



XG

OfficeScan™

Installations- und Upgrade-Handbuch

Für große und mittelständische Unternehmen



Endpoint Security



Protected Cloud



Web Security



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

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

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

Copyright © 2016. Trend Micro Deutschland GmbH. Alle Rechte vorbehalten.

Dokument-Nr.: OSGMXG7614/161028

Release-Datum: Oktober 2016

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	vii
OfficeScan Dokumentation	viii
Zielgruppe	ix
Dokumentationskonventionen	ix
Begriffe	x

Kapitel 1: Planen der OfficeScan Installation und Aktualisierung

Systemvoraussetzungen für Erstinstallation und Upgrade	1-2
Produktversionen	1-2
Registrierungsschlüssel und Aktivierungscodes	1-3
Überlegungen zur Erstinstallation	1-4
IPv6-Unterstützung	1-4
Standort des OfficeScan Servers	1-5
Remote-Installation	1-6
Serverleistung	1-7
Dedizierter Server	1-7
Verteilung der Suchmethode während der Installation	1-7
Netzwerkverkehr	1-9
Sicherheits-Software anderer Anbieter	1-11
Active Directory	1-11
IIS Web Server	1-11
Überlegungen zum Upgrade	1-12
IPv6-Unterstützung	1-12
Nicht unterstützte Betriebssysteme	1-12
Einstellungen und Konfigurationen von OfficeScan	1-13
Verteilung der Suchmethode während des Upgrades	1-15
Installations- und Upgrade-Checkliste	1-16

Testverteilung planen	1-24
Teststandort auswählen	1-24
Rollback-Plan entwerfen	1-24
Testverteilung auswerten	1-24
Bekannte Kompatibilitätsprobleme	1-24
Microsoft Lockdown Tool und URLScan	1-25
Microsoft Exchange Server	1-25
Datenbankserver	1-26

Kapitel 2: Installation von OfficeScan

Durchführen einer Erstinstallation des OfficeScan Servers	2-2
Unbeaufsichtigte Installation	2-2
Unbeaufsichtigte Installation vorbereiten	2-2
Setup-Konfiguration in einer Antwortdatei aufzeichnen	2-3
Unbeaufsichtigte Installation durchführen	2-4
Die Setup-Installationsfenster	2-5
Lizenzvereinbarung	2-8
Installationsziel	2-9
Endpoint Prescan	2-11
Installationspfad	2-13
Proxy-Server	2-14
Webserver	2-15
Serverkennung	2-18
Registrierung und Aktivierung	2-20
OfficeScan Agent-Verteilung	2-22
Integrierten Smart Protection Server installieren	2-23
Installationsziel	2-26
Analyse des Zielpunkts	2-28
OfficeScan Agent installieren	2-30
Smart Protection Network	2-31
Kennwort für das Administratorkonto	2-33
Installation des OfficeScan Agents	2-35
OfficeScan Firewall	2-37
Anti-Spyware-Funktion	2-38
Web-Reputation-Funktion	2-39
Serverauthentifizierungszertifikat	2-40

OfficeScan Programmverknüpfungen	2-43
Installationsdaten	2-44
Der InstallShield Wizard ist abgeschlossen.	2-45

Kapitel 3: OfficeScan upgraden

Aktualisieren des OfficeScan Servers und der Agents	3-2
Vor dem Upgrade des OfficeScan Servers und der Agents	3-2
Durchführen eines lokalen Upgrades	3-21
Aktualisieren von OfficeScan 10.6 SP3 mit Apache	3-21
Aktualisieren von OfficeScan 10.6 SP3 mit IIS	3-39
Aktualisieren von OfficeScan 11.x	3-51
Durchführen eines Remote-Upgrades	3-62
Lizenzvereinbarung	3-63
Installationsziel	3-64
Endpoint Prescan	3-66
Installationspfad	3-68
Proxy-Server	3-69
Webserver	3-70
Serverkennung	3-73
Registrierung und Aktivierung	3-75
OfficeScan Agent-Verteilung	3-77
Integrierten Smart Protection Server installieren	3-78
Installationsziel	3-81
Analyse des Zielpunkts	3-83
Warnung wegen Neustart des OfficeScan Agents	3-85
Datenbanksicherung	3-85
Serverauthentifizierungszertifikat	3-86
Installationsdaten	3-89
Der InstallShield Wizard ist abgeschlossen.	3-90

Kapitel 4: Aufgaben nach der Installation

Die Installation oder das Upgrade des Servers überprüfen	4-2
Überprüfen der Installation des integrierten Smart Protection Servers	4-4
Aktualisieren von OfficeScan Komponenten	4-5
Den OfficeScan Server aktualisieren	4-5

Standardeinstellungen überprüfen	4-5
Sucheinstellungen	4-6
Agent Einstellungen	4-6
Agent-Berechtigungen	4-6
OfficeScan beim Control Manager registrieren	4-6

Kapitel 5: Deinstallieren und Rollback von OfficeScan

Überlegungen zu Deinstallation und Rollback	5-2
Vor der Deinstallation des OfficeScan Servers	5-2
Verschieben von Agents auf einen anderen OfficeScan Server	5-2
OfficeScan Datenbank und Konfigurationsdateien sichern und wiederherstellen	5-3
OfficeScan Server deinstallieren	5-5
Den OfficeScan Server mit Hilfe des Deinstallationsprogramms deinstallieren	5-5
Den OfficeScan Server manuell deinstallieren	5-6
Durchführen eines Rollbacks des OfficeScan Servers und der OfficeScan Agenten mit dem Serversicherungspaket	5-10
Durchführen eines Rollbacks des OfficeScan Agentens	5-10
Wiederherstellen der Vorgängerversion des OfficeScan Servers ..	5-12
Durchführen eines manuellen Rollbacks zu früheren OfficeScan Versionen	5-16
Teil 1: Vorgängerversion des OfficeScan Servers vorbereiten	5-17
Teil 2: Vorbereiten einer Update-Adresse für Agents, für die ein Rollback durchgeführt werden soll	5-19
Teil 3: Durchführen eines Rollbacks des OfficeScan Agents	5-23

Kapitel 6: OfficeScan Ressourcen zur Fehlerbehebung

Support-Informationssystem	6-2
Case Diagnostic Tool	6-2
Trend Micro Performance Tuning Tool	6-2
Systemintensive Anwendungen identifizieren	6-3
Installationsprotokolle	6-5

Debug-Protokolle für den Server	6-5
Aktivieren der Debug-Protokollierung auf dem OfficeScan Server-Computer	6-6
Agent-Debug-Protokolle	6-7
Aktivieren der Debug-Protokollierung auf dem OfficeScan Agent	6-8

Kapitel 7: Technischer Support

Ressourcen zur Fehlerbehebung	7-2
Support-Portal verwenden	7-2
Bedrohungsenzyklopädie	7-2
Kontaktaufnahme mit Trend Micro	7-3
Problemlösung beschleunigen	7-4
Verdächtige Inhalte an Trend Micro senden	7-4
E-Mail-Reputation-Dienste	7-5
File-Reputation-Dienste	7-5
Web-Reputation-Dienste	7-5
Sonstige Ressourcen	7-6
Download Center	7-6
Anregungen und Kritik	7-6

Anhang A: Verteilungsbeispiel

Basisnetzwerk	A-2
Netzwerk mit mehreren Standorten	A-3
Netzwerk mit mehreren Standorten vorbereiten	A-5
Verteilung im Hauptbüro	A-6
Verteilung am Remote-Standort 1	A-6
Verteilung am Remote-Standort 2	A-7

Stichwortverzeichnis

Stichwortverzeichnis	IN-1
----------------------------	------

Vorwort

Vorwort

Willkommen beim Trend Micro™ OfficeScan™ *Installations- und Upgrade-Handbuch*. In diesem Dokument werden die Anforderungen und Verfahren zum Installieren des OfficeScan Servers sowie zum Aktualisieren des Servers und der agents beschrieben.

Themen in diesem Kapitel:

- *OfficeScan Dokumentation auf Seite viii*
- *Zielgruppe auf Seite ix*
- *Dokumentationskonventionen auf Seite ix*
- *Begriffe auf Seite x*



Hinweis

Weitere Informationen zur Installation von agents finden Sie im *Administratorhandbuch*.

OfficeScan Dokumentation

Die OfficeScan Dokumentation umfasst Folgendes:

TABELLE 1. OfficeScan Dokumentation

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

KONVENTION	BESCHREIBUNG
 Tipp	Empfehlungen oder Vorschläge
 Wichtig	Informationen zu den erforderlichen oder standardmäßigen Konfigurationseinstellungen und Produktbeschränkungen
 Warnung!	Wichtige Aktionen und Konfigurationsoptionen

Begriffe

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

TABELLE 3. OfficeScan Terminologie

BEGRIFFE	BESCHREIBUNG
OfficeScan Agent	Das OfficeScan agent Programm
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.

BEGRIFFE	BESCHREIBUNG
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.
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

BEGRIFFE	BESCHREIBUNG
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.
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 • 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

BEGRIFFE	BESCHREIBUNG
Plug-in-Lösungen	Native OfficeScan Funktionen und Plug-in-Programme, die über Plug-in Manager bereitgestellt werden

Kapitel 1

Planen der OfficeScan Installation und Aktualisierung

In diesem Kapitel werden die für die Installation und das Upgrade von Trend Micro™ OfficeScan™ zu treffenden Vorbereitungen beschrieben.

Themen in diesem Kapitel:

- *Systemvoraussetzungen für Erstinstallation und Upgrade auf Seite 1-2*
- *Produktversionen auf Seite 1-2*
- *Registrierungsschlüssel und Aktivierungscode auf Seite 1-3*
- *Überlegungen zur Erstinstallation auf Seite 1-4*
- *Überlegungen zum Upgrade auf Seite 1-12*
- *Installations- und Upgrade-Checkliste auf Seite 1-16*
- *Testverteilung planen auf Seite 1-24*
- *Bekannte Kompatibilitätsprobleme auf Seite 1-24*

Systemvoraussetzungen für Erstinstallation und Upgrade

Führen Sie eine Erstinstallation des OfficeScan Servers und der Agents auf unterstützten Windows Server-Plattformen durch.

Darüber hinaus unterstützt diese OfficeScan Version Aktualisierungen von folgenden Versionen:

- 11.0 Service Pack 1
- 11.0
- 10.6 Service Pack 3



Hinweis

Trend Micro empfiehlt dringend, alle verfügbaren Patches und Hotfixes auf den aktuellen OfficeScan Server vor dem Durchführen eines Upgrades anzuwenden.

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

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

Produktversionen

Installieren Sie entweder die Voll- oder die Testversion von OfficeScan. Für die Installation der beiden Versionen ist jeweils ein anderer Aktivierungscode erforderlich. Registrieren Sie das Produkt bei Trend Micro, um einen Aktivierungscode zu erhalten.

TABELLE 1-1. Versionsvergleich

VERSION	BESCHREIBUNG
Vollversion	Die Vollversion beinhaltet sämtliche Produktfunktionen und bietet Anspruch auf technischen Support. Darüber hinaus ist eine Übergangsfrist (üblicherweise 30 Tage) nach Ablauf der Lizenz enthalten. Nach Ablauf der Übergangsfrist sind kein technischer Support und keine Komponenten-Updates mehr erhältlich. Die Scan Engines durchsuchen weiterhin die Endpunkte unter Verwendung nicht aktueller Komponenten. Diese veralteten Komponenten können die Endpunkte unter Umständen nicht vollständig vor den aktuellen Sicherheitsrisiken schützen. Sie können die Lizenz vor oder nach ihrem Ablauf durch den erneuten Abschluss eines Wartungsvertrags verlängern.
Testversion	Die Testversion umfasst alle Produktfunktionen. Sie können jederzeit ein Upgrade von der Testversion auf die Vollversion durchführen. Falls nach Ablauf des Testzeitraums kein Upgrade durchgeführt wird, deaktiviert OfficeScan Komponenten-Updates, Suchläufe sowie alle agent-Funktionen.

Registrierungsschlüssel und Aktivierungs-codes

Während der Installation geben Sie die Aktivierungscodes für folgende Dienste an:

- Virenschutz
- Damage Cleanup Services™ (optional)
- Web Reputation und Anti-Spyware (optional)

Verwenden Sie den Registrierungsschlüssel, den Sie mit dem Produkt erhalten haben, um Aktivierungscodes abzurufen (falls Sie diese nicht bereits erhalten haben). Setup leitet Sie automatisch zur Produktregistrierung auf die Trend Micro Website.

<http://olr.trendmicro.com>

Nach der Registrierung des Produkts sendet Trend Micro die Aktivierungscodes.

Wenden Sie sich an Ihren Trend Micro Vertriebspartner, um den Registrierungsschlüssel oder Aktivierungscode zu erhalten, falls Sie zum Zeitpunkt der Installation weder über das eine noch über das andere verfügen. Weitere Informationen finden Sie unter *Kontaktaufnahme mit Trend Micro auf Seite 7-3*.



Hinweis

Antworten auf Fragen zur Registrierung finden Sie unter:

<http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326>.

Überlegungen zur Erstinstallation

Beachten Sie Folgendes, wenn Sie eine Erstinstallation des OfficeScan Servers durchführen:

- *IPv6-Unterstützung auf Seite 1-4*
- *Standort des OfficeScan Servers auf Seite 1-5*
- *Remote-Installation auf Seite 1-6*
- *Serverleistung auf Seite 1-7*
- *Dedizierter Server auf Seite 1-7*
- *Verteilung der Suchmethode während der Installation auf Seite 1-7*
- *Netzwerkverkehr auf Seite 1-9*
- *Sicherheits-Software anderer Anbieter auf Seite 1-11*
- *Active Directory auf Seite 1-11*
- *IIS Web Server auf Seite 1-11*

IPv6-Unterstützung

Für die Erstinstallation des OfficeScan Servers gelten folgende IPv6-Voraussetzungen:

- Der Server muss einen IIS Webserver verwenden.
- Wenn der Server IPv4- und IPv6-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-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.

- Stellen Sie sicher, dass die IPv6- oder IPv4-Adresse des Host-Computers beispielsweise mit Hilfe des Befehls "ping" oder "nslookup" abgerufen werden kann.
- Gehen Sie folgendermaßen vor, wenn Sie den OfficeScan Server auf einem reinen IPv6-Endpunkt installieren:
 - Richten Sie einen Dual-Stack-Proxy-Server ein, der zwischen IPv4- und IPv6-Adressen konvertieren kann (wie etwa DeleGate). Platzieren Sie den Proxy-Server zwischen dem OfficeScan Server und dem Internet, damit der Server sich erfolgreich mit den von Trend Micro verwalteten Diensten verbinden kann, z. B. dem ActiveUpdate Server, der Online-Registrierungswebsite und Smart Protection Network.

Standort des OfficeScan Servers

OfficeScan kann an unterschiedliche Netzwerkumgebungen angepasst werden. Sie können beispielsweise eine Firewall zwischen dem OfficeScan Server und den Agents

positionieren oder sowohl den Server als auch alle Agents hinter einer einzigen Netzwerk-Firewall anordnen. Falls sich zwischen dem Server und den Agents eine Firewall befindet, müssen Sie diese so konfigurieren, dass der Datenverkehr zwischen dem Agent- und dem Server-Listening-Port zugelassen wird.

Informationen zur Lösung möglicher Probleme bei der Verwaltung von OfficeScan Agents in einem Netzwerk mit NAT (Network Address Translation) finden Sie im *Administratorhandbuch*.



Wichtig

Aus Sicherheitsgründen empfiehlt Trend Micro die Installation des OfficeScan Servers im Firmenintranet. Wenn Sie Endpunkte verwalten müssen, die das lokale Intranet verlassen, empfiehlt Trend Micro die Installation des OfficeScan Edge-Relais-Servers in der DMZ.

Remote-Installation

Bei einer Remote-Installation können Sie die Installation auf einem Endpunkt starten, während Sie OfficeScan auf einem anderen Endpunkt installieren. Das Setup-Programm überprüft bei einer Remote-Installation, ob der Ziel-Endpunkt die Voraussetzungen für die Installation des Servers erfüllt.

Sicherstellen, dass die Installation fortgesetzt werden kann:

- Starten Sie den Remote-Registrierungsdienst auf jedem Ziel-Endpunkt über ein Administratorkonto und nicht über ein lokales Systemkonto. Der Remote-Registrierungsdienst wird von der Microsoft Management-Konsole aus verwaltet. (Klicken Sie auf **Start** > **Ausführen**, und geben Sie `services.msc` ein.)
- Notieren Sie sich den Host-Namen des Endpunkts und die Anmeldedaten (Benutzername und Kennwort).
- Stellen Sie sicher, dass der Endpunkt die Systemvoraussetzungen für den OfficeScan Server erfüllt. Weitere Informationen finden Sie unter *Systemvoraussetzungen für Erstinstallation und Upgrade auf Seite 1-2*.

Serverleistung

Server in Netzwerken großer Unternehmen müssen höher dimensioniert werden als in mittelständischen Betrieben.



Tipp

Trend Micro empfiehlt als OfficeScan Server einen Computer, der über zwei Prozessoren mit mindestens 2 GHz und mehr als 2 GB Arbeitsspeicher verfügt.

Wie viele Endpunkt-agents im Netzwerk ein einziger OfficeScan Server verwalten kann, hängt von verschiedenen Faktoren ab, wie beispielsweise den verfügbaren Serverressourcen und der Netzwerktopologie. Wenden Sie sich an den Trend Micro Vertriebspartner, um Unterstützung bei der Bestimmung der Anzahl der vom Server zu verwaltenden agents zu erhalten.

Dedizierter Server

Beim Auswählen des Endpunkts, auf dem Sie den OfficeScan Server hosten, beachten Sie Folgendes:

- Die CPU-Auslastung des Endpunkts
- Andere Aufgaben des Endpunkts

Falls der Ziel-Endpunkt noch andere Funktionen zu erfüllen hat, wählen Sie einen anderen Endpunkt, auf dem keine kritischen oder ressourcenintensiven Anwendungen ausgeführt werden.

Verteilung der Suchmethode während der Installation

In dieser OfficeScan Version können Sie agents entweder für die Verwendung der intelligenten Suche oder für die Verwendung der herkömmlichen Suche konfigurieren.

Herkömmliche Suche

Die herkömmliche Suche ist die in allen Vorgängerversionen von OfficeScan verwendete Suchmethode. Ein agent der herkömmlichen Suche speichert alle OfficeScan Komponenten auf dem agent-Endpunkt und durchsucht alle Dateien lokal.

Intelligente Suche

Bei der intelligenten Suche werden Bedrohungssignaturen verwendet, die im Internet gespeichert sind. Im intelligenten Suchmodus sucht der OfficeScan agent zunächst lokal nach Sicherheitsrisiken. Wenn der agent das Risiko der Datei während der Suche nicht ermitteln kann, stellt der agent eine Verbindung zu einem Smart Protection Server her.

Die intelligente Suche bietet die folgenden Merkmale und Vorteile:

- Bietet schnelle Nachschlagefunktionen in Echtzeit für den Sicherheitsstatus im Web
- Verkürzt die Zeitspanne, bis Schutz vor neu entstandenen Bedrohungen bereitgestellt werden kann
- Reduziert die während Pattern-Updates benötigte Netzwerkbandbreite. Die große Menge an Pattern-Definitions-Updates muss lediglich an die Cloud und nicht an die zahlreichen agents gesendet werden.
- Verringert die Kosten und den Overhead, die mit unternehmensweiten Pattern-Verteilungen verbunden sind
- Vermindert den Kernel-Arbeitsspeicherverbrauch an Endpunkten. Der Verbrauch erhöht sich mit der Zeit nur leicht.

Verteilung der Suchmethode

Während Erstinstallationen wird als Standardsuchmethode für agents die intelligente Suche verwendet. Nach der Installation des Servers ermöglicht OfficeScan die Anpassung der Suchmethode für jede Domäne. Beachten Sie Folgendes:

- Wenn Sie die Suchmethode nach der Installation des Servers nicht geändert haben, verwenden alle installierten agents die intelligente Suche.

- Wenn die herkömmliche Suche auf allen Agents verwendet werden soll, ändern Sie nach der Installation des Servers die Suchmethode auf Stammebene in die herkömmliche Suche.
- Wenn Sie sowohl die herkömmliche als auch die intelligente Suche verwenden möchten, empfiehlt Trend Micro, die intelligente Suche als Suchmethode auf Stammebene beizubehalten. Ändern Sie anschließend die Suchmethode in den Domänen, in denen die herkömmliche Suche angewendet werden soll.

Netzwerkverkehr

Kalkulieren Sie bei der Verteilungsplanung die Menge an Netzwerkverkehr ein, der von OfficeScan verursacht wird. Es entsteht Netzwerkverkehr, wenn der Server einen der folgenden Vorgänge ausführt:

- Stellt eine Verbindung zum Trend Micro ActiveUpdate Server her, um nach aktualisierten Komponenten zu suchen und diese herunterzuladen
- Fordert Agents zum Download aktualisierter Komponenten auf
- Benachrichtigt Agents bei Konfigurationsänderungen

Es entsteht Netzwerkverkehr, wenn der OfficeScan Agent einen der folgenden Vorgänge ausführt:

- Beim Systemstart
- Beim Aktualisieren von Komponenten
- Beim Aktualisieren von Einstellungen und Installieren eines Hotfix
- Bei der Suche nach Sicherheitsrisiken
- Beim Wechsel vom „unabhängigen“ Modus in den „Normalbetrieb“
- Beim Wechsel von der herkömmlichen zur intelligenten Suche

Netzwerkverkehr während eines Komponenten-Updates

Beim Update einer Komponente erzeugt OfficeScan erheblichen Netzwerkverkehr. Um den bei Komponenten-Updates entstehenden Netzwerkverkehr zu verringern, führt

OfficeScan eine Komponentenduplizierung durch. Anstatt bei der Aktualisierung die vollständige Pattern-Datei herunterzuladen, lädt OfficeScan nur die inkrementellen Pattern (kleinere Versionen der vollständigen Pattern-Datei) herunter und führt diese nach dem Download mit der alten Pattern-Datei zusammen.

OfficeScan Agents, die regelmäßig aktualisiert werden, laden nur das inkrementelle Pattern herunter. Anderenfalls wird die vollständige Pattern-Datei heruntergeladen.

Trend Micro stellt regelmäßig neue Pattern-Dateien bereit. Darüber hinaus stellt Trend Micro eine neue Pattern-Datei bereit, sobald sich im Umlauf befindliche, schädliche Viren oder Malware entdeckt wird.

Update-Agents und Netzwerkverkehr

Wenn sich zwischen den Agents und dem OfficeScan Server Netzwerkabschnitte mit geringer Bandbreite oder hohen Datenaufkommen befinden, können Sie ausgewählte OfficeScan Agents als Update-Agents oder Update-Adressen für andere Agents festlegen. Dadurch wird die durch die Verteilung von Komponenten entstehende Last auf alle Agents aufgeteilt.

