server Protokolle, 16-8
 Debug-Protokoll der Viren-Scan-Engine, 16-13
 Debug-Protokolle, 16-3
 Debug-Protokolle des ServerProtect Migration Tools, 16-11
 Debug-Protokolle von VSEncrypt, 16-11
 Komponenten-Update-Protokolle, 16-7
 Lokale Installations-/Upgrade-Protokolle, 16-5
 Protokolle der Gerätesteuerung, 16-10
 Protokolle zum Control Manager MCP Agent, 16-11
 Protokolle zur ausgelagerten Serververwaltung, 16-9
 Protokolle zur Einhaltung der Sicherheitsrichtlinien, 16-9
 Protokolle zur rollenbasierten Administration, 16-6
 Protokolle zur Unterstützung von Virtual Desktop, 16-14
 Remote-Installations-/Upgrade-Protokolle, 16-5
 Web-Reputation-Protokolle, 16-10

Server Tuner, 13-64

Server-Update

 Komponentenduplizierung, 6-23
 Manuelles Update, 6-28

- Protokolle, 6-29
- Proxy-Einstellungen, 6-21
- Update-Methoden, 6-28
- Zeitgesteuertes Update, 6-29
- Sicherheits-Patches, 6-12
- Sicherheitsrisiken, 7-2, 7-5, 7-6, 7-8
 - Phishing-Angriffe, E-10
 - Schutz vor, 1-13
 - Spyware/Grayware, 7-5, 7-6, 7-8
- Sicherheits-Software anderer Anbieter, 5-67
- Smart Feedback, 4-3
- smart protection, 4-3, 4-6–4-10, 4-24, 4-25
 - Adresse, 4-7, 4-8
 - File-Reputation-Dienste, 4-3
 - Pattern-Dateien, 4-8–4-10
 - Agent-Pattern der intelligenten Suche, 4-8
 - Suche, 4-8
 - Pattern der intelligenten Suche, 4-9
 - Update-Vorgang, 4-10
 - Websperrliste, 4-9
 - Quellen, 4-24, 4-25
 - IPv6-Unterstützung, 4-24
 - Protokolle, 4-8
 - Standorte, 4-25
 - 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, 4-18–4-22
 - Bewährte Methoden, 4-18
 - Eigenständig, 4-7, 4-19
 - installation, 4-14
 - integriert, 4-7, 4-19–4-22
 - update, 6-17, 6-30
- SMB-Protokoll, 10-31
- Speichergeräte
 - Berechtigungen, 9-4
 - Erweiterte Berechtigungen, 9-6, 9-7
- Sperren des Malware-Verhaltens, 8-2
- spyware/grayware
 - Mögliche Bedrohungen, 7-7
 - spyware, 7-5
 - Wiederherstellen, 7-56
- 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-Aktivmonitor-Pattern, 6-8
- Spyware-Pattern, 6-8
- Spyware-Scan-Engine, 6-8
- SQL Server Migration Tool, 13-49, 13-53
 - Konfigurieren, 13-50
 - Warnmeldung, 13-52
- Standorte, 4-33
 - awareness, 4-33
- Statistik der 10 häufigsten Sicherheitsrisiken, 2-22
- Suchaktionen, 7-38
 - spyware/grayware, 7-52
 - Viren/Malware, 7-80
- Suchausschlüsse, 7-34
 - Dateien, 7-37

- Dateierweiterungen, 7-38
- Verzeichnisse, 7-35
- Suchberechtigungen, 7-59
- Suche nach Spyware/Grayware
 - Aktionen, 7-52
 - Ergebnisse, 7-108
 - Zulässige Liste, 7-54
- Suche nach Viren/Malware
 - Allgemeine Einstellungen, 7-76
 - Ergebnisse, 7-100
- Suchkriterien
 - Benutzerdefinierte Aktionen für Dateien, 7-29
 - CPU-Auslastung, 7-32
 - Dateikomprimierung, 7-31
 - Zeitplan, 7-33
 - Zu durchsuchende Dateien, 7-29
- Suchmethode, 5-28
 - Standardeinstellung, 7-9
- Suchtypen, 5-3, 5-6, 7-16
- Such-Zwischenspeicher, 7-70
- support
 - knowledge base, 17-2
 - Probleme schneller beheben, 17-4
 - TrendLabs, 17-7
- Support-Informationssystem, 2-5, 16-2
- SYN-Flooding, 12-5
- System- und Anwendungskanäle, 10-27, 10-34, 10-35, 10-38–10-41
 - CD/DVD, 10-35
 - Cloud Storage Service, 10-35
 - Drucker, 10-39
 - peer-to-peer (P2P), 10-38
 - PGP-Verschlüsselung, 10-38
 - Synchronisierungs-Software, 10-40
 - Wechseldatenträger, 10-39

- Windows-Zwischenablage, 10-41
- Systemvoraussetzungen
 - Update-Agent, 6-59

T

- Teardrop, 12-5
- Testsuche, 5-74
- Testversion, 13-44
- test virus, 7-3
- Tiny Fragment Attack, 12-6
- TMPerftool, 16-2
- TMTouch.exe, 6-57
- touch tool, 6-57
- Treiber der Verhaltensüberwachung, 6-10
- Treiber für die allgemeine Firewall, 6-9, 16-20
- TrendLabs, 17-7
- Trojaner, 1-13, 6-7, 7-3