Definieren Sie beispielsweise einen Update-Agent, der für ein externes Büro mit mindestens 20 Endpunkten Updates vom OfficeScan Server repliziert und als lokaler Verteilungspunkt für die übrigen Agent-Endpunkte im lokalen Netzwerk fungiert. Weitere Informationen über Update-Agents finden Sie im *Administratorhandbuch*.

Trend Micro Control Manager und Netzwerkverkehr

Trend Micro Control Manager™ verwaltet Produkte und Dienste von Trend Micro auf Gateways, Mail-Servern, Dateiservern und Unternehmensdesktops. Die webbasierte Management-Konsole von Control Manager bietet einen zentralen Überwachungspunkt für Produkte und Dienste im gesamten Netzwerk.

Control Manager ermöglicht die zentrale Verwaltung mehrerer OfficeScan Server. Ein Control Manager Server mit einer schnellen vertrauenswürdigen Internetverbindung kann Komponenten vom Trend Micro ActiveUpdate Server herunterladen. Control Manager verteilt die Komponenten dann auf einen oder mehrere OfficeScan Server mit einer unzuverlässigen oder keiner Internetverbindung.

Weitere Informationen finden Sie in der Control Manager-Dokumentation.

Sicherheits-Software anderer Anbieter

Entfernen Sie Endpunkt-Sicherheitssoftware von Drittanbietern von dem Endpunkt, auf dem Sie den OfficeScan Server installieren. Das Vorhandensein solcher Anwendungen kann die erfolgreiche Installation eines OfficeScan Servers verhindern oder dessen Leistung beeinträchtigen. Installieren Sie den OfficeScan Server und den OfficeScan Agent sofort, nachdem Sie die Sicherheitssoftware von Drittanbietern entfernt haben, um den Endpunkt weiterhin vor Sicherheitsrisiken zu schützen.



Hinweis

OfficeScan kann nur die agent-Komponente, nicht jedoch die Serverkomponente anderer Virenschutzprodukte automatisch deinstallieren. Weitere Informationen finden Sie im *Administratorhandbuch für OfficeScan*.

Active Directory

Alle OfficeScan Server müssen zu einer Active Directory-Domäne gehören, um die Vorteile der Funktionen für die rollenbasierte Administration und die Einhaltung von Sicherheitsrichtlinien nutzen zu können.

IIS Web Server

Zu den Funktionen des OfficeScan Webservers gehören:

- Gewährt Benutzern Zugriff auf die Webkonsole
- Nimmt Befehle von Agents entgegen
- Erlaubt Agents, auf Server-Benachrichtigungen zu antworten

Stellen Sie bei Verwendung eines IIS Webservers sicher, dass auf dem Server keine Anwendungen ausgeführt werden, die IIS sperren. Setup beendet den IIS Dienst automatisch während der Installation und startet ihn erneut.

Überlegungen zum Upgrade

Beachten Sie Folgendes, wenn Sie ein Upgrade des OfficeScan Servers und der Agents durchführen:

- *IPv6-Unterstützung auf Seite 1-12*
- *Nicht unterstützte Betriebssysteme auf Seite 1-12*
- *Einstellungen und Konfigurationen von OfficeScan auf Seite 1-13*
- *Verteilung der Suchmethode während des Upgrades auf Seite 1-15*

IPv6-Unterstützung

Für OfficeScan Server- und Agent-Upgrades gelten folgende IPv6-Voraussetzungen:

- Der zu aktualisierende OfficeScan Server muss in der Version 10.6 SP3 oder 11.x vorliegen.
- Der Server muss bereits einen IIS Webserver verwenden.
- Weisen Sie dem Server eine IPv6-Adresse zu. Zusätzlich muss der Server über seinen Host-Namen identifiziert werden, vorzugsweise seinen vollqualifizierten Domännennamen (FQDN). Wenn der Server über seine IPv6-Adresse identifiziert wird, verlieren alle aktuell vom Server verwalteten Agents ihre Verbindung mit dem Server. Wenn der Server über seine IPv4-Adresse identifiziert wird, kann der Server den Agent nicht an reine IPv6-Computer verteilen.
- Stellen Sie sicher, dass die IPv6- oder IPv4-Adresse des Host-Computers beispielsweise mit Hilfe des Befehls **ping** oder **nslookup** abgerufen werden kann.

Nicht unterstützte Betriebssysteme

Windows 95, 98, Me, NT, 2000 und die Itanium-Architektur werden von OfficeScan nicht mehr unterstützt.

Gehen Sie wie folgt vor, wenn Sie ein Upgrade auf diese Version durchführen möchten und über OfficeScan Agents mit den folgenden Betriebssystemen verfügen:

- Aktualisieren Sie nicht alle OfficeScan Server auf diese OfficeScan Version.
- Bestimmen Sie mindestens einen OfficeScan Server (übergeordneten Server) für die Verwaltung der Agents, auf denen nicht unterstützte Betriebssysteme ausgeführt werden.
- Vor dem Upgrade der anderen Server:
 - Für OfficeScan 10.x Server:
 - Melden Sie sich bei der Webkonsole an, und klicken Sie im Hauptmenü auf **Netzwerkcomputer > Client-Verwaltung**.
 - Wählen Sie in der Client-Hierarchie die zu verschiebenden Clients aus und klicken Sie anschließend auf **Client-Hierarchie verwalten > Client verschieben**.
 - Geben Sie unterhalb von **Ausgewählte(n) Client(s) auf einen anderen OfficeScan Server verschieben** den Namen oder die IP-Adresse des übergeordneten Servers sowie den Server-Listening-Port an.
 - Klicken Sie auf **Verschieben**.
 - Für OfficeScan 11.x Server:
 - Melden Sie sich bei der Webkonsole an und klicken Sie im Hauptmenü auf **Agents > Agent-Verwaltung**.
 - Wählen Sie in der Agent-Hierarchie die zu verschiebenden Agents aus und klicken Sie anschließend auf **Agent-Hierarchie verwalten > Agent verschieben**.
 - Geben Sie unterhalb von **Ausgewählte(n) Agent(s) auf einen anderen OfficeScan Server verschieben** den Namen oder die IP-Adresse des übergeordneten Servers sowie den Server-Listening-Port an.
 - Klicken Sie auf **Verschieben**.

Einstellungen und Konfigurationen von OfficeScan

Sichern Sie die OfficeScan Datenbank und wichtige Konfigurationsdateien, bevor Sie den OfficeScan Server upgraden. Erstellen Sie eine Sicherungskopie der OfficeScan

Server-Datenbank an einem Speicherort außerhalb des OfficeScan Programmverzeichnis.



Tipp

Diese Version von OfficeScan enthält einen Sicherungsmechanismus für Rollback-Zwecke. Führen Sie eine manuelle Datenbanksicherung durch, wenn Sie nicht vorhaben, die automatische Sicherung bei der Installation zu verwenden.

Sichern und Wiederherstellen der OfficeScan Datenbank und der Konfigurationsdateien

Prozedur

1. Sichern Sie die Datenbank über die Webkonsole von OfficeScan 10.x oder 11.x, indem Sie zu **Administration > Datenbanksicherung** navigieren.

Detaillierte Anweisungen finden Sie im *Administratorhandbuch* oder in der *Server-Hilfe* für diese Produktversionen.



Warnung!

Verwenden Sie kein anderes Tool oder keine andere Anwendung zur Datenbanksicherung.

2. Beenden Sie den OfficeScan Master Service von der Microsoft Management-Konsole aus.
3. Führen Sie eine manuelle Datensicherung der folgenden Dateien und Ordner durch, die sich unter dem Pfad <Installationsordner des Servers> \PCCSRV befinden:



Hinweis

Sichern Sie diese Dateien und Ordner, um ein Rollback von OfficeScan durchführen zu können, falls beim Upgrade Probleme auftreten.

- `ofcscan.ini`: Enthält globale Agent-Einstellungen

- `ous.ini`: Diese Datei enthält die Liste der Update-Adressen für die Verteilung von Antiviren-Komponenten.
 - `Persönlicher Ordner`: Dieser Ordner enthält die Einstellungen der Firewall und der Update-Adressen.
 - `Ordner Web\tmlOPP`: Dieser Ordner enthält die Einstellungen der Ausbruchsprävention.
 - `Pccnt\Common\OfcPfw*.dat`: Diese Datei enthält die Einstellungen der Firewall.
 - `Download\OfcPfw*.dat`: Diese Datei enthält die Einstellungen zur Verteilung der Firewall.
 - `Ordner Log`: Dieser Ordner enthält Systemereignisse und das Verbindungsprotokoll.
 - `Ordner Virus`: Dieser Ordner enthält die in Quarantäne verschobenen Dateien.
 - `Ordner HTTPDB`: Dieser Ordner enthält die OfficeScan Datenbank.
4. Führen Sie ein Upgrade des OfficeScan Servers durch.

**Hinweis**

Falls Probleme beim Upgrade auftreten, kopieren Sie die Sicherungsdateien aus Schritt 3 in den Ordner `<Installationsordner des Servers>\PCCSRV` auf dem Zielendpunkt, und starten Sie den OfficeScan Master Service neu.

Verteilung der Suchmethode während des Upgrades

In dieser OfficeScan Version können Administratoren Agents entweder für die Verwendung der intelligenten Suche oder der herkömmlichen Suche konfigurieren.

Beim OfficeScan Upgrade von einer früheren Version können Sie für jede Domäne abhängig von der ausgewählten Upgrade-Methode die Suchmethode beibehalten oder anpassen. Beachten Sie Folgendes:

- Wenn Sie ein direktes Upgrade von OfficeScan 10.x oder 11.x Server auf dem Server planen, sind keine Änderungen an der Suchmethode über die Webkonsole erforderlich, weil die Agents nach dem Upgrade ihre Einstellungen für die Suchmethode beibehalten.
- Wenn Sie ein Upgrade von OfficeScan 10.x oder 11.x Agents durch Verschieben auf einen OfficeScan XG Server planen:
 - Wählen Sie auf dem OfficeScan XG Server "Manuelle Agent-Gruppierung" aus. Bei dieser Methode zur Agent-Gruppierung können Sie neue Domänen erstellen.



Hinweis

Wenn Sie die automatische Agent-Gruppierung verwenden, aktivieren Sie diese erst, nachdem alle Agents das Upgrade erhalten haben, um sicherzustellen, dass während des Agent-Upgrades die Einstellungen für die Suchmethode beibehalten werden.

- Verwenden Sie die Einstellungen für die Domänenstruktur und die Suchmethode auf dem OfficeScan 10.x oder 11.x Server auch auf dem OfficeScan XG Server. Wenn die Einstellungen für die Domänenstruktur und die Suchmethode auf beiden Servern nicht identisch sind, werden auf bestimmten Agents, die auf den OfficeScan XG Server verschoben wurden, nicht die ursprünglichen Einstellungen für die Suchmethode angewendet.

Installations- und Upgrade-Checkliste

Während der Installation oder Aktualisierung des OfficeScan Servers werden Sie vom Setup-Programm zur Eingabe folgender Informationen aufgefordert.

TABELLE 1-2. Installations- und Upgrade-Checkliste

INSTALLATIONS DATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAU FSICHTIG TE ERSTINS TALLATI ON	REMOTE - ERSTINS TALLATI ON	LOKAL/ UNBEAU FSICHTIG TES UPGRAD E	REMOTE - UPGRAD E
OfficeScan Installationspfad Der Standardinstallationspfad auf dem Server lautet: • C:\Programme\Trend Micro\OfficeScan • C:\Programme (x86)\Trend Micro\OfficeScan (für x64-Plattformen) Geben Sie den Installationspfad an, oder verwenden Sie den Standardpfad. Wenn der Pfad nicht vorhanden ist, erstellt Setup ihn automatisch.	Ja	Ja	Nein	Ja
Proxy-Server-Einstellungen Wenn sich der OfficeScan Server über einen Proxy-Server mit dem Internet verbindet, geben Sie Folgendes an: • Proxy-Typ (HTTP oder SOCKS 4) • Servername oder IP-Adresse • Port • Anmeldedaten für die Proxy-Authentifizierung	Ja	Ja	Nein	Ja

INSTALLATIONS DATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAUF- SICHTIG- TE ERSTIN- STALLATI- ON	REMOTE - ERSTIN- STALLATI- ON	LOKAL/ UNBEAUF- SICHTIG- TES UPGRAD- E	REMOTE - UPGRAD- E
Web-Server-Einstellungen Der Webserver führt CGI-Skripts für die Webkonsole aus und nimmt Befehle von agents entgegen. Geben Sie Folgendes ein: • HTTP-Port: Der Standardport lautet 8080. Wenn Sie die IIS-Standardwebsite verwenden, überprüfen Sie den TCP-Port des HTTP-Servers.  Warnung! Viele Hacker- und Viren- bzw. Malware-Angriffe gelangen über HTTP-Datenverkehr und die Ports 80 und/oder 8080 in das System, da die meisten Unternehmen diese Ports als Standard-TCP-Ports für den HTTP-Datenverkehr nutzen. Verwenden Sie andere Ports, falls die Standardports derzeit verwendet werden. Falls sichere Verbindungen aktiviert werden: • Gültigkeitsdauer des SSL-Zertifikats • SSL-Port (Standard: 4343)	Ja	Ja	Nein	Ja

INSTALLATIONS DATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAU FSICHTIG TE ERSTINS TALLATI ON	REMOTE - ERSTINS TALLATI ON	LOKAL/ UNBEAU FSICHTIG TES UPGRAD E	REMOTE - UPGRAD E
Registrierung Registrieren Sie das Produkt, um die Aktivierungs codes zu erhalten. Folgende Angaben sind zur Registrierung des Produkts erforderlich: - Für Benutzer mit Benutzerkonto: - Online-Registrierungskonto (Anmeldename und -Kennwort) - Für Benutzer ohne Benutzerkonto: - Registrierungsschlüssel	Ja	Ja	Ja	Ja
Aktivierung Beziehen Sie die Aktivierungs codes für folgende Produkt-Dienste: - Virenschutz - Damage Cleanup Services - Web Reputation und Anti-Spyware	Ja	Ja	Ja	Ja
Installation des integrierten Smart Protection Servers Geben Sie Folgendes an, wenn Sie den integrierten Server installieren: - Gültigkeitsdauer des SSL-Zertifikats - SSL-Port	Ja	Ja	Ja	Ja

INSTALLATIONS DATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAUFSICHTIGTE ERSTINSTALLATION	REMOTE - ERSTINSTALLATION	LOKAL/ UNBEAUFSICHTIGTES UPGRADE	REMOTE - UPGRADE
Ziel der Remote-Installation Geben Sie die Endpunkte an, auf denen der OfficeScan Server installiert/aktualisiert werden soll. Bereiten Sie Folgendes vor: • Eine Liste der Endpunktnamen oder IP-Adressen • (Optional) Eine Textdatei mit einer Liste der Namen oder IP-Adressen der Zielpunkte Beispiel der Textdatei: <pre>Benutzer_01 Admin_01 123.12.12.123</pre>	Nein	Ja	Nein	Ja
Remote-Installation – Endpunktanalyse Vor der Analyse des Zielpunkts fordert Sie das Setup-Programm zur Eingabe folgender Informationen auf: • Benutzername und Kennwort eines Administratorkontos auf dem Zielpunkt mit der Berechtigung "Anmeldung als Dienst"	Nein	Ja	Nein	Ja
Installieren Sie den OfficeScan Agent	Ja	Nein	Nein	Nein

INSTALLATIONS DATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAU FSICHTIG TE ERSTINS TALLATI ON	REMOTE - ERSTINS TALLATI ON	LOKAL/ UNBEAU FSICHTIG TES UPGRAD E	REMOTE - UPGRAD E
Kennwort für das Administratorkonto Setup erstellt ein Root-Konto für die Anmeldung an der Webkonsole. Geben Sie Folgendes ein: • Kennwort für das Root-Konto Verhindern Sie das unbefugte Deinstallieren oder Beenden des OfficeScan Agents, indem Sie Folgendes angeben: • Kennwort zum Deinstallieren/ Beenden des OfficeScan Agents	Ja	Ja	Nein	Nein

INSTALLATIONS DATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAU FSICHTIG TE ERSTINS TALLATI ON	REMOTE - ERSTINS TALLATI ON	LOKAL/ UNBEAU FSICHTIG TES UPGRAD E	REMOTE - UPGRAD E
Installationspfad des OfficeScan Agents Geben Sie das Verzeichnis auf dem Agent-Endpunkt an, auf dem der OfficeScan Agent installiert werden soll. Geben Sie Folgendes ein: • Installationspfad: Der Standardpfad für die Agent-Installation lautet <code>\$Programme\Trend Micro\OfficeScan Client</code>. Geben Sie den Installationspfad an, oder verwenden Sie den Standardpfad. Falls der Pfad nicht vorhanden ist, erstellt Setup ihn während der Agent-Installation. • Nummer des Kommunikationsports des OfficeScan Agents: OfficeScan erzeugt die Portnummer über einen Zufallsgenerator. Übernehmen Sie die generierte Portnummer, oder geben Sie eine neue an.	Ja	Ja	Nein	Nein

INSTALLATIONS DATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAU FSICHTIG TE ERSTINS TALLATI ON	REMOTE - ERSTINS TALLATI ON	LOKAL/ UNBEAU FSICHTIG TES UPGRAD E	REMOTE - UPGRAD E
Datenbanksicherung Geben Sie einen Speicherort auf dem Server an, um die OfficeScan Datenbank für Rollback-Zwecke zu sichern.  Hinweis Das Sicherungspaket benötigt mindestens 300 MB freien Festplattenspeicher. Die Sicherung kann einige Zeit in Anspruch nehmen.	Nein	Nein	Ja	Ja
Serverauthentifizierungszertifikat OfficeScan versucht, bereits vorhandene Authentifizierungszertifikate während der Installation zu erkennen. Wenn OfficeScan kein Zertifikat erkennt, geben Sie das Sicherungskennwort für das neue Zertifikat an.	Ja	Ja	Ja (beim Aktualisieren von OfficeScan 10.6 SP3)	Ja
Verknüpfung mit Programmordner Die Verknüpfung zum Installationsordner des OfficeScan Servers wird im Windows-Startmenü angezeigt. Der Standardname der Verknüpfung lautet Trend Micro OfficeScan Server- <Server_name>. Geben Sie einen anderen Namen an, oder übernehmen Sie den Standardnamen.	Ja	Nein	Nein	Nein

Testverteilung planen

Führen Sie vor der vollständigen Verteilung zunächst eine Testverteilung in einer kontrollierten Umgebung durch. Bei dieser Testverteilung haben Sie die Möglichkeit festzustellen, wie die Funktionen arbeiten und in welchem Umfang nach der vollständigen Verteilung Support erforderlich sein wird. Sie ermöglicht Ihrem Installationsteam, den Verteilungsprozess zu proben und zu verfeinern. Außerdem können Administratoren damit feststellen, ob der Verteilungsplan den Sicherheitsanforderungen des Unternehmens entspricht.

Weitere Informationen zu einer OfficeScan Testbereitstellung finden Sie unter *[Verteilungsbeispiel auf Seite A-1](#)*.

Teststandort auswählen

Wählen Sie einen Pilotstandort aus, der der Produktionsumgebung entspricht. Versuchen Sie, eine Netzwerktopologie zu simulieren, die die Produktionsumgebung abbildet.

Rollback-Plan entwerfen

Erstellen Sie einen Wiederherstellungs- oder Rollback-Plan für den Fall, dass bei der Installation oder beim Upgrade Probleme auftreten.

Testverteilung auswerten

Erstellen Sie eine Liste mit den positiven und negativen Aspekten der Testverteilung. Notieren Sie potenzielle Gefahren, und planen Sie entsprechend. Beziehen Sie diesen Testauswertungsplan in den endgültigen Verteilungsplan ein.

Bekannte Kompatibilitätsprobleme

In diesem Abschnitt werden Kompatibilitätsprobleme erläutert, die auftreten können, wenn Sie den OfficeScan Server zusammen mit Software anderer Hersteller auf

demselben Endpunkt installieren. Weitere Informationen zu Anwendungen von anderen Herstellern finden Sie in der Dokumentation.

Microsoft Lockdown Tool und URLScan

Wenn Sie das Microsoft IIS Lockdown Tool oder URLScan verwenden, kann die Sperrung der folgenden OfficeScan Dateien die Kommunikation zwischen dem OfficeScan Agent und dem Server blockieren:

- Konfigurationsdateien (.ini)
- Datendateien (.dat)
- DLL-Dateien (.dll)
- Programmdateien (.exe)

Verhindern von Konflikten mit URLScan bei der Agent-Server-Kommunikation

Prozedur

1. Beenden Sie den WWW-Publishingdienst auf dem OfficeScan Server-Computer.
 2. Ändern Sie die Konfigurationsdatei für URLScan, um die oben angegebenen Dateitypen zuzulassen.
 3. Starten Sie den WWW-Publishingdienst neu.
-

Microsoft Exchange Server

Wenn Sie während der Serverinstallation auch den OfficeScan Agent installieren, benötigt OfficeScan Zugriff auf alle Dateien, die vom Agent durchsucht werden. Da der Microsoft Exchange Server E-Mails in lokalen Verzeichnissen speichert, müssen diese Verzeichnisse aus der Suche ausgeschlossen werden, damit der Exchange Server E-Mails verarbeiten kann.

OfficeScan schließt automatisch alle Microsoft Exchange 2000/2003 Verzeichnisse von der Suche aus. Konfigurieren Sie diese Einstellung auf der Webkonsole (**Agents > Globale Agent-Einstellungen > Sucheinstellungen** auf der Registerkarte **Sicherheitseinstellungen**). Einzelheiten zu Suchausschlüssen bei Microsoft Exchange 2007 finden Sie unter:

[http://technet.microsoft.com/en-us/library/bb332342\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb332342(EXCHG.80).aspx)

Datenbankserver

Administratoren können Datenbankserver nach Viren durchsuchen. Die Suche kann jedoch bei den Anwendungen, die auf diese Datenbanken zugreifen, zu Leistungseinbußen führen. Daher sollten Datenbanken und deren Backup-Ordner ggf. von der Echtzeitsuche ausgeschlossen werden. Führen Sie eine manuelle Suche an Zeiten mit geringem Arbeitsaufkommen durch, um die Auswirkungen der Virensuche in Datenbanken so gering wie möglich zu halten.

Kapitel 2

Installation von OfficeScan

In diesem Kapitel werden die Schritte für die Installation von Trend Micro™ OfficeScan™ beschrieben.

Themen in diesem Kapitel:

- *Durchführen einer Erstinstallation des OfficeScan Servers auf Seite 2-2*
- *Unbeaufsichtigte Installation auf Seite 2-2*
- *Die Setup-Installationsfenster auf Seite 2-5*

Durchführen einer Erstinstallation des OfficeScan Servers

Zur Durchführung von Erstinstallationen führen Sie das Setup-Programm auf Endpunkten aus, die die Installations- und Upgrade-Anforderungen für den OfficeScan Server erfüllen (Einzelheiten hierzu finden Sie unter *[Systemvoraussetzungen für Erstinstallation und Upgrade auf Seite 1-2](#)*).

Das Setup-Programm installiert den OfficeScan Server und Plug-in Manager 2.3. Diese Version von Plug-in Manager stellt die Widget-Funktionalität in OfficeScan bereit. Informationen zu den Installationsfenstern und Konfigurationsoptionen finden Sie unter *[Die Setup-Installationsfenster auf Seite 2-5](#)*.

Methoden und Anweisungen zur Erstinstallation des Agents sowie Informationen zur Installation des Edge-Relais-Servers finden Sie im *Administratorhandbuch*.

Unbeaufsichtigte Installation

Sie können mehrere OfficeScan Server unbeaufsichtigt installieren oder aktualisieren, sofern die Installationseinstellungen der Server übereinstimmen.

Wenn auf dem Zielpunkt eine unbeaufsichtigte Installation ausgeführt wird, werden OfficeScan XG und Plug-in Manager 2.3 vom Setup-Programm installiert. Plug-in Manager 2.3 stellt die Widget-Funktionalität in OfficeScan bereit.

Unbeaufsichtigte Installation vorbereiten

Prozedur

1. Erstellen Sie eine Antwortdatei, indem Sie Setup ausführen und die Installationseinstellungen in einer `.iss`-Datei aufzeichnen. Die Einstellungen werden von allen Servern verwendet, die unbeaufsichtigt mit Hilfe der Antwortdatei installiert wurden.

**Wichtig**

- Die Setup-Fenster beziehen sich nur auf eine lokale Installation.
- Erstellen Sie bei Erstinstallationen eine Antwortdatei auf einem beliebigen Endpunkt ohne installierten OfficeScan Server.

2. Führen Sie Setup über die Befehlszeile aus, und verweisen Sie Setup auf den Speicherort der Antwortdatei für die unbeaufsichtigte Installation.

Setup-Konfiguration in einer Antwortdatei aufzeichnen

Bei diesem Vorgang wird OfficeScan nicht installiert. Es wird nur die Setup-Konfiguration in einer Antwortdatei aufgezeichnet.

Prozedur

1. Laden Sie die Datei `OSCE.exe` herunter und extrahieren Sie die Inhalte.
2. Öffnen Sie eine Befehlszeile und geben Sie das Verzeichnis der OfficeScan Datei `setup.exe` ein.

Beispiel: `"CD C:\OfficeScan Installer\setup.exe"`.

3. Geben Sie folgenden Befehl ein:

`setup.exe -r`

Der Parameter `-r` weist das Programm an, zu starten und die Installationsdetails in einer Antwortdatei aufzuzeichnen.

4. Führen Sie die Installationsschritte in Setup durch.
5. Prüfen Sie anschließend die Antwortdatei `setup.iss` im Verzeichnis `%windir%`.

Unbeaufsichtigte Installation durchführen

Prozedur

1. Kopieren Sie das Installationspaket und die Datei `setup.iss` auf den Ziel-Endpunkt.
2. Öffnen Sie eine Eingabeaufforderung auf dem Ziel-Endpunkt und geben Sie das Verzeichnis des Installationspakets ein.
3. Geben Sie folgenden Befehl ein:

```
setup.exe -s <-f1Pfad>setup.iss <-f2Pfad>setup.log.
```

Beispiel: `C:\setup.exe -s -f1C:\setup.iss -f2C:\setup.log`

Wobei gilt:

- `-s`: Weist das Setup-Programm an, eine unbeaufsichtigte Installation durchzuführen.
 - `<-f1path>setup.iss`: Dies ist der Speicherort der Antwortdatei. Setzen Sie den Pfad in Anführungsstriche, falls Leerzeichen enthalten sind. Beispiel: `-f1"C:\osce script\setup.iss"`.
 - `<-f2path>setup.log`: Dies ist der Speicherort der Protokolldatei, die Setup im Anschluss an die Installation erstellt. Setzen Sie den Pfad in Anführungsstriche, falls Leerzeichen enthalten sind. Beispiel: `-f2"C:\osce log\setup.log"`.
4. Drücken Sie auf EINGABE.

Das Setup-Programm führt nun eine unbeaufsichtigte Installation des Servers auf dem Endpunkt durch.
 5. Um festzustellen, ob die Installation ordnungsgemäß durchgeführt wurde:
 - Überprüfen Sie die OfficeScan Programmverknüpfungen auf dem Ziel-Endpunkt. Falls keine Verknüpfungen erstellt wurden, führen Sie die Installation erneut durch.

- Melden Sie sich bei der OfficeScan Webkonsole an.

Die Setup-Installationsfenster

Nachfolgend finden Sie eine Liste der Installationsfenster (in der entsprechenden Reihenfolge), die angezeigt werden, wenn Sie eine Erstinstallation des OfficeScan Servers lokal, remote oder unbeaufsichtigt durchführen.

TABELLE 2-1. Installationsfenster und -aufgaben

FENSTER	LOKAL/ UNBEAUF SICHTI GTE ERSTINSTALLAT ION	REMOTE- ERSTINSTALLAT ION
Voraussetzungen für OfficeScan Installation		
Begrüßungsfenster		
<i>Lizenzvereinbarung auf Seite 2-8</i>		
<i>Installationsziel auf Seite 2-9</i>		
<i>Endpoint Prescan auf Seite 2-11</i>		
Setup-Status (Endpunktanalyse)		
 Hinweis Die Analyse kann einige Zeit in Anspruch nehmen, insbesondere während der Initialisierung der HTTP-Server.		
<i>Installationspfad auf Seite 2-13</i>		

FENSTER	LOKAL/ UNBEAUF SICHTI GTE ERSTINSTALLAT ION	REMOTE- ERSTINSTALLAT ION
<i>Proxy-Server auf Seite 2-14</i>		
<i>Webserver auf Seite 2-15</i>		
<i>Serverkennung auf Seite 2-18</i>		
<i>Registrierung und Aktivierung auf Seite 2-20</i>		
<i>OfficeScan Agent-Verteilung auf Seite 2-22</i>		
<i>Integrierten Smart Protection Server installieren auf Seite 2-23</i>		
<i>Installationsziel auf Seite 2-26</i>		
<i>Analyse des Zielendpunkts auf Seite 2-28</i>		
<i>OfficeScan Agent installieren auf Seite 2-30</i>		
<i>Smart Protection Network auf Seite 2-31</i>		
<i>Kennwort für das Administratorkonto auf Seite 2-33</i>		
<i>Installation des OfficeScan Agents auf Seite 2-35</i>		
<i>OfficeScan Firewall auf Seite 2-37</i>		
<i>Anti-Spyware-Funktion auf Seite 2-38</i>		

FENSTER	LOKAL/ UNBEAUF SICHTI GTE ERSTINSTALLAT ION	REMOTE- ERSTINSTALLAT ION
<i>Web-Reputation-Funktion auf Seite 2-39</i>		
<i>Serverauthentifizierungszertifikat auf Seite 2-40</i>		
<i>OfficeScan Programmverknüpfungen auf Seite 2-43</i>		
<i>Installationsdaten auf Seite 2-44</i>		
Installation des OfficeScan Servers		
<i>Der InstallShield Wizard ist abgeschlossen. auf Seite 2-45</i>		

Lizenzvereinbarung

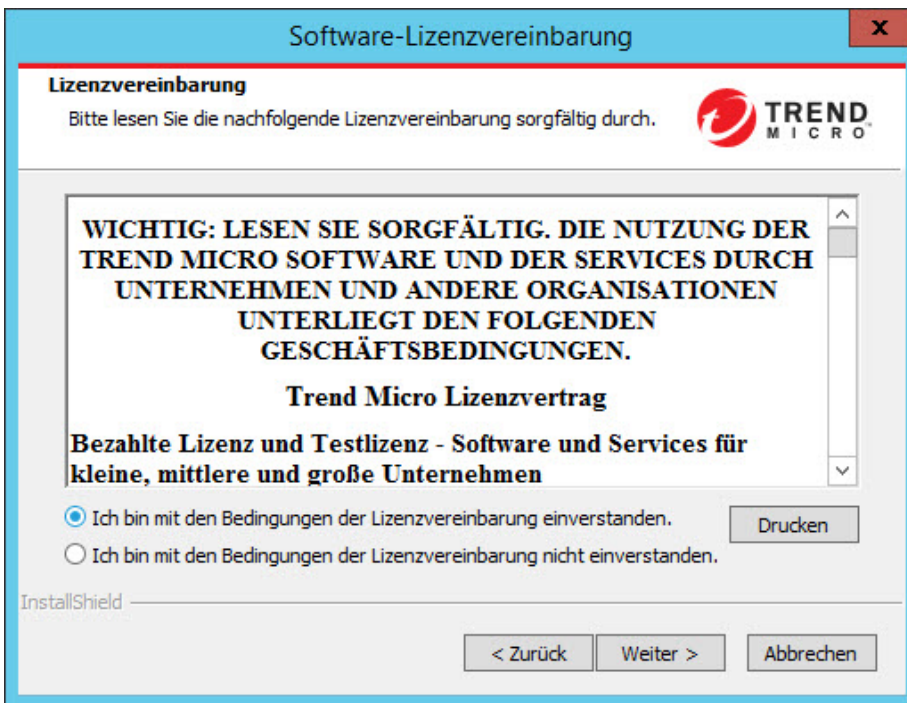


ABBILDUNG 2-1. Fenster "Lizenzvereinbarung"

Lesen Sie die Lizenzvereinbarung aufmerksam durch, und stimmen Sie den Bedingungen der Lizenzvereinbarung zu, um die Installation fortzusetzen. Die Installation kann nicht fortgesetzt werden, wenn Sie den Bedingungen der Lizenzvereinbarung nicht zustimmen.

Installationsziel

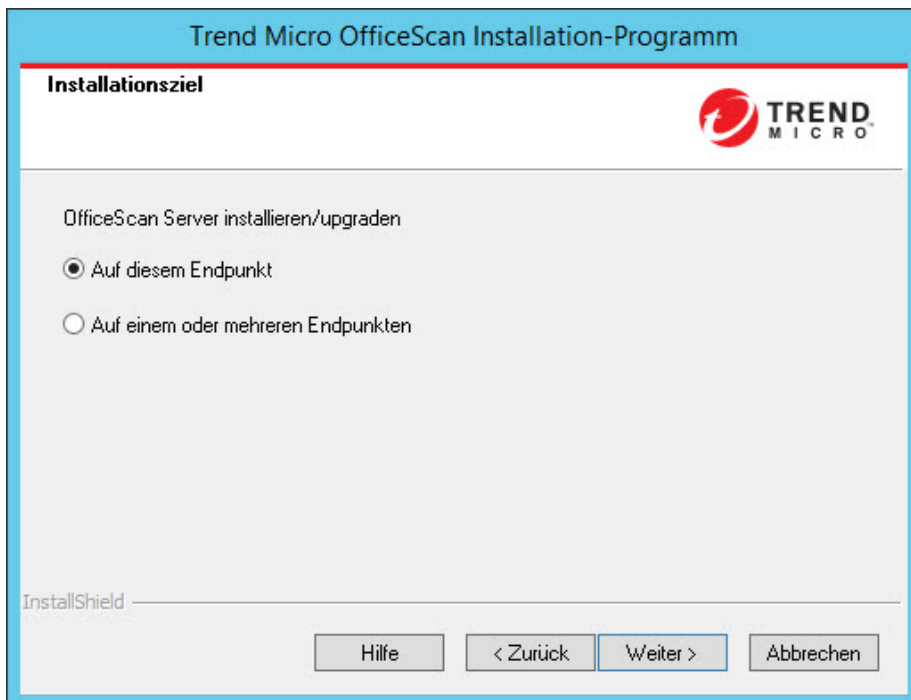


ABBILDUNG 2-2. Das Fenster "Installationsziel"

Führen Sie das Setup-Programm aus und installieren Sie den OfficeScan Server auf dem aktuellen Endpunkt oder auf anderen Endpunkten im Netzwerk. Wenn vom Setup-Programm eine frühere Version von OfficeScan auf dem Zielpunkt erkannt wird, wird bei der Installation automatisch ein Upgrade durchgeführt. Nur die folgenden Versionen von OfficeScan können auf diese Version aktualisiert werden:

- 11.0 Service Pack 1
- 11.0
- 10.6 Service Pack 3



Hinweis

Trend Micro empfiehlt dringend, alle verfügbaren Patches und Hotfixes auf den aktuellen OfficeScan Server vor dem Durchführen eines Upgrades anzuwenden.

Hinweise zur Remote-Installation

Bei der Remote-Installation prüft Setup, ob der Zielendpunkt die Voraussetzungen für die Installation des Servers erfüllt. Bevor Sie den Vorgang fortsetzen:

- Sie müssen auf dem Zielendpunkt über Administratorrechte verfügen.
- Notieren Sie sich den Host-Namen und die Anmeldedaten (Benutzername und Kennwort) für die Zielendpunkte.
- Stellen Sie sicher, dass die Zielendpunkte die Anforderungen für die Installation des OfficeScan Servers erfüllen.
- Stellen Sie sicher, dass auf dem Endpunkt Microsoft IIS Server 7.0 oder höher installiert ist, wenn er als Webserver eingesetzt wird.

Endpoint Prescan

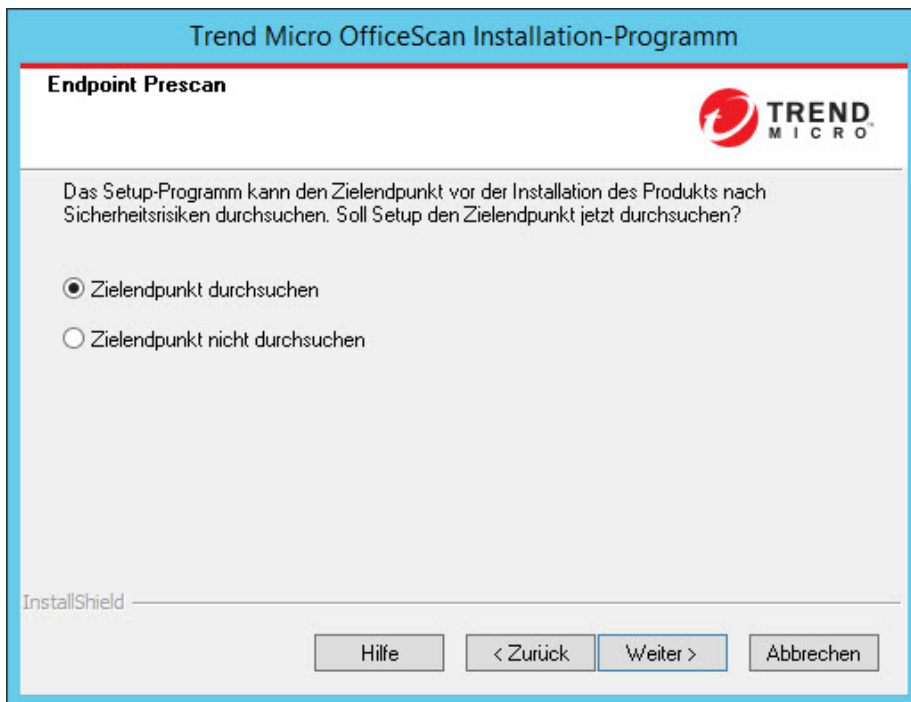


ABBILDUNG 2-3. Das Fenster "Endpoint Prescan"

Vor der Installation des OfficeScan Servers kann das Setup-Programm den Zielpunkt auf Viren und Malware überprüfen. Setup durchsucht die anfälligsten Bereiche des Endpunkts, wie beispielsweise:

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

Bei der Entdeckung von Viren/Malware und Trojanern kann Setup folgende Aktionen durchführen:

- **Löschen:** Löscht die infizierte Datei.
- **Säubern:** Eine Datei, die gesäubert werden kann, wird gesäubert, bevor der vollständige Zugriff möglich ist. Eine Datei, die nicht gesäubert werden kann, wird gemäß der festgelegten Aktion bearbeitet.
- **Umbenennen:** Die Erweiterung der infizierten Datei wird in *vir* geändert. Der Benutzer kann die 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:** Ermöglicht den vollständigen Zugriff auf die Datei, ohne sie zu verändern. Die Datei kann kopiert, gelöscht oder geöffnet werden.

Bei der lokalen Installation startet die Suche, wenn Sie auf **Weiter** klicken. Bei der Remote-Installation startet die Suche vor der eigentlichen Installation.



Wichtig

Während der lokalen Installation eines Upgrades werden Sie vom Setup-Programm aufgefordert, die Einstellungen für den Ransomware-Schutz zu aktualisieren, damit optimaler Schutz vor Ransomware-Bedrohungen gewährleistet werden kann.

Die Anwendung der aktualisierten Einstellungen wirkt sich nur auf Agents aus, die die Verhaltensüberwachung bereits aktiviert haben.

Installationspfad

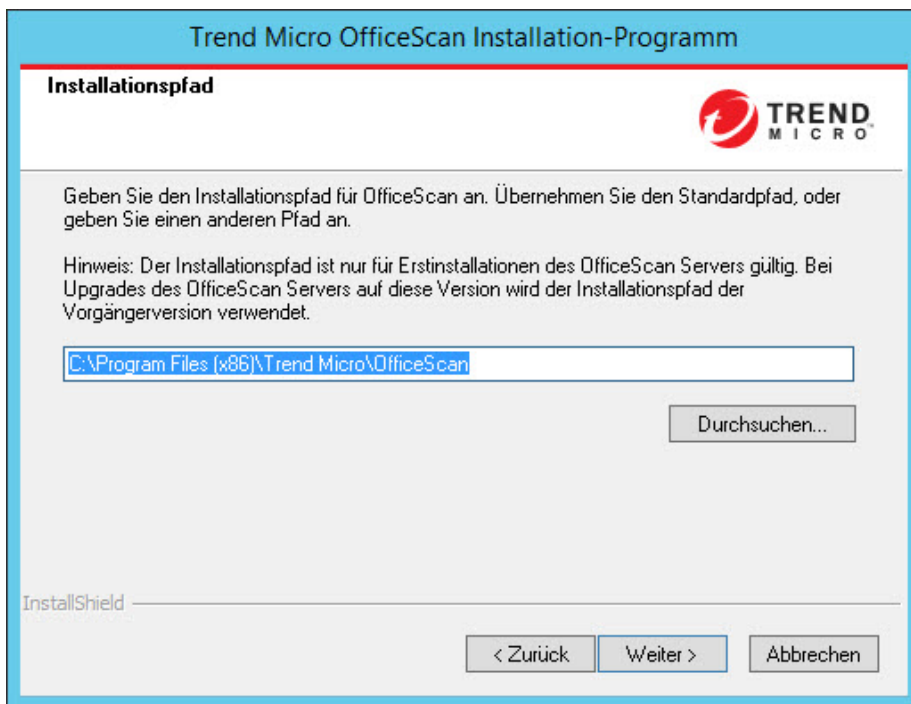


ABBILDUNG 2-4. Das Fenster "Installationspfad"

Übernehmen Sie den Standard-Installationspfad, oder geben Sie einen neuen Pfad an.

Der angegebene Installationspfad wird nur bei einer remote durchgeführten Erstinstallation angewendet. Bei remote durchgeführten Upgrades verwendet OfficeScan die Einstellungen aus der Vorgängerversion.

Proxy-Server

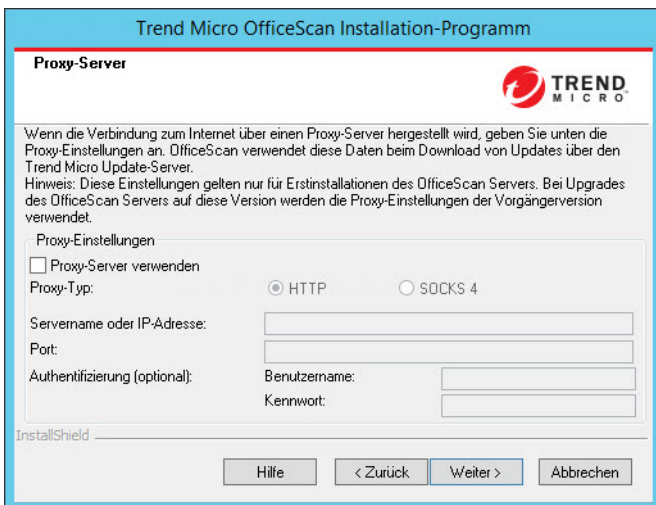


ABBILDUNG 2-5. Das Fenster "Proxy-Server"

Der OfficeScan Server verwendet für die Kommunikation zwischen agent und Server, für die Verbindung mit dem Trend Micro ActiveUpdate Server und für das Herunterladen von Updates das HTTP-Protokoll. Wenn Sie im Netzwerk den Zugriff auf das Internet über einen Proxy-Server steuern, benötigt OfficeScan die Proxy-Einstellungen zum Herunterladen von Updates vom ActiveUpdate Server.

Der Administrator kann die Proxy-Einstellungen auch nach der Installation über die OfficeScan Webkonsole eingeben.

Die Proxy-Einstellungen betreffen nur eine Remote-Erstinstallation. Bei remote durchgeführten Upgrades verwendet OfficeScan die Einstellungen aus der früheren Version.

**Hinweis**

Wenn Sie den OfficeScan Server auf einem reinen IPv6-Endpoint installieren, richten Sie einen Dual-Stack-Proxy-Server ein, der IP-Adressen umwandeln kann. Auf diese Weise kann der Server erfolgreich eine Verbindung zum ActiveUpdate Server herstellen.

Webserver

Trend Micro OfficeScan Installation-Programm

Webserver

Konfigurieren Sie den Webserver, der für den OfficeScan Server verwendet werden soll. OfficeScan verwendet SSL als Übertragungsprotokoll für die Webkonsole.

Hinweis: Die Einstellungen des Webserverns gelten nur für Erstinstallationen des OfficeScan Servers. Bei Upgrades des OfficeScan Servers auf diese Version werden die Einstellungen der Vorgängerversion verwendet.

IIS-Server: Virtuelle IIS Website

HTTP-Port: 8080

SSL-Einstellungen

Gültigkeitsdauer des Zertifikats: 3 Jahr(e)

SSL-Port: 4343

InstallShield

Hilfe < Zurück Weiter > Abbrechen

ABBILDUNG 2-6. Das Fenster "Webserver"

Der OfficeScan Webserver hostet die Webkonsole, nimmt Befehle von den agents entgegen und ermöglicht dem Administrator, CGI-Skripte (Common Gateway Interface) auszuführen. Der Webserver konvertiert diese Befehle in agent-CGI-Skripte und leitet sie an den OfficeScan Master Service weiter.