U

- Überlappendes Fragment, 12-5
- überwachte E-Mail-Subdomänen, 10-28
- Überwachte Systemereignisse, 8-4
- überwachte Ziele, 10-32, 10-34
- Unterstützung von Virtual Desktop, 14-79
- update
 - Smart Protection Server, 6-17, 6-30
- Update-Adresse
 - agents, 6-33
 - OfficeScan server, 6-21
 - Update-Agents, 6-61
- Update-Agent, 5-3, 5-6, 6-58
 - 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, 6-28
- Update-Agent, 6-66
- updates, 4-20, 4-21
 - agents, 6-30
 - durchsetzen, 6-56
 - Integrierter Smart Protection Server, 4-20, 4-21
 - OfficeScan Server, 6-17
 - Update-Agent, 6-58
- URL-Filter-Engine, 6-9
- USB-Geräte
 - Zulässige Liste, 9-13
 - konfigurieren, 9-13

V

- VBScript-Virus, 7-4
- VDI, 14-79
 - Protokolle, 16-14
- VDI Tool zur Generierung von Prescan-Vorlagen, 14-91
- Verbindungsüberprüfung, 14-45
- Verhaltensüberwachung, 8-16
 - Aktion bei Systemereignissen, 8-6
 - Ausschlussliste, 8-7
 - Protokolle, 8-16
- Verschlüsselte Dateien, 7-48
- Viren-Cleanup-Engine, 6-7
- Viren-Cleanup-Template, 6-7
- Viren-Enzyklopädie, 7-5
- Viren-Pattern, 6-3, 6-55, 6-57
- Viren-Scan-Engine, 6-4
- Virensuchtreiber, 6-5
- 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
- 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, 10-6
 - anzeigen, 10-7
- Vordefinierte Registerkarten, 2-11
- Vordefinierte Schlüsselwörter
 - Abstand, 10-16
 - Anzahl der Schlüsselwörter, 10-16
- Vordefinierte Vorlagen, 10-22
- Vordefinierte Widgets, 2-11
- Vorlagen, 10-22–10-24, 10-26
 - Bedingungsanweisungen, 10-23
 - benutzerdefiniert, 10-23, 10-24, 10-26
 - logische Operatoren, 10-23
 - vordefiniert, 10-22
- Vulnerability Scanner, 5-15, 5-40
 - DHCP-Einstellungen, 5-49
 - Effektivität, 5-40
 - Endpunktbeschreibung abrufen, 5-60
 - Ping-Einstellungen, 5-63
 - Produktabfrage, 5-56
 - Unterstützte Protokolle, 5-58

W

- Wahrscheinlich Virus/Malware, 7-5, 7-101
- Web-Installationsseite, 5-11, 5-16

- Webkonsole, 1-12, 2-2–2-4
 - Anmeldekonto, 2-4
 - Banner, 2-4
 - Info über, 2-2
 - Kennwort, 2-4
 - URL, 2-3
 - Voraussetzungen, 2-3
 - webmail, 10-31
 - web reputation, 1-14, 5-4, 5-6, 11-4
 - Protokolle, 16-10
 - Richtlinien, 11-5
 - Web-Reputation-Dienste, 4-3, 4-4
 - Websperlliste, 4-9, 4-22
 - widgets, 2-7, 2-12, 2-15, 2-16, 2-20, 2-23, 2-24, 2-31–2-33, 15-3
 - Ausbrüche, 2-20
 - Widgets, 2-25, 2-27, 2-29
 - Agent-Server-Konnektivität, 2-15
 - Agent-Updates, 2-23
 - Antivirus-Agent-Konnektivität, 2-16
 - C & C-Callback-Ereignisse, 2-29
 - File Reputation – Bedrohungskarte, 2-33
 - OfficeScan- und Plug-in-Mashup, 2-24
 - Prävention vor Datenverlust –
 - Erkennungen im Zeitverlauf, 2-27
 - Prävention vor Datenverlust –
 - Häufigste Entdeckungen, 2-25
 - Sicherheitsrisiko-Funde, 2-20
 - Verfügbar, 2-12
 - Web Reputation – am häufigsten
 - bedrohte Benutzer, 2-32
 - Web Reputation – häufigste
 - Bedrohungsquellen, 2-31
 - Windows Server Core, B-2
 - Befehle, B-7
 - unterstützte Installationsmethoden, B-2
 - verfügbare Agent-Funktionen, B-6
 - Windows-Zwischenablage, 10-41
 - Wurm, 7-4
- Z**
- Zeitgesteuerte Bewertungen, 14-72
 - Zeitgesteuerte Suche, 7-22
 - Automatisch beenden, 7-85
 - Erinnerung, 7-84
 - Fortsetzen, 7-85
 - Überspringen und beenden, 7-63, 7-85
 - Verschieben, 7-84
 - Zulässige Liste, 7-54
 - Zusammenfassung
 - dashboard, 2-6, 2-7, 2-11
 - updates, 6-68
 - Zusätzliche Diensteinstellungen, 14-6, 14-7



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: OSGM116958/150522