Die Webserver-Einstellungen betreffen nur eine Remote-Erstinstallation. Bei einem remote durchgeführten Upgrade verwendet OfficeScan die Einstellungen aus der Vorgängerversion.

IPv6-Unterstützung

Wählen Sie für Neuinstallationen den IIS-Server zum Aktivieren der IPv6-Unterstützung.

Wenn ein Upgrade auf diese OfficeScan Version durchgeführt wird, muss der zu aktualisierende OfficeScan Server bereits IIS verwenden.



Wichtig

Wenn Sie Apache mit Hilfe des Installationspakets des vorherigen OfficeScan Servers installiert haben, installiert und konfiguriert OfficeScan den IIS Webserver automatisch während des Upgrades. Wenn Sie den Apache-Server manuell installiert haben, müssen Sie diesen vor dem Aktualisieren des OfficeScan Servers manuell entfernen.

IIS-Unterstützung für Webserver

- Die folgenden Versionen von Microsoft Internet Information Server (IIS) sind erforderlich:
 - Version 7.0 unter Windows Server 2008
 - Version 7.5 unter Windows Server 2008 R2
 - Version 8.0 unter Windows Server 2012
 - Version 8.5 unter Windows Server 2012 R2
 - Version 10.0 unter Windows Server 2016

Der Webserver sollte auf keinem Endpunkt installiert werden, auf dem Anwendungen den IIS blockieren, da die Installation sonst fehlschlagen könnte. Weitere Informationen finden Sie in der Dokumentation des IIS.

HTTP-Port

Der Webserver hört den HTTP-Port auf agent-Anfragen ab und leitet diese an den OfficeScan Master Service weiter. Der Dienst sendet Informationen an agents auf dem

festgelegten agent-Kommunikationsport. Das Setup-Programm erzeugt bei der Installation eine zufällige Portnummer für die agent-Kommunikation.

SSL-Unterstützung

OfficeScan verwendet SSL (Secure Sockets Layer) für eine sichere Kommunikation zwischen der Webkonsole und dem Server. SSL bietet eine zusätzliche Schutzebene vor Hacker-Angriffen. Obwohl OfficeScan die in der Webkonsole festgelegten Kennwörter vor dem Versenden an den OfficeScan Server verschlüsselt, können Hacker das Paket auskundschaften und es ohne Entschlüsselung erneut senden, um Zugriff auf die Konsole zu erlangen. Im SSL-Tunnel ist das Paket bei der Weiterleitung über das Netzwerk vor Hacker-Übergriffen geschützt.

Die verwendete SSL-Version hängt von der Version ab, die der Webserver unterstützt.

Wenn Sie SSL auswählen, erstellt Setup automatisch ein für SSL-Verbindungen erforderliches SSL-Zertifikat. Das Zertifikat enthält Server-Angaben sowie einen öffentlichen und einen privaten Schlüssel.

Das SSL-Zertifikat sollte einen Gültigkeitszeitraum zwischen 1 und 20 Jahren haben. Der Administrator kann das Zertifikat auch nach Ablauf dieses Zeitraums verwenden. Es wird jedoch bei jedem Verbindungsaufbau mit diesem SSL-Zertifikat eine Warnmeldung angezeigt.

Der Ablauf einer SSL-Kommunikation:

1. Der Administrator sendet über die Webkonsole Daten per SSL-Verbindung an den Webserver.
2. Der Webserver antwortet der Webkonsole mit dem erforderlichen Zertifikat.
3. Der Browser führt die Schlüsselübergabe per RSA-Verschlüsselung durch.
4. Die Webkonsole sendet per RC4-Verschlüsselung Daten an den Webserver.

Die RSA-Verschlüsselung bietet zwar einen besonders wirksamen Schutz, verlangsamt jedoch den Kommunikationsfluss. Daher wird sie nur bei der Schlüsselübergabe eingesetzt. Die Datenweiterleitung wird über die schnellere Alternative RC4 verschlüsselt.

Webserver-Ports

Die folgende Tabelle enthält eine Liste der Standard-Portnummern für den Webserver.

TABELLE 2-2. Portnummern für den OfficeScan Webserver

WEBSERVER UND EINSTELLUNGEN	PORTS:	
	HTTP	HTTPS (SSL)
IIS Standard-Website mit aktiviertem SSL	80 (not configurable)	443 (not configurable)
IIS virtuelle Website mit aktiviertem SSL	8080 (configurable)	4343 (configurable)

Serverkennung

Trend Micro OfficeScan Installation-Programm

Serverkennung

Geben Sie an, ob OfficeScan Agents den Server über den Domänennamen oder die IP-Adresse ermitteln.

Trend Micro empfiehlt die Verwendung der IP-Adresse, wenn auf dem Server mehrere Netzwerkkarten vorhanden sind, und die Verwendung des vollqualifizierten Domänennamens (FQDN) oder Hostnames, wenn es sich bei der IP-Adresse um eine dynamisch zugewiesene Adresse handelt.

☐ Vollqualifizierter Domänenname (FQDN) oder Hostname:

☒ IP-Adresse:

Tipp: Überprüfen Sie, ob der Domänenname aufgelöst werden kann, bevor Sie den Vorgang fortsetzen.

InstallShield

ABBILDUNG 2-7. Das Fenster "Serverkennung"

Die in diesem Fenster gewählte Option betrifft nur eine remote durchgeführte Erstinstallation. Bei einem remote durchgeführten Upgrade verwendet OfficeScan die Einstellungen aus der Vorgängerversion.

Legen Sie fest, ob OfficeScan agents den Server über den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN), Host-Namen (Domäne) oder die IP-Adresse identifizieren.

Die Kommunikation zwischen dem Server und den agents ist von der angegebenen IP-Adresse abhängig. Wenn Sie die IP-Adresse ändern, können die agents nicht mehr mit dem OfficeScan Server kommunizieren. Die Kommunikation kann dann nur durch eine erneute Verteilung aller agents wiederhergestellt werden. Dasselbe gilt für den Fall, dass der Server-Computer über einen Host-Namen ermittelt und dieser Host-Name dann geändert wird.

In den meisten Netzwerken ändert sich eher die IP-Adresse als der Hostname des Server-Computers. Der Server-Computer sollte deshalb vorzugsweise über den Hostnamen identifiziert werden.



Tipp

Administratoren, die anstelle des Host-Namens die IP-Adresse verwenden, empfiehlt Trend Micro, die IP-Adresse (die vom DHCP-Server bezogen wurde) nach der Installation nicht zu ändern. Administratoren können weitere Kommunikationsprobleme mit OfficeScan Agents vermeiden, indem sie mit Hilfe derselben vom DHCP-Server bezogenen IP-Adressinformationen die IP-Adresskonfiguration (auf dem DHCP-Server) auf "Statisch" setzen.

Eine weitere Methode zur Beibehaltung der IP-Adresskonfiguration ist die ausschließliche Reservierung der IP-Adresse für den OfficeScan Server. Dadurch wird der DHCP-Server gezwungen, OfficeScan dieselbe IP-Adresse auch bei aktiviertem DHCP zuzuweisen.

Wenn Sie statische IP-Adressen verwenden, identifizieren Sie den Server über seine IP-Adresse. Sind außerdem mehrere Netzwerk-Schnittstellenkarten (NICs) auf dem Server vorhanden, sollte anstelle des Host-Namens eine entsprechende IP-Adresse verwendet werden, um eine erfolgreiche Kommunikation zwischen agent und Server zu gewährleisten.

IPv6-Unterstützung

Wenn der Server IPv4- und IPv6-agents verwaltet, muss er eine IPv4- und eine IPv6-Adresse aufweisen. Darüber hinaus müssen Administratoren den Server über seinen Host-Namen identifizieren. Wenn Administratoren den Server über seine IPv4-Adresse

identifizieren, können IPv6-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 Host-Namen oder seine IPv6-Adresse identifiziert werden. Wenn der Administrator den Server über seinen Host-Namen identifiziert, sollte er vorzugsweise den vollqualifizierten Domännennamen (FQDN) verwenden. Der Grund hierfür ist, dass ein WINS Server in einer reinen IPv6-Umgebung einen Hostnamen nicht in seine entsprechende IPv6-Adresse übersetzen kann.



Hinweis

Geben Sie den FQDN nur bei einer lokalen Installation des Servers an. Der FQDN wird für Remote-Installationen nicht unterstützt.

Registrierung und Aktivierung

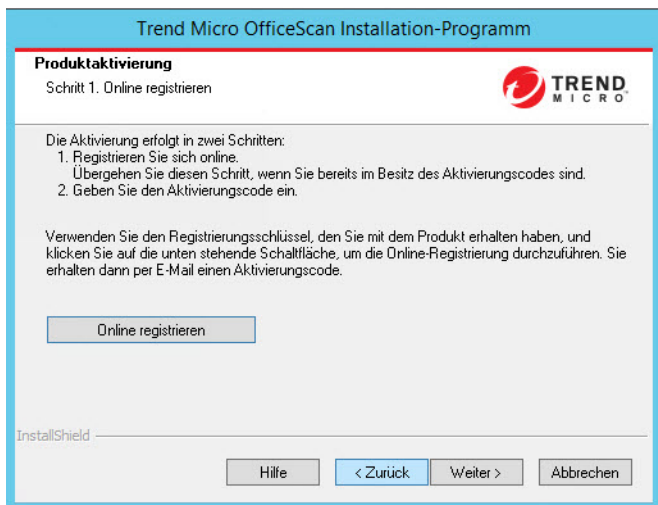


ABBILDUNG 2-8. Fenster "Produktaktivierung - Schritt 1"

Registrieren Sie OfficeScan über den Registrierungsschlüssel, den Sie mit dem Produkt erhalten haben. Die Aktivierungs-codes werden Ihnen anschließend zugesendet. Überspringen Sie diesen Schritt, falls die Aktivierungs-codes bereits zur Verfügung stehen.

Um die Aktivierungs-codes anzufordern, klicken Sie auf **Online-Registrierung**. Das Setup-Programm öffnet die Registrierungs-website von Trend Micro. Nachdem Sie das Registrierungsformular ausgefüllt haben, erhalten Sie von Trend Micro eine E-Mail mit den Aktivierungs-codes. Fahren Sie nach dem Erhalt der Codes mit dem Installationsvorgang fort.

Wenn Sie den OfficeScan Server auf einem reinen IPv6-Endpunkt installieren, richten Sie einen Dual-Stack-Proxy-Server ein, der IP-Adressen umwandeln kann. Auf diese Weise kann der Server erfolgreich eine Verbindung zur Registrierungs-website von Trend Micro herstellen.

ABBILDUNG 2-9. Fenster "Produktaktivierung - Schritt 2"

Geben Sie die Aktivierungs-codes ein. Achten Sie bei der Eingabe auf Groß- und Kleinschreibung.

Wenn der Aktivierungscode für alle Dienste gültig ist:

1. Geben Sie im Textfeld **Antivirus** den Aktivierungscode ein.
2. Wählen Sie **Verwenden Sie den gleichen Aktivierungscode für Damage Cleanup Services, für Web Reputation und für Anti-Spyware** aus.
3. Klicken Sie auf **Weiter**, und überprüfen Sie die Lizenzdaten.

OfficeScan Agent-Verteilung

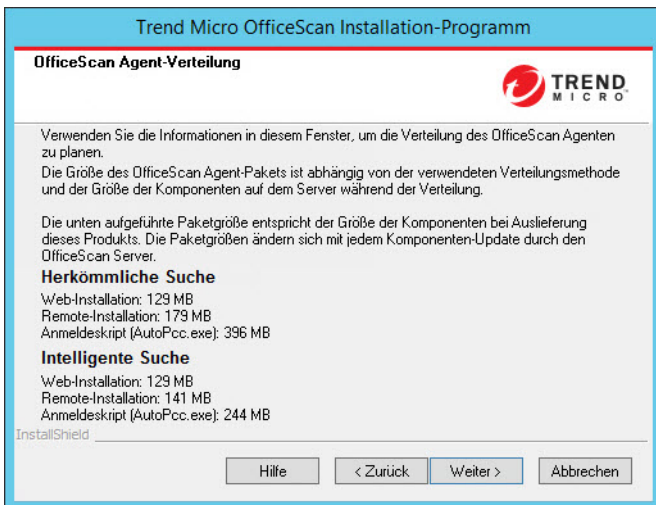


ABBILDUNG 2-10. Fenster "OfficeScan Agent-Verteilung"

Es gibt mehrere Methoden, um OfficeScan agents zu installieren oder zu aktualisieren. In diesem Fenster wird eine Liste der verschiedenen Verteilungsmethoden und der ungefähr erforderlichen Netzwerkbandbreite angezeigt.

Verwenden Sie dieses Fenster, um den auf den Servern benötigten Speicherplatz und die erforderliche Bandbreite für die Verteilung von agents auf die Ziel-Endpunkte abzuschätzen.

**Hinweis**

Für alle Installationsmethoden sind lokale Administrator- oder Domänenadministratorrechte auf den Ziel-Endpunkten erforderlich.

Integrierten Smart Protection Server installieren

**Hinweis**

Dieses Fenster wird nicht angezeigt, wenn Sie eine virtuelle IIS-Website während der Updateinstallationen verwenden.



ABBILDUNG 2-11. Das Fenster "Integrierten Smart Protection Server installieren"

Das Setup-Programm kann den integrierten Smart Protection Server auf dem Ziel-Endpunkt installieren. Der integrierte Server bietet File-Reputation-Dienste für agents mit intelligenter Suche sowie Web-Reputation-Dienste für agents, die den Web-Reputation-Richtlinien unterliegen. Sie können den integrierten Server über die OfficeScan Webkonsole verwalten.

Trend Micro empfiehlt die Installation des eigenständigen Smart Protection Servers, der über die gleichen Funktionen wie der integrierte Server verfügt, aber mehreren agents

dienen kann. Der eigenständige Server wird separat installiert und hat eine eigene Management-Konsole. Weitere Informationen zum eigenständigen Server finden Sie im *Trend Micro Smart Protection Server Administratorhandbuch*.

**Tip**

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. Weitere Informationen zum Konfigurieren von Smart Protection Quellen für Agents finden Sie im *Administratorhandbuch*.

Agent-Verbindungsprotokolle für File-Reputation-Dienste

OfficeScan Agents können sich über HTTP und HTTPS mit den File-Reputation-Diensten des integrierten Smart Protection Servers verbinden. HTTPS ermöglicht eine sicherere Verbindung, während HTTP weniger Bandbreite benötigt.

**Hinweis**

Wenn Endpunkte die Verbindung zum integrierten Server über einen Proxy-Server aufbauen, müssen die internen Proxy-Einstellungen über die Webkonsole konfiguriert werden. Weitere Informationen zum Konfigurieren von Proxy-Einstellungen finden Sie im *Administratorhandbuch*.

Die für File-Reputation-Dienste verwendeten Portnummern richten sich nach dem Webserver, den der OfficeScan Server verwendet. Weitere Informationen finden Sie unter [Webserver auf Seite 2-15](#).

Der HTTP-Port wird im Installationsfenster nicht angezeigt. Der HTTPS-Port wird angezeigt; seine Konfiguration ist jedoch optional.

TABELLE 2-3. Ports für die File-Reputation-Dienste des integrierten Smart Protection Servers

WEBSERVER UND EINSTELLUNGEN	PORTS FÜR FILE-REPUTATION-DIENSTE	
	HTTP	HTTPS (SSL)
IIS-Standard-Website	80	443
Virtuelle IIS-Website	8080	4343

Integrierter Server nicht installiert

Wenn Sie eine Erstinstallation durchführen und nicht ausgewählt haben, den integrierten Server zu installieren:

- Die herkömmliche Suche wird zur standardmäßigen Suchmethode.
- Wenn Sie die Web-Reputation-Richtlinien in einem separaten Installationsfenster aktivieren (ausführliche Hinweise finden Sie unter [Web-Reputation-Funktion auf Seite 2-39](#)), können agents keine Web-Reputation-Abfragen senden, da OfficeScan davon ausgeht, dass kein Smart Protection Server installiert wurde.

Falls ein eigenständiger Server nach der Installation von OfficeScan verfügbar ist, führen Sie die folgenden Aufgaben über die OfficeScan Webkonsole durch:

- Ändern Sie die Suchmethode in die intelligente Suche.
- Fügen Sie den eigenständigen Server zur Liste der Smart Protection Quellen hinzu, sodass agents File- und Web-Reputation-Abfragen an den Server senden können.

Bei der Aktualisierung von OfficeScan Servern der Version 10.x, bei denen der integrierte Server deaktiviert ist, wird der integrierte Server nicht installiert. OfficeScan Agents behalten die Suchmethoden und die Smart Protection Quellen bei, an die sie Abfragen senden.

Installationsziel

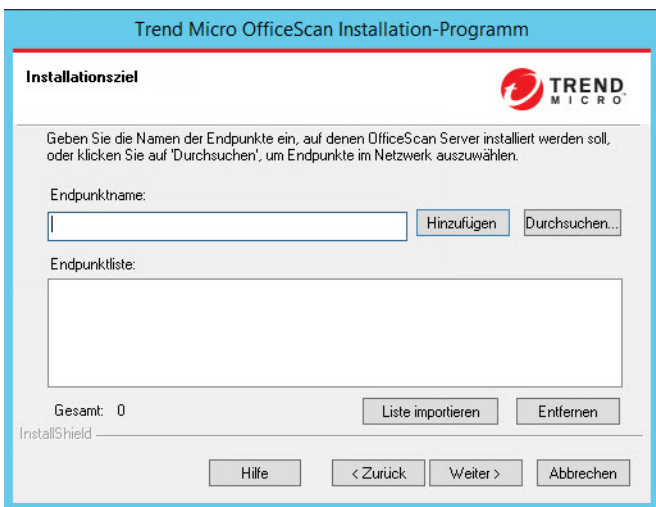


ABBILDUNG 2-12. Das Fenster "Installationsziel"

Geben Sie den Zielendpunkt an, auf dem OfficeScan installiert wird. Geben Sie manuell den Hostnamen oder die IP-Adresse des Endpunkts ein. Klicken Sie auf **Durchsuchen**, um nach Endpunkten im Netzwerk zu suchen.

Importieren Sie die Endpunktnamen aus einer Textdatei, indem Sie auf **Liste importieren** klicken. Wenn der OfficeScan Server auf mehreren Endpunkten gleichzeitig installiert wird und alle Endpunkte die Analyse erfolgreich durchlaufen, erfolgt die Installation nach der Reihenfolge der Endpunkte in der Textdatei.

In der Textdatei:

- Tragen Sie pro Zeile einen Endpunktnamen ein.
- Verwenden Sie das UNC-Format (Unified Naming Convention) (z. B. \\test).
- Verwenden Sie nur die folgenden Zeichen: a-z, A-Z, 0-9, Punkte (.) und Gedankenstriche (-).

Beispiel:

\\domäne1\test-abc

\\domain2\test-123

Hinweise zur Durchführung der Remote-Installation:

- Sie müssen auf dem Zielendpunkt über Administratorrechte verfügen.
- Notieren Sie sich den Host-Namen und die Anmeldedaten des Endpunkts (Benutzername und Kennwort).
- Stellen Sie sicher, dass die Zielendpunkte die Systemanforderungen für die Installation des OfficeScan Servers erfüllen.
- Stellen Sie sicher, dass auf dem Endpunkt Microsoft IIS Server 7.0 oder höher installiert ist, wenn er als Webserver eingesetzt wird.
- Der Endpunkt, auf dem Setup ausgeführt wird, darf nicht als Zielendpunkt angegeben werden. Starten Sie stattdessen die lokale Installation auf dem Endpunkt.

Klicken Sie nach der Angabe der Zielendpunkte auf **Weiter**. Das Setup-Programm überprüft, ob die angegebenen Endpunkte die Installationsvoraussetzungen von OfficeScan erfüllen.

Analyse des Zielpunkts

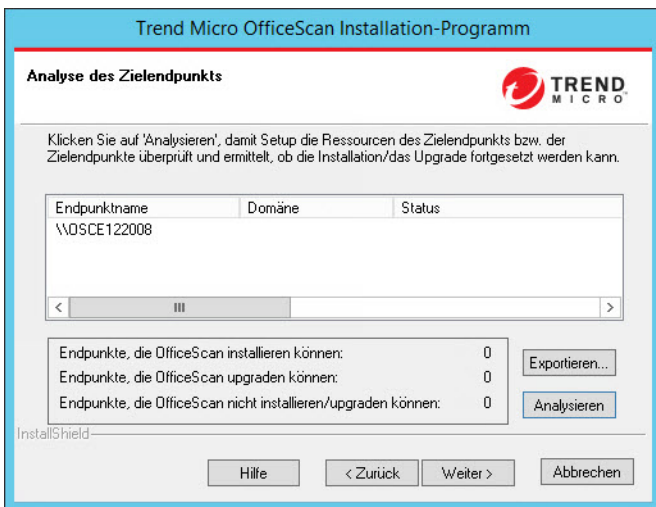


ABBILDUNG 2-13. Das Fenster "Analyse des Zielpunkts"



Wichtig

Das Setup-Programm unterstützt keine Remote-Upgrades von OfficeScan Servern, die den Apache Webserver verwenden. Sie müssen den Apache Webserver manuell deinstallieren, bevor Sie ein Remote-Upgrade von OfficeScan durchführen.

Vor der Durchführung der Remote-Installation muss das Setup-Programm überprüfen, ob der OfficeScan Server auf den ausgewählten Zielpunkten installiert werden kann. Starten Sie die Überprüfung durch Klicken auf **Analysieren**. Setup fordert Sie möglicherweise zur Eingabe des Administrator-Benutzernamens und -kennworts zur Anmeldung beim Zielpunkt auf. Nach der Analyse zeigt Setup das Ergebnis auf dem Bildschirm an.

**Wichtig**

Während der Serveranalyse werden Sie vom Setup-Programm aufgefordert, die Einstellungen für den Ransomware-Schutz zu aktualisieren, damit optimaler Schutz vor Ransomware-Bedrohungen gewährleistet ist.

Die Anwendung der aktualisierten Einstellungen wirkt sich nur auf Agents aus, die die Verhaltensüberwachung bereits aktiviert haben.

Bei der Installation auf mehreren Endpunkten wird die Installation fortgesetzt, wenn mindestens einer der Endpunkte die Voraussetzungen erfüllt. Das Setup-Programm installiert den OfficeScan Server auf diesem Endpunkt und ignoriert die Endpunkte, die die Analyse nicht erfolgreich durchlaufen haben.

Der Fortschritt der Remote-Installation wird nur auf dem Endpunkt angezeigt, auf dem Setup ausgeführt wird, und nicht auf den Zielpunkten.

OfficeScan Agent installieren

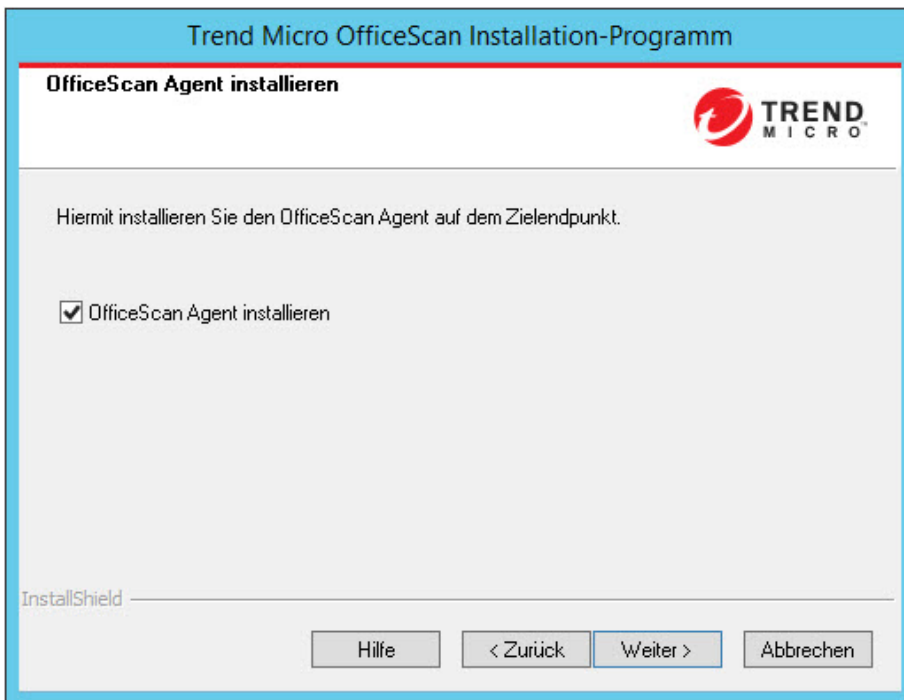


ABBILDUNG 2-14. Fenster "OfficeScan Agent installieren"

Installieren Sie den OfficeScan Agent auf dem Zielsever.

OfficeScan Agent

Das OfficeScan Agent Programm bietet Schutz vor Sicherheitsrisiken. Um den Endpunkt des OfficeScan Servers vor Sicherheitsrisiken zu schützen, wird auch das OfficeScan Agent Programm benötigt. Der Schutz des Servers ist automatisch gewährleistet, wenn Sie den OfficeScan Agent zusammen mit dem Server installieren. Darüber hinaus entfällt die Notwendigkeit, den OfficeScan Agent im Anschluss an die Serverinstallation zu installieren.



Hinweis

Installieren Sie den OfficeScan Agent nach der Installation des Servers auf anderen Endpunkten im Netzwerk. Weitere Informationen zu den OfficeScan Agent-Installationsmethoden finden Sie im *Administratorhandbuch*.

Ist Endpunkt-Sicherheitssoftware von Trend Micro oder Drittanbietern auf dem Server installiert, kann OfficeScan diese Software unter Umständen nicht automatisch deinstallieren und durch den OfficeScan Agent ersetzen. Eine Liste der Programme, die von OfficeScan automatisch deinstalliert werden, erhalten Sie von Ihrem Support-Anbieter. Software, die nicht automatisch deinstalliert werden kann, muss manuell deinstalliert werden, damit die Installation von OfficeScan fortgesetzt werden kann.

Smart Protection Network

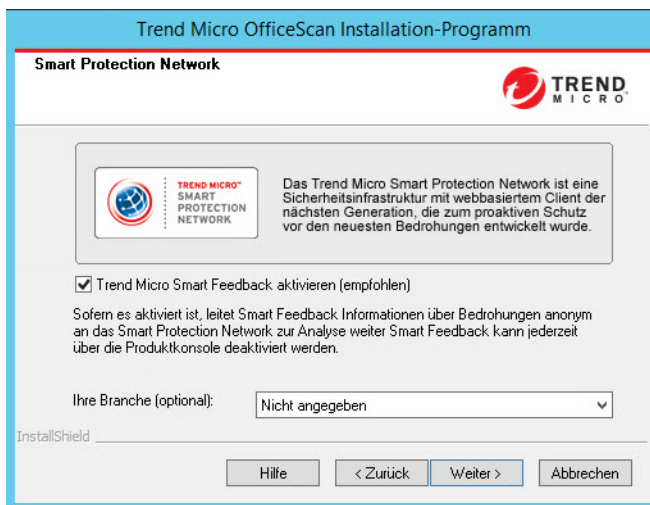


ABBILDUNG 2-15. Das Fenster "Smart Protection Network"

Trend Micro™ Smart Protection Network ist eine Content-Sicherheitsinfrastruktur mit einem webbasierten Client der nächsten Generation, die zum Schutz der Kunden vor Sicherheitsrisiken und Internetbedrohungen eingesetzt wird. Sie umfasst sowohl lokale

als auch gehostete Lösungen und bietet Benutzern umfassenden Schutz im Netzwerk, zu Hause oder unterwegs. Über schlanke agents erhalten die Benutzer Zugriff auf eine einzigartige Kombination aus E-Mail-, Web- und File-Reputation-Technologien und 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 einer Art "Nachbarschaftsschutz" in Echtzeit. Die Smart Protection Network Lösung nutzt das Smart Protection Network für webbasierten Schutz.

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/>

Kennwort für das Administratorkonto

Trend Micro OfficeScan Installation-Programm

Kennwort für das Administratorkonto



Geben Sie die Kennwörter für das Öffnen der Webkonsole oder das Beenden/Deinstallieren des OfficeScan Agenten an. Durch ein Kennwort wird die nicht autorisierte Änderung von Einstellungen der Webkonsole oder das Entfernen des OfficeScan Agenten verhindert.

Kennwort der Webkonsole:

Konto:

Kennwort:

Kennwort bestätigen:

Kennwort zum Beenden und Deinstallieren des OfficeScan Agenten:

Kennwort:

Kennwort bestätigen:

InstallShield

Hilfe < Zurück Weiter > Abbrechen

ABBILDUNG 2-16. Das Fenster "Kennwort für das Administratorkonto"

Geben Sie die Kennwörter für den Zugriff auf die Webkonsole sowie zum Beenden und Deinstallieren des OfficeScan Agents an.

Auf die Webkonsole zugreifen

Setup erstellt während der Installation ein Root-Konto. Das Root-Konto hat Vollzugriff auf alle Funktionen der OfficeScan Webkonsole. Darüber hinaus ermöglicht eine Anmeldung über dieses Konto dem Administrator, benutzerdefinierte Benutzerkonten zu erstellen, mit denen sich andere Benutzer an der Webkonsole anmelden können. Benutzer können eine oder mehrere Webkonsolenfunktionen konfigurieren oder anzeigen, je nach Zugriffsberechtigung ihres Benutzerkontos.

Geben Sie ein Kennwort an, das nur den OfficeScan Administratoren bekannt ist. Wenn Sie Hilfe zum Zurücksetzen eines vergessenen Kennworts benötigen, wenden Sie sich an Ihren Support-Anbieter.

Beenden und Deinstallieren des OfficeScan Agents

Legen Sie ein Kennwort fest, um unberechtigtes Deinstallieren oder Beenden des OfficeScan Agents zu verhindern. Deinstallieren oder beenden Sie den agent nur, wenn Probleme mit agent-Funktionen auftreten und installieren/starten Sie den Agent sofort neu.

Installation des OfficeScan Agents

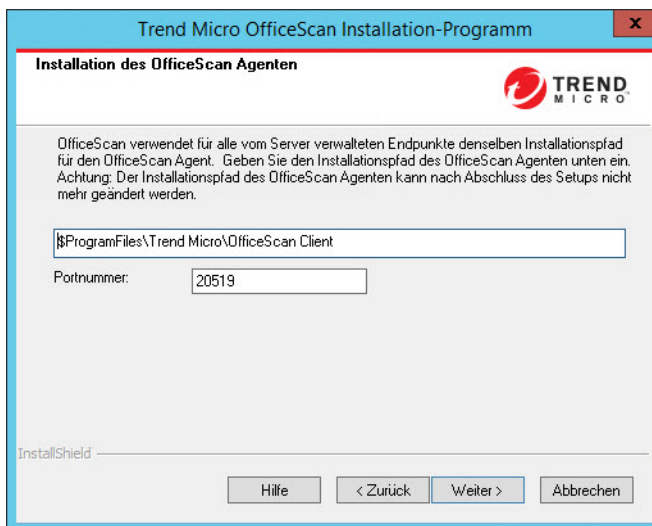


ABBILDUNG 2-17. Fenster „Installation des OfficeScan Agents“

Übernehmen Sie die Standardeinstellungen der agent-Installation oder legen Sie einen anderen Installationspfad für den OfficeScan Agent fest. Ändern Sie den Pfad, wenn im Installationsverzeichnis nicht genügend Speicherplatz vorhanden ist.



Tipp

Trend Micro empfiehlt die Verwendung der Standardeinstellungen.

Falls Sie einen anderen Installationspfad festlegen, geben Sie einen statischen Pfad ein, oder verwenden Sie Variablen. Falls der angegebene Pfad ein Verzeichnis enthält, das auf dem agent nicht vorhanden ist, erstellt das Setup-Programm das Verzeichnis automatisch während der agent-Installation.

Wenn Sie einen statischen Installationspfad für den OfficeScan Agent verwenden möchten, geben Sie den Pfad des Laufwerks sowie den Laufwerksbuchstaben ein. Beispiel: C:\Programme\Trend Micro\OfficeScan Agent.

**Hinweis**

Nach Abschluss der Installation des OfficeScan Servers kann der Installationspfad des OfficeScan Agents nicht mehr geändert werden. Alle installierten OfficeScan Agents verwenden denselben Installationspfad.

Sie können folgende Variablen für den Installationspfad des OfficeScan Agents verwenden:

- `$BOOTDISK`: Der Laufwerksbuchstabe der Festplatte, von der der Endpunkt gestartet wird (standardmäßig C:\).
- `$WINDIR`: Das Windows Verzeichnis (standardmäßig C:\Windows).
- `$ProgramFiles`: Das Verzeichnis "Programme", das in Windows automatisch eingerichtet wird und in dem die Software standardmäßig installiert wird (standardmäßig C:\Programme).

Konfigurieren Sie Folgendes im selben Fenster:

- **Portnummer**: Der OfficeScan Server verwendet diese vom Setup-Programm nach dem Zufallsprinzip erzeugte Portnummer bei der Kommunikation mit den Agents. Übernehmen Sie den Standardwert, oder geben Sie einen anderen Wert ein.
- **Sicherheitsstufe**: Ändern Sie nach der Installation von OfficeScan die Sicherheitsstufe über die OfficeScan Konsole.

Navigieren Sie zu **Agents > Agent-Verwaltung**. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen > Andere Einstellungen**.

- **Normal**: Diese Berechtigung gewährt allen Benutzern (der Benutzergruppe „Alle“) Vollzugriff auf das Programmverzeichnis des Agents und die Registrierungseinträge des Agents.
- **Hoch**: Das Installationsverzeichnis des Agents übernimmt die Rechte des Ordners `Programme`, und die Registrierungseinträge des Agents übernehmen die Berechtigungen des Schlüssels `HKLM\Software`. Dies schränkt die Berechtigungen von „normalen“ Benutzern (Benutzern ohne Administratorrechte) für die meisten Active-Directory-Konfigurationen auf einen Lesezugriff ein.

OfficeScan Firewall

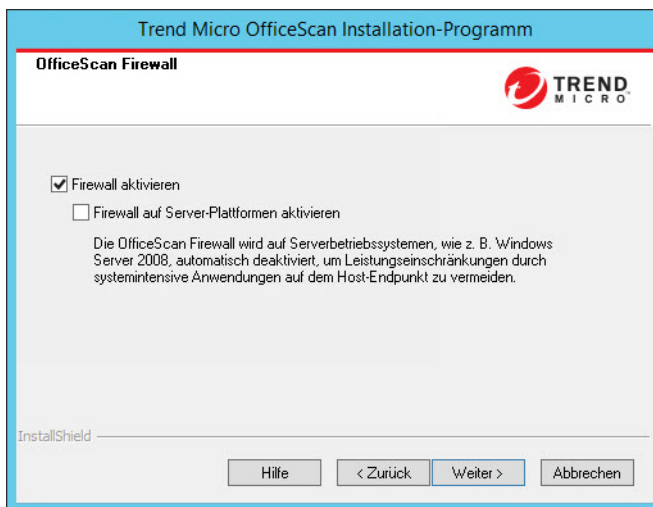


ABBILDUNG 2-18. Fenster „OfficeScan Firewall“

Dieses Fenster wird nur bei aktiviertem Virenschutz angezeigt.

OfficeScan Firewall

Die OfficeScan Firewall schützt agents und Server im Netzwerk mit Hilfe von Stateful-Inspection-Technologie und leistungsstarken Funktionen zur Virensuche und -bekämpfung. Sie können Regeln erstellen, um Verbindungen nach IP-Adresse, Portnummer oder Protokoll zu filtern, und anschließend die Regeln auf unterschiedliche Benutzergruppen anwenden.

Optional können Sie die Firewall deaktivieren und später erneut auf der Webkonsole des OfficeScan Servers aktivieren.

Optional können Sie die Firewall auf Server-Plattformen aktivieren. Wenn Sie ein Upgrade durchführen und der Firewall-Dienst bereits auf den Serverplattformen aktiviert ist, wählen Sie **Firewall auf Server-Plattformen aktivieren**, damit der Firewall-Dienst nach dem Upgrade nicht von OfficeScan deaktiviert wird.

Anti-Spyware-Funktion

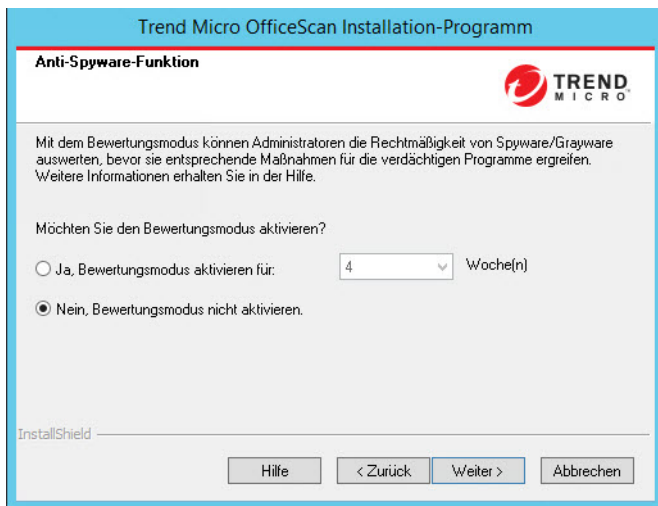


ABBILDUNG 2-19. Das Fenster "Anti-Spyware-Funktion"

Dieses Fenster wird nur bei aktiviertem Web-Reputation- und Anti-Spyware-Dienst angezeigt.

Im Bewertungsmodus protokollieren alle vom Server verwalteten agents Spyware/Grayware, die bei der manuellen, zeitgesteuerten und Echtzeitsuche sowie bei der Funktion "Jetzt durchsuchen" gefunden wurde. Die Spyware-/Grayware-Komponenten werden dabei jedoch nicht bereinigt. Bei der Säuberung werden Prozesse beendet oder Registrierungseinträge, Dateien, Cookies und Shortcuts gelöscht.

Mit dem Bewertungsmodus von Trend Micro können Sie Elemente überprüfen, die von Trend Micro als Spyware/Grayware eingestuft werden. Administratoren können dann eine geeignete Aktion konfigurieren. Sie können beispielsweise als Sicherheitsrisiko erkannte Spyware/Grayware zur Liste der zugelassenen Spyware/Grayware hinzufügen.

Weitere Informationen zu empfohlenen Aktionen im Bewertungsmodus finden Sie nach der Installation im *Administratorhandbuch*.

Konfigurieren Sie den Bewertungsmodus so, dass er jeweils nur für einen bestimmten Zeitraum gültig ist, indem Sie in diesem Fenster die Anzahl der Wochen angeben. Nach

der Installation können Sie die Einstellungen des Bewertungsmodus auf der Webkonsole ändern (**Agents > Globale Agent-Einstellungen**, Abschnitt **Spyware-/Grayware-Einstellungen**).

Web-Reputation-Funktion

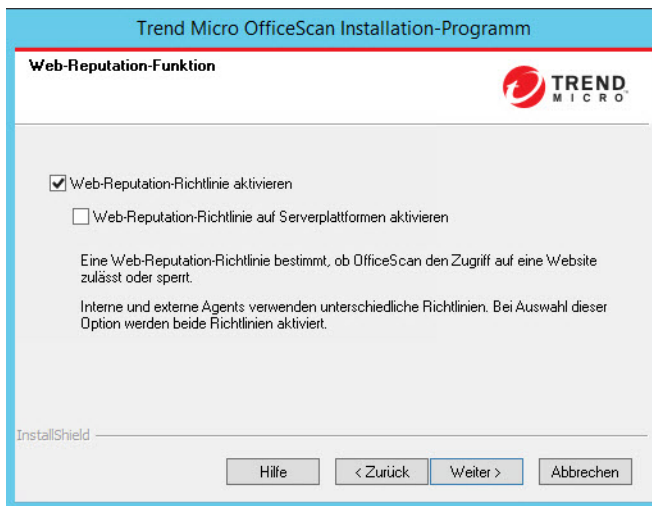


ABBILDUNG 2-20. Das Fenster "Web-Reputation-Funktion"

Mit Web-Reputation-Richtlinien wird angegeben, ob OfficeScan den Zugriff auf eine Website zulässt oder sperrt. Weitere Informationen zu Richtlinien finden Sie im *Administratorhandbuch*.

Wenn Sie die Option **Web-Reputation-Richtlinie aktivieren** auswählen, werden Richtlinien für interne und externe agents aktiviert, die auf Desktop-Plattformen installiert sind, wie z. B. Windows XP, Vista, Windows 7, Windows 8 und Windows 8.1. Wählen Sie die Option **Web-Reputation-Richtlinie auf &Serverplattformen aktivieren**, wenn Serverplattformen wie Windows Server 2003, Windows Server 2008 und Windows Server 2012 denselben Grad an Schutz vor Internet-Bedrohungen erfordern wie Desktop-Plattformen.

OfficeScan Agents ermitteln ihren Standort und die anzuwendende Richtlinie anhand der Standortkriterien, die in der Webkonsole im Fenster **Endpunktspeicherort** festgelegt wurden. OfficeScan Agents ändern die Richtlinien bei jedem Standortwechsel.

Konfigurieren Sie die Einstellungen für Web-Reputation-Richtlinien nach der Installation über die Webkonsole. OfficeScan Administratoren konfigurieren in der Regel eine strengere Richtlinie für externe agents.

Bei Web-Reputation-Richtlinien handelt es sich um detaillierte Einstellungen in der OfficeScan agent-Hierarchie. Erzwingen Sie bestimmte Richtlinien für alle agents, agent-Gruppen oder einzelne agents.

Wenn Sie Web-Reputation-Richtlinien aktivieren, müssen Sie Smart Protection Server (integriert oder eigenständig) installieren und zur Liste der Smart Protection Quellen in der OfficeScan Webkonsole hinzufügen. OfficeScan Agents senden Web-Reputation-Abfragen an die Server, um die Sicherheit von Websites zu überprüfen, auf die Benutzer zugreifen.

**Hinweis**

Der integrierte Server wird mit dem OfficeScan Server installiert. Weitere Informationen finden Sie unter *[Integrierten Smart Protection Server installieren auf Seite 2-23](#)*. Der eigenständige Server wird separat installiert.

Serverauthentifizierungszertifikat

Das Setup-Programm versucht, bisher vorhandene Authentifizierungszertifikate während der Installation zu entdecken. Ist bereits ein Zertifikat vorhanden, ordnet OfficeScan die Datei automatisch im Fenster **Serverauthentifizierungszertifikat** zu. Wenn kein Zertifikat vorhanden ist, verwendet OfficeScan standardmäßig die Option **Neues Authentifizierungszertifikat generieren**.

**Hinweis**

Während der Durchführung von Upgrade-Installationen über einen Remote-Standort wird das Fenster **Serverauthentifizierungszertifikat** nur angezeigt, wenn ein OfficeScan 10.6 SP3 Server aktualisiert wird.

Trend Micro OfficeScan Installation-Programm

Serverauthentifizierungszertifikat



Erlauben Sie OfficeScan, ein neues Zertifikat für die Kommunikation mit OfficeScan Agenten zu generieren, oder importieren Sie ein vorhandenes Zertifikat.
Hinweis: OfficeScan erstellt eine Sicherung des neuen oder importierten Zertifikats im Ordner <Server_installation_folder>\AuthCertBackup\.

☒ Neues Authentifizierungszertifikat generieren

Sicherungskennwort:

Kennwort bestätigen:

☐ Vorhandenes Zertifikat importieren

Hinweis: Bei dem Zertifikat handelt es sich entweder um ein ZIP-Paket, das vom Zertifikat-Manager für Serverauthentifizierung generiert wurde, oder eine korrekt formatierte PFX-Datei.

Kennwort:

InstallShield

ABBILDUNG 2-21. Fenster "Serverauthentifizierungszertifikat" für neue Zertifikate

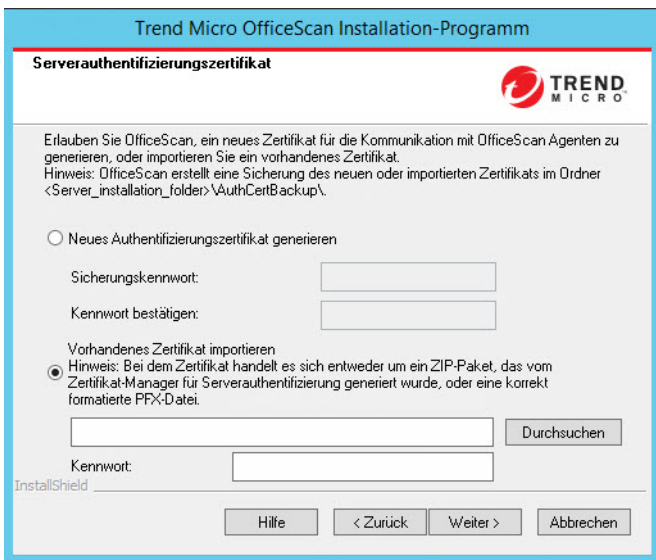


ABBILDUNG 2-22. Fenster "Serverauthentifizierungszertifikat" für bisher vorhandene Zertifikate

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.

OfficeScan kann das Authentifizierungszertifikat während der Installation erzeugen. Alternativ können Administratoren ein bereits vorhandenes Authentifizierungszertifikat von einem anderen OfficeScan Server importieren.



Tipp

Trend Micro empfiehlt, das Zertifikat beim Sichern mit einem Kennwort zu verschlüsseln.

OfficeScan Programmverknüpfungen

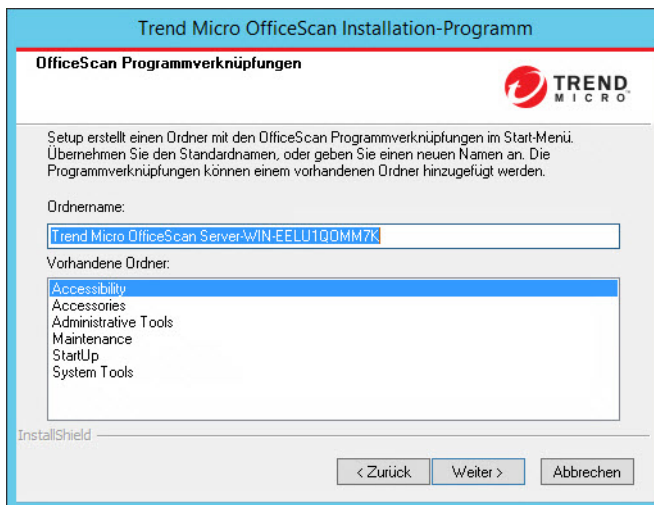


ABBILDUNG 2-23. Fenster "OfficeScan Programmverknüpfungen"

Übernehmen Sie den Standard-Ordernamen, oder geben Sie einen neuen Namen an. Sie können auch einen bereits vorhandenen Ordner auswählen, zu dem Setup die Programmverknüpfungen hinzufügt.

Installationsdaten

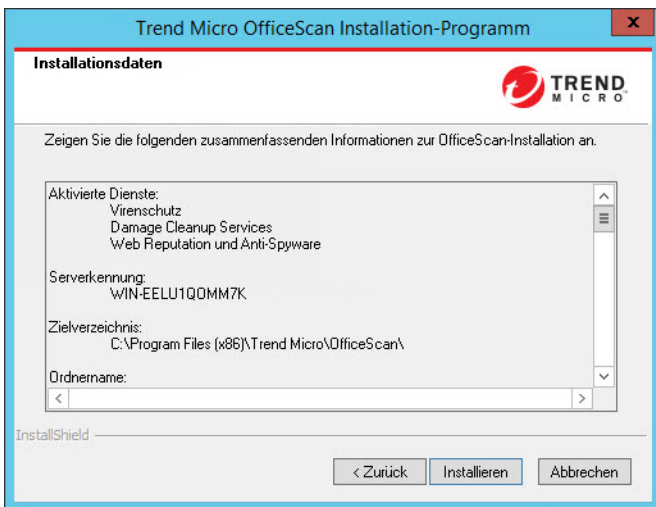


ABBILDUNG 2-24. Das Fenster mit den Installationsdaten

In diesem Fenster finden Sie eine Zusammenfassung der Installationseinstellungen. Überprüfen Sie die Installationsdaten, und klicken Sie auf **Zurück**, um Einstellungen oder Optionen zu ändern. Klicken Sie auf **Installieren**, um die Installation zu starten.

Der InstallShield Wizard ist abgeschlossen.

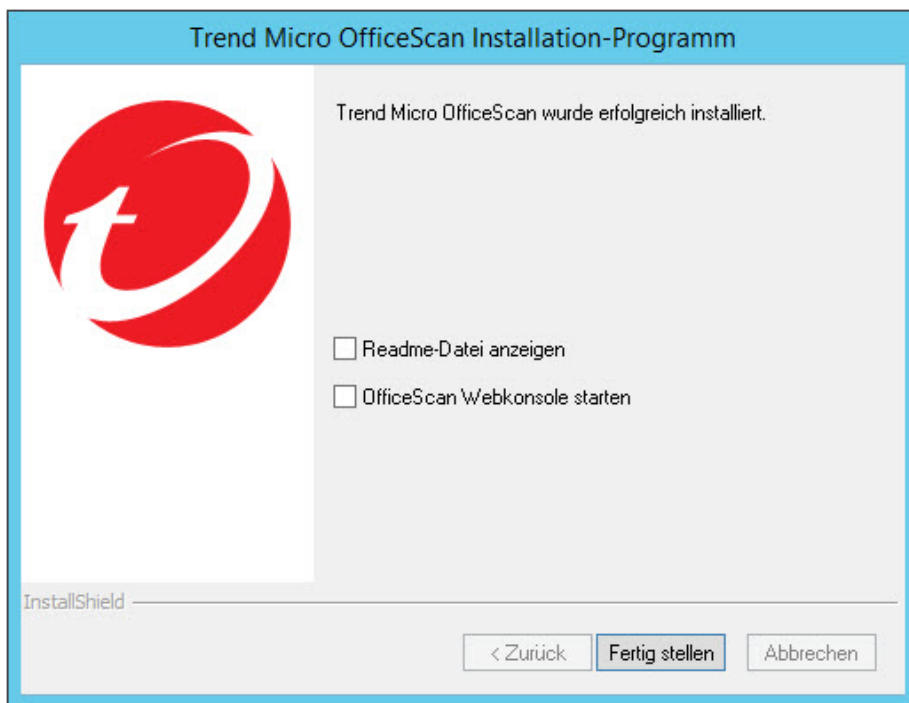


ABBILDUNG 2-25. Fenster "Der InstallShield Wizard ist abgeschlossen"

Lesen Sie nach Abschluss der Installation die Readme-Datei mit allgemeinen Informationen zum Produkt und den bekannten Problemen.

Administratoren können die Webkonsole starten, um die OfficeScan Einstellungen zu konfigurieren.

Kapitel 3

OfficeScan upgraden

In diesem Kapitel werden die Schritte für die Aktualisierung von Trend Micro™ OfficeScan™ beschrieben.

Themen in diesem Kapitel:

- *Aktualisieren des OfficeScan Servers und der Agents auf Seite 3-2*
- *Durchführen eines lokalen Upgrades auf Seite 3-21*
- *Durchführen eines Remote-Upgrades auf Seite 3-62*

Aktualisieren des OfficeScan Servers und der Agents

Wenn Sie das Setup-Programm auf einem zuvor konfigurierten OfficeScan Server der Version 10.x oder 11.x ausführen, wird der Server aktualisiert. Wenn auf einem Endpunkt Plug-in Manager installiert ist, aktualisiert Setup auch Plug-in Manager auf Version 2.3. Wenn Plug-in Manager nicht installiert ist, wird automatisch Version 2.3 installiert. Diese Version von Plug-in Manager stellt die Widget-Funktionalität in OfficeScan bereit.

Wenn der OfficeScan Server den Agents die Berechtigung erteilt, ein Upgrade für das OfficeScan Agent-Programm durchzuführen, aktualisiert das Installationspaket alle Agents direkt nach dem Upgrade des Servers.

Wenn der OfficeScan Server Agent-Upgrades sperrt, verarbeiten Sie je nach Netzwerkbandbreite und Anzahl der vom OfficeScan Server verwalteten Agents die Agent-Upgrades gruppenweise.



Tip

Trend Micro empfiehlt dringend einen Neustart der OfficeScan Agents nach dem Upgrade, um sicherzustellen, dass alle OfficeScan Komponenten aktualisiert wurden.

Vor dem Upgrade des OfficeScan Servers und der Agents

Beachten Sie Folgendes, bevor Sie ein Upgrade des OfficeScan Servers und der Agents durchführen:

1. Das Installationspaket enthält Updates für OfficeScan Firewall-Treiber. Ist die OfficeScan Firewall in der aktuellen OfficeScan Version aktiviert, kann es beim Verteilen des Pakets zu folgenden Störungen des Agent-Endpunkts kommen:
 - Beim Start des Updates für den Treiber für die allgemeine Firewall werden die Agent-Endpunkte vorübergehend vom Netzwerk getrennt. Die Benutzer werden vor der Verbindungstrennung nicht benachrichtigt.

Durch eine standardmäßig aktivierte Option in der OfficeScan Webkonsole wird das Update des Treibers für die allgemeine Firewall erst nach dem

Neustart des Agent-Endpunkts durchgeführt. Stellen Sie sicher, dass diese Option aktiviert ist, um Probleme wegen der unterbrochenen Verbindung zu vermeiden.

So überprüfen Sie den Status dieser Option:

- a.
 - Navigieren Sie für OfficeScan 10.x Versionen zu **Netzwerkcomputer > Allgemeine Client-Einstellungen**.
 - Navigieren Sie für OfficeScan 11.x Versionen zu **Agents > Globale Agent-Einstellungen**.
- b. Gehen Sie zum Abschnitt **Firewall-Einstellungen**. Die Option lautet **OfficeScan Firewall-Treiber nur nach einem Neustart des Systems aktualisieren**
- Nach der Verteilung des Pakets ist auf dem Agent-Endpunkt noch die Vorgängerversion des OfficeScan TDI-Treibers vorhanden. Die neue Version wird erst beim Neustart des Endpunkts geladen. Wird der Neustart des OfficeScan Agents nicht sofort ausgeführt, treten wahrscheinlich Probleme auf.

Ist in der Webkonsole die Option zur Anzeige der Neustartbenachrichtigung aktiviert, werden die Benutzer zum Neustart aufgefordert. Entscheidet sich der Benutzer, den Neustart zu einem späteren Zeitpunkt vorzunehmen, wird keine weitere Benachrichtigung angezeigt. Bei deaktivierter Option erfolgt keinerlei Benachrichtigung.

Die Option zur Anzeige der Neustartbenachrichtigung ist standardmäßig aktiviert. So überprüfen Sie den Status dieser Option:

- Für OfficeScan 10.x Versionen:
 - a. Navigieren Sie zu **Netzwerkcomputer > Allgemeine Client-Einstellungen**.
 - b. Navigieren Sie zum Abschnitt **Alarmeinstellungen**. Die Option lautet **Eine Benachrichtigung anzeigen, wenn der Client-Computer zum Laden eines Kernetreibers neu gestartet werden muss**.

- Für OfficeScan 11.x Versionen:
 - a. Navigieren Sie zu **Agents > Globale Agent-Einstellungen**.
 - b. Navigieren Sie zum Abschnitt **Alarmeinstellungen**. Die Option lautet **Eine Benachrichtigung anzeigen, wenn der Endpunkt zum Laden eines Kernaltreibers neu gestartet werden muss**.
- 2. Der OfficeScan Server kann nicht auf diese Version upgraden, wenn:
 - Der Agent während des Server-Upgrades das Anmeldeskript-Setup (`AutoPcc.exe`) ausführt. Stellen Sie vor dem Upgrade des Servers sicher, dass kein Agent das Anmeldeskript ausführt.
 - Der Server führt zurzeit datenbankbezogene Aufgaben aus. Überprüfen Sie vor dem Upgrade den Status der OfficeScan Datenbank (`DbServer.exe`). Öffnen Sie z. B. den Windows Task-Manager, und überprüfen Sie, ob die Prozessorauslastung für `DbServer.exe` 00 beträgt. Ist die Auslastung höher, warten Sie, bis Sie wieder auf 00 sinkt. Dies zeigt an, dass alle datenbankbezogenen Aufgaben abgeschlossen sind. Wenn beim Upgrade Probleme auftreten, könnten möglicherweise gesperrte Datenbankdateien die Ursache dafür sein. Starten Sie in diesem Fall den Server-Computer neu, damit die Dateien entsperrt werden, und wiederholen Sie anschließend das Upgrade.

Verwenden Sie eine der folgenden Upgrade-Methoden:

- *Upgrade-Methode 1: Automatisches Agent-Upgrade deaktivieren auf Seite 3-4*
- *Upgrade-Methode 2: Update-Agents aktualisieren auf Seite 3-7*
- *Upgrade-Methode 3: Agents auf den OfficeScan XG Server verschieben auf Seite 3-15*
- *Upgrade-Methode 4: Das automatische Agent-Upgrade aktivieren auf Seite 3-18*

Upgrade-Methode 1: Automatisches Agent-Upgrade deaktivieren

Wenn Sie das automatische Agent-Upgrade deaktivieren, können Sie zuerst das Upgrade des Servers durchführen und im Anschluss daran die Agents gruppenweise aktualisieren.

Verwenden Sie diese Upgrade-Methode, wenn Sie eine große Zahl von Agents upgraden müssen.

Teil 1: Update-Einstellungen auf dem OfficeScan Server konfigurieren

Prozedur

- Für OfficeScan 10.x Server:
 - a. Navigieren Sie zu **Netzwerkcomputer > Client-Verwaltung**.
 - b. Klicken Sie in der Client-Struktur auf das Symbol der Root-Domäne () , um alle Clients auszuwählen.
 - c. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.
 - d. Wählen Sie **Clients können Komponenten aktualisieren, aber kein Upgrade des Client-Programms durchführen oder Hotfixes verteilen** aus.
 - e. Klicken Sie auf **Für alle Clients übernehmen**.



Tipp

Die Verteilung der Einstellungen auf Online-Clients kann etwas Zeit in Anspruch nehmen, wenn Sie über eine komplexe Netzwerkumgebung und eine große Anzahl an Clients verfügen. Planen Sie vor dem Upgrade genügend Zeit für die Verteilung der Einstellungen auf alle Clients ein. OfficeScan Clients, die die Einstellungen nicht übernehmen, führen automatisch ein Upgrade durch.

- Für OfficeScan 11.x Server:
 - a. Navigieren Sie zu **Agents > Agent-Verwaltung**.
 - b. Klicken Sie in der Agent-Ansicht auf das Symbol der Root-Domäne () , um alle Agents auszuwählen.
 - c. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.

- d. Wählen Sie die Option **OfficeScan Agents können Komponenten aktualisieren, aber kein Upgrade des Agent-Programms durchführen oder Hotfixes verteilen** aus.
- e. Klicken Sie auf **Auf alle Agents anwenden**.

Es kann etwas dauern, die Einstellungen auf eine große Anzahl von Agents sowie auf Online-Agents in einer komplexen Netzwerkumgebung zu verteilen. Planen Sie vor dem Upgrade genügend Zeit für die Verteilung der Einstellungen auf alle Agents ein. OfficeScan Agents, die die Einstellungen nicht übernehmen, werden automatisch aktualisiert.

Teil 2: Upgrade des OfficeScan Servers

Weitere Informationen zum Aktualisieren des OfficeScan Servers finden Sie unter *Durchführen eines lokalen Upgrades auf Seite 3-21* oder *Durchführen eines Remote-Upgrades auf Seite 3-62*.



Hinweis

Zur Beschleunigung des Upgrade-Prozesses beenden Sie den OfficeScan Agent, bevor Sie ein OfficeScan Server aktualisieren, auf dem Windows Server 2008 Standard 64-Bit ausgeführt wird.

Konfigurieren Sie sofort nach Abschluss der Installation und vor dem Upgrade der Agents die Einstellungen des OfficeScan Servers über die Webkonsole.

Ausführliche Anweisungen zur Konfiguration von OfficeScan Einstellungen finden Sie im *Administratorhandbuch* oder in der *OfficeScan Server-Hilfe*.

Teil 3: OfficeScan Agenten aktualisieren

Prozedur

1. Navigieren Sie zu **Updates > Agents > Automatisches Update** und stellen Sie sicher, dass die folgenden Optionen aktiviert sind:

- **Komponenten-Update auf den Agents sofort nach dem Download einer neuen Komponente auf dem OfficeScan Server starten**
 - **Agents beginnen nach dem Neustart und dem Herstellen einer Verbindung zum OfficeScan Server mit dem Komponenten-Update (mit Ausnahme unabhängiger Agents)**
2. Navigieren Sie zu **Agents > Agent-Verwaltung**.
 3. Wählen Sie in der Agent-Hierarchie die Agents aus, bei denen Sie ein Upgrade durchführen möchten. Sie können eine oder mehrere Domänen bzw. einzelne oder alle Agents innerhalb einer Domäne auswählen.
 4. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.
 5. Deaktivieren Sie die Option **OfficeScan Agents können Komponenten aktualisieren, aber kein Upgrade des Agents durchführen oder Hotfixes verteilen**.
 6. Klicken Sie auf **Speichern**.
 7. Prüfen Sie die Upgrade-Ergebnisse.
 - *[Online-Agents auf Seite 3-13](#)*
 - *[Offline-Agents auf Seite 3-14](#)*
 - *[Unabhängige \(Roaming-\) Agents auf Seite 3-15](#)*
 8. Führen Sie einen Neustart der Agent-Endpunkte durch, um das Upgrade der Agents abzuschließen.
 9. Wiederholen Sie Schritt 2 bis Schritt 8, bis das Upgrade für alle Agents durchgeführt wurde.

Upgrade-Methode 2: Update-Agents aktualisieren

Verwenden Sie diese Upgrade-Methode, wenn Sie eine große Zahl von Agents über Update-Agents aktualisieren müssen. Diese Agents führen das Upgrade über ihre entsprechenden Update-Agents durch.

OfficeScan Agents, die nicht über Update-Agents aktualisiert werden, führen das Upgrade über den OfficeScan Server durch.

Teil 1: Update-Einstellungen auf dem OfficeScan Server konfigurieren

Prozedur

- Für OfficeScan 10.x Server:
 - a. Navigieren Sie zu **Netzwerkcomputer > Client-Verwaltung**.
 - b. Klicken Sie in der Client-Struktur auf das Symbol der Root-Domäne () , um alle Clients auszuwählen.
 - c. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.
 - d. Wählen Sie **Clients können Komponenten aktualisieren, aber kein Upgrade des Client-Programms durchführen oder Hotfixes verteilen** aus.
 - e. Klicken Sie auf **Für alle Clients übernehmen**.



Tipp

Die Verteilung der Einstellungen auf Online-Clients kann etwas Zeit in Anspruch nehmen, wenn Sie über eine komplexe Netzwerkumgebung und eine große Anzahl an Clients verfügen. Planen Sie vor dem Upgrade genügend Zeit für die Verteilung der Einstellungen auf alle Clients ein. OfficeScan Clients, die die Einstellungen nicht übernehmen, führen automatisch ein Upgrade durch.

- Für OfficeScan 11.x Server:
 - a. Navigieren Sie zu **Agents > Agent-Verwaltung**.
 - b. Klicken Sie in der Agent-Ansicht auf das Symbol der Root-Domäne () , um alle Agents auszuwählen.
 - c. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.

- d. Wählen Sie die Option **OfficeScan Agents können Komponenten aktualisieren, aber kein Upgrade des Agent-Programms durchführen oder Hotfixes verteilen** aus.
- e. Klicken Sie auf **Auf alle Agents anwenden**.

Es kann etwas dauern, die Einstellungen auf eine große Anzahl von Agents sowie auf Online-Agents in einer komplexen Netzwerkumgebung zu verteilen. Planen Sie vor dem Upgrade genügend Zeit für die Verteilung der Einstellungen auf alle Agents ein. OfficeScan Agents, die die Einstellungen nicht übernehmen, werden automatisch aktualisiert.

Teil 2: Upgrade des OfficeScan Servers

Weitere Informationen zum Aktualisieren des OfficeScan Servers finden Sie unter *Durchführen eines lokalen Upgrades auf Seite 3-21* oder *Durchführen eines Remote-Upgrades auf Seite 3-62*.



Hinweis

Zur Beschleunigung des Upgrade-Prozesses beenden Sie den OfficeScan Agent, bevor Sie ein OfficeScan Server aktualisieren, auf dem Windows Server 2008 Standard 64-Bit ausgeführt wird.

Konfigurieren Sie sofort nach Abschluss der Installation und vor dem Upgrade der Agents die Einstellungen des OfficeScan Servers über die Webkonsole.

Ausführliche Anweisungen zur Konfiguration von OfficeScan Einstellungen finden Sie im *Administratorhandbuch* oder in der *OfficeScan Server-Hilfe*.

Teil 3: Update-Agents aktualisieren

Prozedur

1. Navigieren Sie zu **Agents > Agent-Verwaltung**.
2. Wählen Sie in der Agent-Ansicht die Update-Agents aus, die aktualisiert werden sollen.



Tipp

Um Update-Agents leichter zu lokalisieren, wählen Sie eine Domäne, navigieren Sie zur **Agent-Hierarchie-Ansicht** oberhalb der Agent-Hierarchie, und wählen Sie anschließend **Update-Agent-Ansicht**.

3. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.
4. Deaktivieren Sie die Option **OfficeScan Agents können Komponenten aktualisieren, aber kein Upgrade des Agents durchführen oder Hotfixes verteilen**.
5. Klicken Sie auf **Speichern**.
6. Navigieren Sie zu **Updates > Agents > Manuelles Update**.
7. Wählen Sie die Option **Agents manuell auswählen** und klicken Sie auf **Auswählen**.
8. Wählen Sie in der Agent-Ansicht, die geöffnet wird, die Update-Agents aus, für die ein Upgrade durchgeführt werden soll.



Tipp

Um Update-Agents leichter zu lokalisieren, wählen Sie eine Domäne, navigieren Sie zur **Agent-Hierarchie-Ansicht** oberhalb der Agent-Hierarchie, und wählen Sie anschließend **Update-Agent-Ansicht**.

9. Klicken Sie oben in der Agent-Ansicht auf **Update starten**.
10. Prüfen Sie die Upgrade-Ergebnisse.
 - Das Upgrade der Online-Update-Agents wird sofort durchgeführt, nachdem Sie das Komponenten-Update gestartet haben.
 - Offline-Update-Agents werden upgegradet, wenn sie wieder online sind.
 - Das Upgrade für unabhängige Update-Agents (die zuvor als Roaming-Agents bezeichnet wurden) wird durchgeführt, sobald sie online sind oder zeitgesteuerte Updates für sie ausgeführt werden (vorausgesetzt, der Update-Agent weist Berechtigungen für zeitgesteuerte Updates auf).

11. Starten Sie die Endpunkte mit den Update-Agents neu, um das Upgrade der Agents abzuschließen.
12. Wiederholen Sie Schritt 1 bis Schritt 11, bis das Upgrade für alle Update-Agents durchgeführt wurde.

Teil 4: Update-Agent-Einstellungen konfigurieren

Prozedur

1. Navigieren Sie zu **Agents > Agent-Verwaltung**.
2. Wählen Sie in der Agent-Ansicht die Update-Agents aus, die aktualisiert werden sollen.



Tipp

Um Update-Agents leichter zu lokalisieren, wählen Sie eine Domäne, navigieren Sie zur **Agent-Hierarchie-Ansicht** oberhalb der Agent-Hierarchie, und wählen Sie anschließend **Update-Agent-Ansicht**.

3. Stellen Sie sicher, dass die Update-Agents über die neuesten Komponenten verfügen.
4. Klicken Sie auf **Einstellungen > Update-Agent-Einstellungen**.
5. Wählen Sie die folgenden Optionen:
 - **Komponenten-Updates**
 - **Domäneneinstellungen**
 - **OfficeScan Agent-Programme und Hotfixes**
6. Klicken Sie auf **Speichern**.

Warten Sie, bis der Update-Agent das Herunterladen des Agent-Programms beendet hat, bevor Sie zu Teil 5 weitergehen.

7. Wiederholen Sie Schritt 1 bis Schritt 6, bis alle Update-Agents die erforderlichen Einstellungen übernommen haben.

Teil 5: OfficeScan Agenten aktualisieren

Prozedur

1. Navigieren Sie zu **Updates > Agents > Automatisches Update** und stellen Sie sicher, dass die folgenden Optionen aktiviert sind:
 - **Komponenten-Update auf den Agents sofort nach dem Download einer neuen Komponente auf dem OfficeScan Server starten**
 - **Agents beginnen nach dem Neustart und dem Herstellen einer Verbindung zum OfficeScan Server mit dem Komponenten-Update (mit Ausnahme unabhängiger Agents)**
2. Navigieren Sie zu **Agents > Agent-Verwaltung**.
3. Wählen Sie in der Agent-Hierarchie die Agents aus, bei denen Sie ein Upgrade durchführen möchten. Sie können eine oder mehrere Domänen bzw. einzelne oder alle Agents innerhalb einer Domäne auswählen.
4. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.
5. Deaktivieren Sie die Option **OfficeScan Agents können Komponenten aktualisieren, aber kein Upgrade des Agents durchführen oder Hotfixes verteilen**.
6. Klicken Sie auf **Speichern**.
7. Prüfen Sie die Upgrade-Ergebnisse.
 - *Online-Agents auf Seite 3-13*
 - *Offline-Agents auf Seite 3-14*
 - *Unabhängige (Roaming-) Agents auf Seite 3-15*
8. Führen Sie einen Neustart der Agent-Endpunkte durch, um das Upgrade der Agents abzuschließen.

9. Wiederholen Sie Schritt 2 bis Schritt 8, bis das Upgrade für alle Agents durchgeführt wurde.
-

Upgrade-Ergebnisse

Online-Agents



Hinweis

Starten Sie die Agent-Endpunkte nach dem Upgrade neu.

- Automatisches Upgrade

Online-Agents beginnen mit dem Upgrade, wenn eines der folgenden Ereignisse auftritt:

- Der OfficeScan Server lädt eine neue Komponente herunter und fordert die Agents zum Update auf.
- Der Agent wird neu geladen.
- Der Agent wird neu gestartet und stellt eine Verbindung zum OfficeScan Server her.
- Ein Agent-Endpunkt unter Windows Server 2003 oder Windows XP Professional meldet sich bei einem Server an, dessen Anmeldeskript Sie mithilfe des Dienstprogramms Anmeldeskript-Setup (AutoPcc.exe) geändert haben.
- Auf dem Agent-Endpunkt wird ein zeitgesteuertes Update ausgeführt (nur für Agents mit Berechtigungen für zeitgesteuerte Updates).

- Manuelles Upgrade

Wenn keines der obigen Ereignisse eingetreten ist, führen Sie eine der folgenden Aufgaben durch, um sofort ein Agent-Upgrade auszuführen:

- Erstellen Sie ein EXE- oder MSI-OfficeScan Agent-Paket und verteilen Sie es.

**Hinweis**

Weitere Anweisungen zum Erstellen eines Agent-Pakets finden Sie im *Administratorhandbuch*.

- Fordern Sie Benutzer auf, **Jetzt aktualisieren** auf dem Agent-Endpunkt auszuführen.
- Wenn auf dem Agent-Endpunkt Windows Server 2003, XP Professional, Server 2008, Vista™ (alle Editionen außer Vista Home), 7™ (alle Editionen außer 7 Home), Windows 8 (Pro/Enterprise), Windows Server 2012 oder Windows Server 2016 ausgeführt wird, weisen Sie den Benutzer zur Durchführung folgender Schritte an:
 - Stellen Sie eine Verbindung zum Servercomputer her.
 - Navigieren Sie zu \\<Name des Server-Computers>\ofcscan.
 - Starten Sie AutoPcc.exe.
- Wenn auf dem Agent-Endpunkt Windows Vista Home, Windows 7 Home, Windows 8 oder Windows 10 ausgeführt wird, weisen Sie den Benutzer an, mit der rechten Maustaste auf die Datei AutoPcc.exe zu klicken und die Option **Als Administrator ausführen** auszuwählen.
- Starten Sie ein manuelles Agent-Update.

Sie initiieren Sie manuelle Updates:

1. Navigieren Sie zu **Updates > Agents > Manuelles Update**.
2. Wählen Sie die Option **Agents manuell auswählen** und klicken Sie auf **Auswählen**.
3. Wählen Sie in der Agent-Ansicht, die geöffnet wird, die Agents aus, für die ein Upgrade durchgeführt werden soll.
4. Klicken Sie oberhalb der Agent-Ansicht auf **Komponenten-Update starten**.

Offline-Agents

Das Upgrade für Offline-agents wird durchgeführt, sobald die Agents online sind.

Unabhängige (Roaming-) Agents

Das Upgrade für unabhängige Agents (die zuvor als Roaming-Agents bezeichnet wurden) wird durchgeführt, sobald die Agents wieder online sind oder zeitgesteuerte Updates für sie ausgeführt werden (vorausgesetzt der Agent weist Berechtigungen für zeitgesteuerte Updates auf).

Upgrade-Methode 3: Agents auf den OfficeScan XG Server verschieben

Führen Sie eine Erstinstallation des OfficeScan XG Servers durch und verschieben Sie anschließend Agents auf diesen Server. Die Agents werden beim Verschieben automatisch auf OfficeScan XG aktualisiert.

Teil 1: Erstinstallation des OfficeScan Servers durchführen und Update-Einstellungen konfigurieren

Prozedur

1. Führen Sie eine Erstinstallation des OfficeScan XG Servers durch.
Weitere Informationen finden Sie unter [Die Setup-Installationsfenster auf Seite 2-5](#).
2. Melden Sie sich an der Webkonsole an.
3. Navigieren Sie zu **Updates > Agents > Automatisches Update** und stellen Sie sicher, dass die folgenden Optionen aktiviert sind:
 - **Komponenten-Update auf den Agents sofort nach dem Download einer neuen Komponente auf dem OfficeScan Server starten**
 - **Agents beginnen nach dem Neustart und dem Herstellen einer Verbindung zum OfficeScan Server mit dem Komponenten-Update (mit Ausnahme unabhängiger Agents)**
4. Navigieren Sie zu **Agents > Agent-Verwaltung**.
5. Klicken Sie in der Agent-Ansicht auf das Symbol der Root-Domäne () , um alle Agents auszuwählen.

6. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.
 7. Deaktivieren Sie die Option **OfficeScan Agents können Komponenten aktualisieren, aber kein Upgrade des Agents durchführen oder Hotfixes verteilen**.
 8. Klicken Sie auf **Auf alle Agents anwenden**.
 9. Notieren Sie sich folgende Informationen über den OfficeScan XG Server. Stellen Sie diese Informationen auf dem OfficeScan 10.x Server bereit, wenn Sie Agents verschieben:
 - Endpunktname oder IP-Adresse
 - Server-Listening-Port

Navigieren Sie zum Anzeigen des Server-Listening-Ports zu **Administration > Einstellungen > Agent-Verbindung**. Die Portnummer wird auf dem Bildschirm angezeigt.
-

Teil 2: OfficeScan Agenten aktualisieren

Prozedur

1. Navigieren Sie in der Vorgängerversion der OfficeScan Webkonsole zu **Updates > Zusammenfassung**.
 2. Klicken Sie auf **Benachrichtigung abbrechen**. Diese Funktion löscht die Benachrichtigungswarteschlange des Servers, wodurch Probleme beim Verschieben von Clients/Agents auf den OfficeScan XG Server vermieden werden.
-



Warnung!

Führen Sie die anschließenden Schritte sofort danach durch. Wenn die Benachrichtigungswarteschlange des Servers vor dem Verschieben von Clients/Agents aktualisiert wird, können diese unter Umständen nicht erfolgreich verschoben werden.

3. Wechsel Sie in folgendes Fenster:
 - Für OfficeScan 10.x Server: **Netzwerkcomputer > Client-Verwaltung**
 - Für OfficeScan 11.x Server: **Agents > Agent-Verwaltung**
 4. Wählen Sie in der Client-/Agent-Hierarchie die Clients/Agents aus, für die Sie ein Upgrade durchführen möchten. Wählen Sie nur Online-Clients/-Agents aus, da Offline-Clients/-Agents und Roaming-Clients/-Agents nicht verschoben werden können.
 5. Verschieben Sie Clients/Agents folgendermaßen:
 - Für OfficeScan 10.x Server:
 - a. Klicken Sie auf **Client-Hierarchie verwalten > Client verschieben**.
 - b. Geben Sie den Namen, die IP-Adresse und den Server-Listening-Port des OfficeScan XG Servers unter **Ausgewählte Clients online auf anderen OfficeScan Server verschieben** an.
 - Für OfficeScan 11.x Server:
 - a. Klicken Sie auf **Agent-Hierarchie verwalten > Agent verschieben**.
 - b. Geben Sie den Namen, die IP-Adresse und den Server-Listening-Port des OfficeScan XG Servers unter **Ausgewählte(n) Agent(s) online auf einen anderen OfficeScan Server verschieben** an.
 6. Klicken Sie auf **Verschieben**.
-

Upgrade-Ergebnisse

- Die Verschiebung und das Upgrade der Online-Agents beginnt.
- Tipps zur Verwaltung von Offline- und unabhängigen Agents (zuvor als Roaming-Agents bezeichnet):
 - Deaktivieren Sie den unabhängigen Modus (zuvor als Roaming-Modus bezeichnet) auf Agents, um diese aktualisieren zu können.
 - Weisen Sie bei Offline-Agents die Benutzer an, eine Verbindung zum Netzwerk herzustellen, damit die Agents in den Online-Modus wechseln

können. Weisen Sie bei Agents, die seit längerer Zeit offline sind, die Benutzer an, den Agent über den Endpunkt zu deinstallieren. Verwenden Sie anschließend eine geeignete im *Administratorhandbuch* beschriebene Agent-Installationsmethode (wie Agent Packager) zum Installieren des OfficeScan Agents.

**Hinweis**

Führen Sie einen Neustart der Agent-Endpunkte durch, um das Upgrade der Agents abzuschließen.

Upgrade-Methode 4: Das automatische Agent-Upgrade aktivieren

Sofort nach dem Upgrade des OfficeScan Servers auf diese Version fordert der Server alle von ihm verwalteten Agents auf, ebenfalls ein Upgrade durchzuführen.

Falls der Server nur eine kleine Zahl von Agents verwaltet, ziehen Sie in Betracht, den Agents das sofortige Upgrade zu erlauben. Sie können jedoch ebenso die zuvor erläuterten Upgrade-Methoden verwenden.

Teil 1: Update-Einstellungen auf dem OfficeScan Server konfigurieren

Prozedur

- Für OfficeScan 10.x Server:
 - a. Navigieren Sie zu **Updates > Netzwerkcomputer > Automatisches Update** und aktivieren Sie die folgenden Optionen:
 - **Komponenten-Update auf den Clients sofort nach dem Download einer neuen Komponente auf dem OfficeScan Server starten**
 - **Clients beginnen beim Neustart mit dem Komponenten-Update, wenn sie sich mit dem OfficeScan Server verbinden (Ausnahme: Roaming-Clients)**

- b. Navigieren Sie zu **Netzwerkcomputer > Client-Verwaltung**.
- c. Klicken Sie in der Client-Struktur auf das Symbol der Root-Domäne () , um alle Clients auszuwählen.
- d. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.
- e. Wählen Sie **Clients können Komponenten aktualisieren, aber kein Upgrade des Client-Programms durchführen oder Hotfixes verteilen** aus.
- f. Klicken Sie auf **Für alle Clients übernehmen**.



Tipp

Die Verteilung der Einstellungen auf Online-Clients kann etwas Zeit in Anspruch nehmen, wenn Sie über eine komplexe Netzwerkumgebung und eine große Anzahl an Clients verfügen. Planen Sie vor dem Upgrade genügend Zeit für die Verteilung der Einstellungen auf alle Clients ein. OfficeScan Clients, die die Einstellungen nicht übernehmen, führen automatisch ein Upgrade durch.

- Für OfficeScan 11.x Server:
 - a. Navigieren Sie zu **Updates > Agents > Automatisches Update** und stellen Sie sicher, dass die folgenden Optionen aktiviert sind:
 - **Komponenten-Update auf den Agents sofort nach dem Herunterladen einer neuen Komponente auf dem OfficeScan Server starten**
 - **Agents beginnen nach dem Neustart und dem Herstellen einer Verbindung mit dem OfficeScan Server mit dem Komponenten-Update (Ausnahme: Roaming-Agents)**
 - b. Navigieren Sie zu **Agents > Agent-Verwaltung**.
 - c. Klicken Sie in der Agent-Ansicht auf das Symbol der Root-Domäne () , um alle Agents auszuwählen.
 - d. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.

- e. Wählen Sie die Option **OfficeScan Agents können Komponenten aktualisieren, aber kein Upgrade des Agent-Programms durchführen oder Hotfixes verteilen** aus.
- f. Klicken Sie auf **Auf alle Agents anwenden**.

Es kann etwas dauern, die Einstellungen auf eine große Anzahl von Agents sowie auf Online-Agents in einer komplexen Netzwerkumgebung zu verteilen. Planen Sie vor dem Upgrade genügend Zeit für die Verteilung der Einstellungen auf alle Agents ein. OfficeScan Agents, die die Einstellungen nicht übernehmen, werden automatisch aktualisiert.

Teil 2: Upgrade des OfficeScan Servers

Weitere Informationen zum Aktualisieren des OfficeScan Servers finden Sie unter *Durchführen eines lokalen Upgrades auf Seite 3-21* oder *Durchführen eines Remote-Upgrades auf Seite 3-62*.



Hinweis

Zur Beschleunigung des Upgrade-Prozesses beenden Sie den OfficeScan Agent, bevor Sie ein OfficeScan Server aktualisieren, auf dem Windows Server 2008 Standard 64-Bit ausgeführt wird.

Konfigurieren Sie sofort nach Abschluss der Installation und vor dem Upgrade der Agents die Einstellungen des OfficeScan Servers über die Webkonsole.

Ausführliche Anweisungen zur Konfiguration von OfficeScan Einstellungen finden Sie im *Administratorhandbuch* oder in der *OfficeScan Server-Hilfe*.

Upgrade-Ergebnisse

- Das Upgrade der Online-Agents wird sofort nach Abschluss des Server-Upgrades durchgeführt.
- Das Upgrade für Offline-Agents wird durchgeführt, sobald die Agents online gehen.

- Das Upgrade für unabhängige Agents (die zuvor als Roaming-Agents bezeichnet wurden) wird durchgeführt, sobald die Agents wieder online sind oder zeitgesteuerte Updates für sie ausgeführt werden (vorausgesetzt, der Agent weist Berechtigungen für zeitgesteuerte Updates auf).

**Hinweis**

Führen Sie einen Neustart der Agent-Endpunkte durch, um das Upgrade der Agents abzuschließen.

Durchführen eines lokalen Upgrades

Während eines lokalen Upgrades wendet OfficeScan die Einstellungen an, die von der Vorgängerversion des OfficeScan Servers verwendet werden. Eine begrenzte Anzahl von Fenstern wird angezeigt, in denen Sie neue von OfficeScan XG bereitgestellte Funktionen konfigurieren können.

Aktualisieren von OfficeScan 10.6 SP3 mit Apache

Diese Version von OfficeScan bietet keine weitere Unterstützung für den Apache Webserver. Während eines Upgrades von OfficeScan 10.6 SP3, das den Apache-Server verwendet, werden Sie von OfficeScan darüber informiert, dass das Setup-Programm die IIS Webserver-Rolle auf dem Server installiert. Nach Abschluss der Installation wird der Apache-Server von OfficeScan nicht mehr verwendet.

**Wichtig**

OfficeScan kann den Apache-Server nur durch den IIS-Server ersetzen, wenn Sie den Apache-Server mit Hilfe des vorherigen OfficeScan Installation-Programms installiert haben. Wenn Sie den Apache-Server manuell installiert haben, müssen Sie diesen vor dem Aktualisieren von OfficeScan deinstallieren.

Lizenzvereinbarung

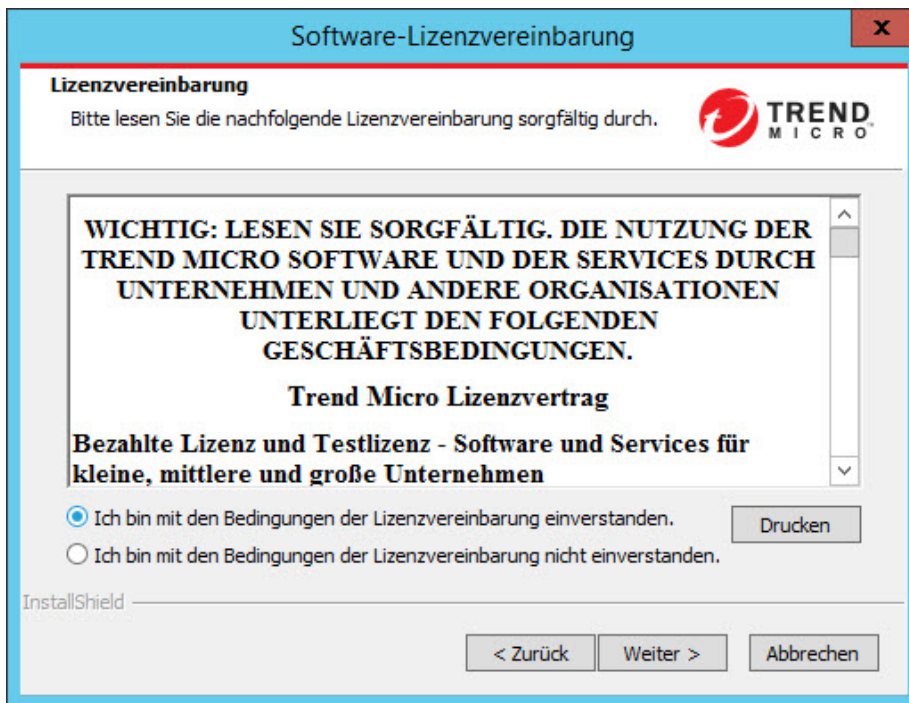


ABBILDUNG 3-1. Fenster "Lizenzvereinbarung"

Lesen Sie die Lizenzvereinbarung aufmerksam durch, und stimmen Sie den Bedingungen der Lizenzvereinbarung zu, um die Installation fortzusetzen. Die Installation kann nicht fortgesetzt werden, wenn Sie den Bedingungen der Lizenzvereinbarung nicht zustimmen.

Installationsziel

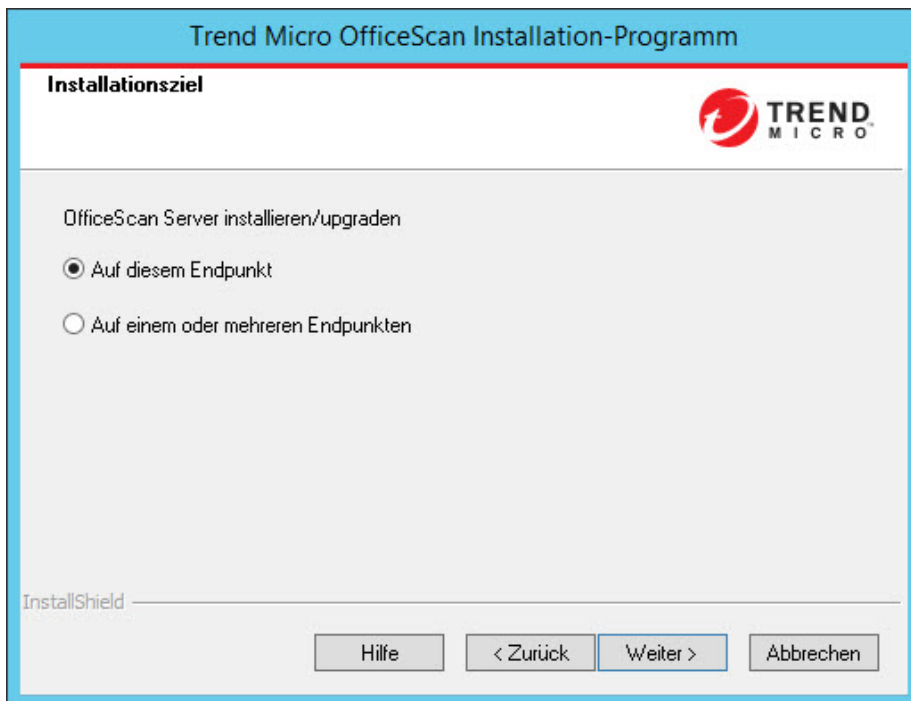


ABBILDUNG 3-2. Das Fenster "Installationsziel"

Führen Sie das Setup-Programm aus und installieren Sie den OfficeScan Server auf dem aktuellen Endpunkt oder auf anderen Endpunkten im Netzwerk. Wenn vom Setup-Programm eine frühere Version von OfficeScan auf dem Zielpunkt erkannt wird, wird bei der Installation automatisch ein Upgrade durchgeführt. Nur die folgenden Versionen von OfficeScan können auf diese Version aktualisiert werden:

- 11.0 Service Pack 1
- 11.0
- 10.6 Service Pack 3



Hinweis

Trend Micro empfiehlt dringend, alle verfügbaren Patches und Hotfixes auf den aktuellen OfficeScan Server vor dem Durchführen eines Upgrades anzuwenden.

Hinweise zum Remote-Upgrade

Beim Remote-Upgrade prüft Setup, ob der Zielpunkt die Voraussetzungen für das Upgrade des Servers erfüllt. Bevor Sie den Vorgang fortsetzen:

- Sie müssen auf dem Zielpunkt über Administratorrechte verfügen.
- Notieren Sie sich den Host-Namen und die Anmeldedaten (Benutzername und Kennwort) für die Zielpunkte.
- Stellen Sie sicher, dass die Zielpunkte die Anforderungen für die Installation des OfficeScan Servers erfüllen.
- Stellen Sie sicher, dass auf dem Endpunkt Microsoft IIS Server 7.0 oder höher installiert ist, wenn er als Webserver eingesetzt wird.

Bei lokalen Upgrades behält OfficeScan die Einstellungen der früheren Installation bei, einschließlich des Servernamens, der Angaben zum Proxy-Server und der Portnummern. Es ist nicht möglich, diese Einstellungen beim Upgrade zu ändern. Ändern Sie die Einstellungen nach dem Upgrade über die OfficeScan Webkonsole.



Wichtig

Beim Remote-Upgrade müssen alle Einstellungen erneut vorgenommen werden. Diese Einstellungen bleiben jedoch nach dem Server-Upgrade unberücksichtigt, da der Server die Einstellungen der vorherigen Version übernimmt.

Endpoint Prescan

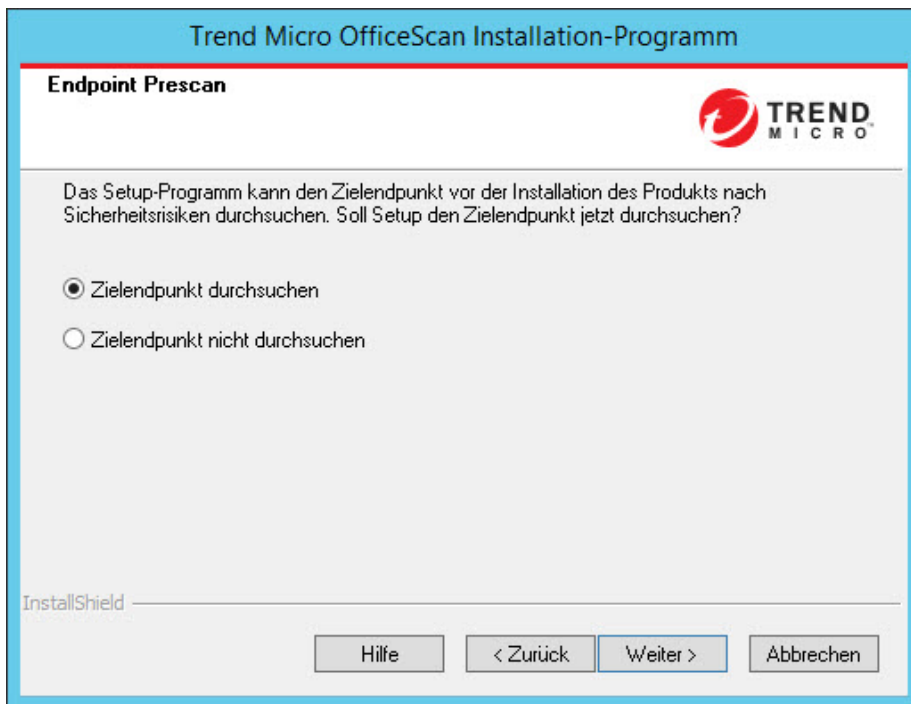


ABBILDUNG 3-3. Das Fenster "Endpoint Prescan"

Vor der Installation des OfficeScan Servers kann das Setup-Programm den Zielpunkt auf Viren und Malware überprüfen. Setup durchsucht die anfälligsten Bereiche des Endpunkts, wie beispielsweise:

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

Bei der Entdeckung von Viren/Malware und Trojanern kann Setup folgende Aktionen durchführen:

- **Löschen:** Löscht die infizierte Datei.
- **Säubern:** Eine Datei, die gesäubert werden kann, wird gesäubert, bevor der vollständige Zugriff möglich ist. Eine Datei, die nicht gesäubert werden kann, wird gemäß der festgelegten Aktion bearbeitet.
- **Umbenennen:** Die Erweiterung der infizierten Datei wird in *vir* geändert. Der Benutzer kann die 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:** Ermöglicht den vollständigen Zugriff auf die Datei, ohne sie zu verändern. Die Datei kann kopiert, gelöscht oder geöffnet werden.

Bei der lokalen Installation startet die Suche, wenn Sie auf **Weiter** klicken. Bei der Remote-Installation startet die Suche vor der eigentlichen Installation.



Wichtig

Während der lokalen Installation eines Upgrades werden Sie vom Setup-Programm aufgefordert, die Einstellungen für den Ransomware-Schutz zu aktualisieren, damit optimaler Schutz vor Ransomware-Bedrohungen gewährleistet werden kann.

Die Anwendung der aktualisierten Einstellungen wirkt sich nur auf Agents aus, die die Verhaltensüberwachung bereits aktiviert haben.

Warnung wegen Neustart des OfficeScan Agents

Das Setup-Programm bewertet die Ressourcen des Ziel-Endpunkts. Während eines Upgrade-Szenarios wird eine Warnung angezeigt, wenn das OfficeScan Agent-Programm auf dem Ziel-Endpunkt vorhanden ist.

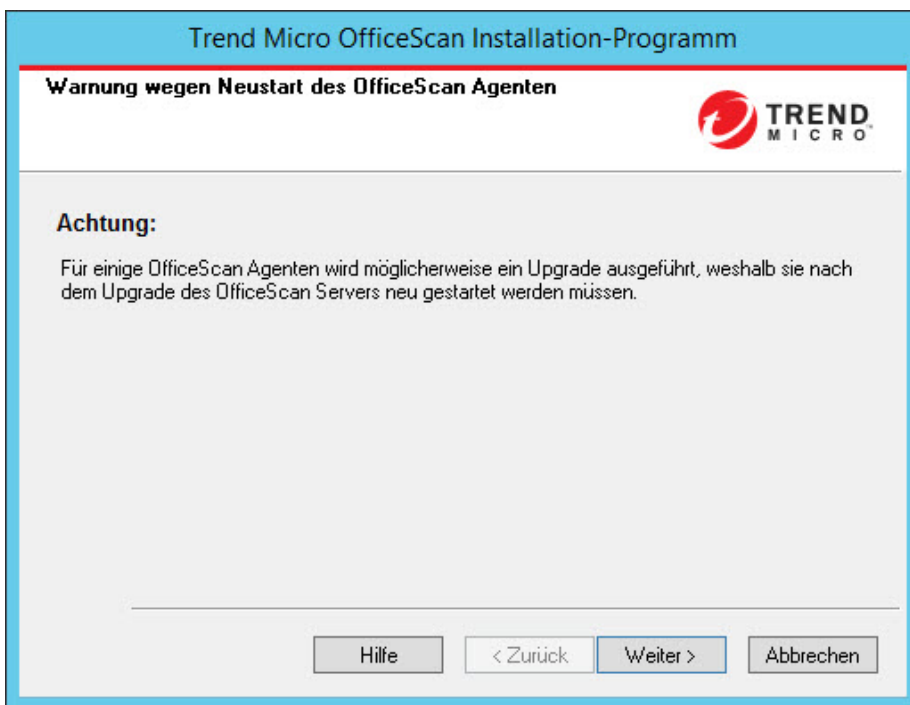


ABBILDUNG 3-4. Warnung wegen Neustart des OfficeScan Agents

Apache-Deinstallationswarnung

Beim Aktualisieren auf OfficeScan XG wird eine Warnung angezeigt, wenn der Apache Webserver für den vorherigen OfficeScan Server konfiguriert ist. OfficeScan bietet keine weitere Unterstützung für den Apache Webserver.

- Wenn Sie den Apache Webserver mit Hilfe des Setup-Programms in der Vorgängerversion von OfficeScan installiert haben, kann OfficeScan den

Webserver automatisch deinstallieren und den IIS Webserver während der Installation installieren.

- Wenn Sie den Apache Webserver vor der Installation der Vorgängerversion von OfficeScan manuell installiert haben, müssen Sie den Apache Webserver manuell deinstallieren, bevor Sie mit der Aktualisierung auf den OfficeScan Server fortfahren können.



Hinweis

Diese Warnung wird nicht angezeigt, wenn die Vorgängerversion des OfficeScan Servers mit dem IIS Webserver konfiguriert wurde.

Datenbanksicherung

Während Upgrades bietet das Setup-Programm die Möglichkeit, die OfficeScan Datenbank vor dem Upgrade auf die aktuelle Version zu sichern. Diese Sicherungsinformationen können Ihnen bei einem Rollback hilfreich sein.



Hinweis

Für das Sicherungspaket sind möglicherweise mehr als 300 MB freier Festplattenspeicher erforderlich.

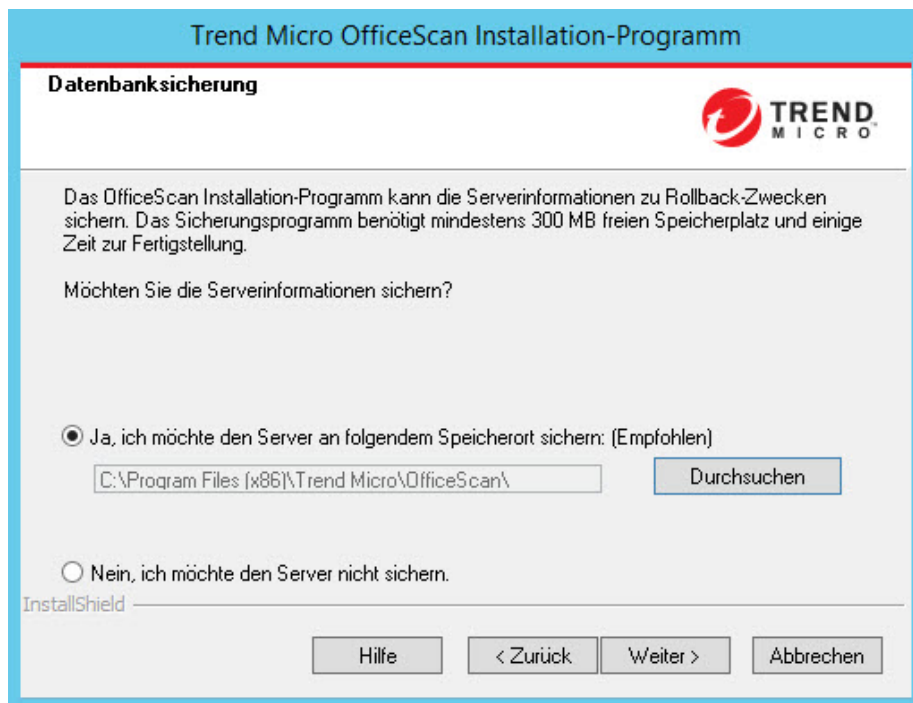


ABBILDUNG 3-5. Fenster „Datenbanksicherung“

OfficeScan Agent-Verteilung

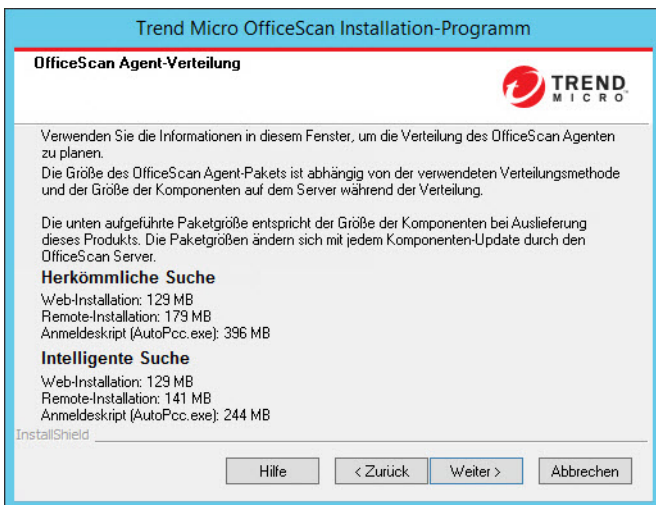


ABBILDUNG 3-6. Fenster "OfficeScan Agent-Verteilung"

Es gibt mehrere Methoden, um OfficeScan agents zu installieren oder zu aktualisieren. In diesem Fenster wird eine Liste der verschiedenen Verteilungsmethoden und der ungefähr erforderlichen Netzwerkbandbreite angezeigt.

Verwenden Sie dieses Fenster, um den auf den Servern benötigten Speicherplatz und die erforderliche Bandbreite für die Verteilung von agents auf die Ziel-Endpunkte abzuschätzen.



Hinweis

Für alle Installationsmethoden sind lokale Administrator- oder Domänenadministratorrechte auf den Ziel-Endpunkten erforderlich.

Integrierten Smart Protection Server installieren



Hinweis

Dieses Fenster wird nicht angezeigt, wenn Sie eine virtuelle IIS-Website während der Updateinstallationen verwenden.



ABBILDUNG 3-7. Das Fenster "Integrierten Smart Protection Server installieren"

Das Setup-Programm kann den integrierten Smart Protection Server auf dem Ziel-Endpunkt installieren. Der integrierte Server bietet File-Reputation-Dienste für agents mit intelligenter Suche sowie Web-Reputation-Dienste für agents, die den Web-Reputation-Richtlinien unterliegen. Sie können den integrierten Server über die OfficeScan Webkonsole verwalten.

Trend Micro empfiehlt die Installation des eigenständigen Smart Protection Servers, der über die gleichen Funktionen wie der integrierte Server verfügt, aber mehreren agents dienen kann. Der eigenständige Server wird separat installiert und hat eine eigene Management-Konsole. Weitere Informationen zum eigenständigen Server finden Sie im *Trend Micro Smart Protection Server Administratorhandbuch*.

**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. Weitere Informationen zum Konfigurieren von Smart Protection Quellen für Agents finden Sie im *Administratorhandbuch*.

Agent-Verbindungsprotokolle für File-Reputation-Dienste

OfficeScan Agents können sich über HTTP und HTTPS mit den File-Reputation-Diensten des integrierten Smart Protection Servers verbinden. HTTPS ermöglicht eine sicherere Verbindung, während HTTP weniger Bandbreite benötigt.

**Hinweis**

Wenn Endpunkte die Verbindung zum integrierten Server über einen Proxy-Server aufbauen, müssen die internen Proxy-Einstellungen über die Webkonsole konfiguriert werden. Weitere Informationen zum Konfigurieren von Proxy-Einstellungen finden Sie im *Administratorhandbuch*.

Die für File-Reputation-Dienste verwendeten Portnummern richten sich nach dem Webserver, den der OfficeScan Server verwendet. Weitere Informationen finden Sie unter [Webserver auf Seite 2-15](#).

Der HTTP-Port wird im Installationsfenster nicht angezeigt. Der HTTPS-Port wird angezeigt; seine Konfiguration ist jedoch optional.

TABELLE 3-1. Ports für die File-Reputation-Dienste des integrierten Smart Protection Servers

WEBSERVER UND EINSTELLUNGEN	PORTS FÜR FILE-REPUTATION-DIENSTE	
	HTTP	HTTPS (SSL)
IIS-Standard-Website	80	443
Virtuelle IIS-Website	8080	4343

Integrierter Server nicht installiert

Wenn Sie eine Erstinstallation durchführen und nicht ausgewählt haben, den integrierten Server zu installieren:

- Die herkömmliche Suche wird zur standardmäßigen Suchmethode.
- Wenn Sie die Web-Reputation-Richtlinien in einem separaten Installationsfenster aktivieren (ausführliche Hinweise finden Sie unter [Web-Reputation-Funktion auf Seite 2-39](#)), können agents keine Web-Reputation-Abfragen senden, da OfficeScan davon ausgeht, dass kein Smart Protection Server installiert wurde.

Falls ein eigenständiger Server nach der Installation von OfficeScan verfügbar ist, führen Sie die folgenden Aufgaben über die OfficeScan Webkonsole durch:

- Ändern Sie die Suchmethode in die intelligente Suche.
- Fügen Sie den eigenständigen Server zur Liste der Smart Protection Quellen hinzu, sodass agents File- und Web-Reputation-Abfragen an den Server senden können.

Bei der Aktualisierung von OfficeScan Servern der Version 10.x, bei denen der integrierte Server deaktiviert ist, wird der integrierte Server nicht installiert. OfficeScan Agents behalten die Suchmethoden und die Smart Protection Quellen bei, an die sie Abfragen senden.

Web-Reputation-Dienste aktivieren

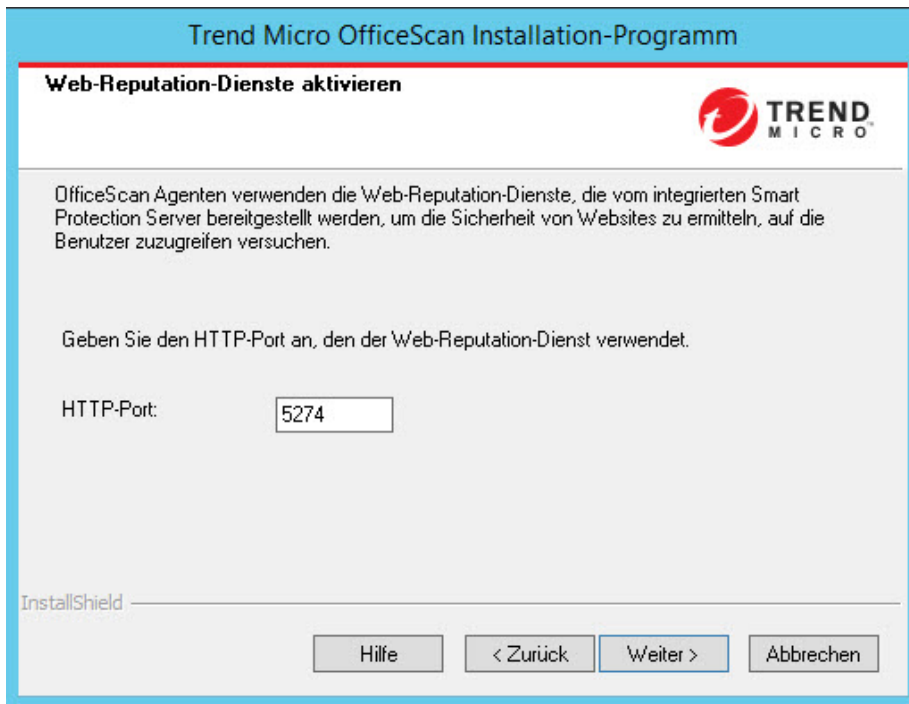


ABBILDUNG 3-8. Fenster "Web-Reputation-Dienste aktivieren"

Die Web-Reputation-Dienste untersuchen das potenzielle Sicherheitsrisiko aller angeforderten URLs zum Zeitpunkt einer jeden HTTP-Anfrage. Abhängig von der von der Datenbank zurückgegebenen Bewertung und der konfigurierten Sicherheitsstufe, wird die Anfrage von Web Reputation entweder gesperrt oder genehmigt. Web-Reputation-Dienste werden vom integrierten Smart Protection Server bereitgestellt, der zusammen mit dem OfficeScan Server installiert wird.

Mit der Aktivierung der Web-Reputation-Dienste (ausgeführt unter dem Prozessnamen `LWCSService.exe`) wird der Bandbreitenverbrauch reduziert. Dies liegt daran, dass OfficeScan agents Web-Reputation-Daten von einem lokalen Server beziehen, anstatt eine Verbindung zum Smart Protection Network herzustellen.

Serverauthentifizierungszertifikat

Das Setup-Programm versucht, bisher vorhandene Authentifizierungszertifikate während der Installation zu entdecken. Ist bereits ein Zertifikat vorhanden, ordnet OfficeScan die Datei automatisch im Fenster **Serverauthentifizierungszertifikat** zu. Wenn kein Zertifikat vorhanden ist, verwendet OfficeScan standardmäßig die Option **Neues Authentifizierungszertifikat generieren**.



Hinweis

Während der Durchführung von Upgrade-Installationen über einen Remote-Standort wird das Fenster **Serverauthentifizierungszertifikat** nur angezeigt, wenn ein OfficeScan 10.6 SP3 Server aktualisiert wird.

Trend Micro OfficeScan Installation-Programm

Serverauthentifizierungszertifikat

Erlauben Sie OfficeScan, ein neues Zertifikat für die Kommunikation mit OfficeScan Agenten zu generieren, oder importieren Sie ein vorhandenes Zertifikat.
Hinweis: OfficeScan erstellt eine Sicherung des neuen oder importierten Zertifikats im Ordner <Server_installation_folder>\AuthCertBackup\.

☒ Neues Authentifizierungszertifikat generieren

Sicherungskennwort:

Kennwort bestätigen:

☐ Vorhandenes Zertifikat importieren

Hinweis: Bei dem Zertifikat handelt es sich entweder um ein ZIP-Paket, das vom Zertifikat-Manager für Serverauthentifizierung generiert wurde, oder eine korrekt formatierte PFX-Datei.

Kennwort:

InstallShield

ABBILDUNG 3-9. Fenster "Serverauthentifizierungszertifikat" für neue Zertifikate

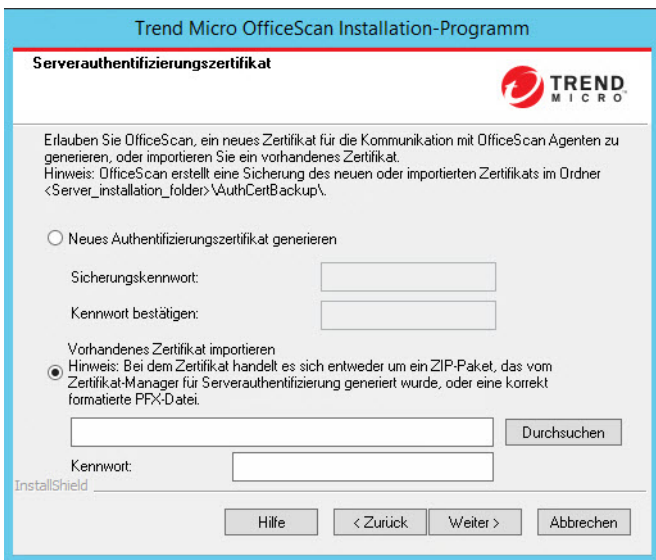


ABBILDUNG 3-10. Fenster "Serverauthentifizierungszertifikat" für bisher vorhandene Zertifikate

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.

OfficeScan kann das Authentifizierungszertifikat während der Installation erzeugen. Alternativ können Administratoren ein bereits vorhandenes Authentifizierungszertifikat von einem anderen OfficeScan Server importieren.



Tipp

Trend Micro empfiehlt, das Zertifikat beim Sichern mit einem Kennwort zu verschlüsseln.

Installationsdaten

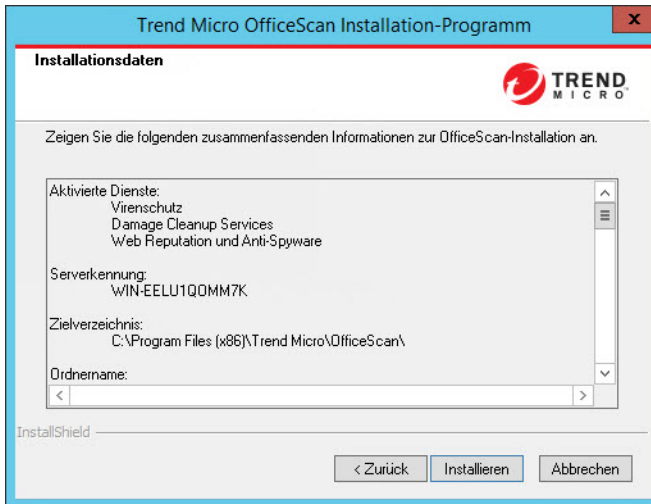


ABBILDUNG 3-11. Das Fenster mit den Installationsdaten

In diesem Fenster finden Sie eine Zusammenfassung der Installationseinstellungen. Überprüfen Sie die Installationsdaten, und klicken Sie auf **Zurück**, um Einstellungen oder Optionen zu ändern. Klicken Sie auf **Installieren**, um die Installation zu starten.

Der InstallShield Wizard ist abgeschlossen.

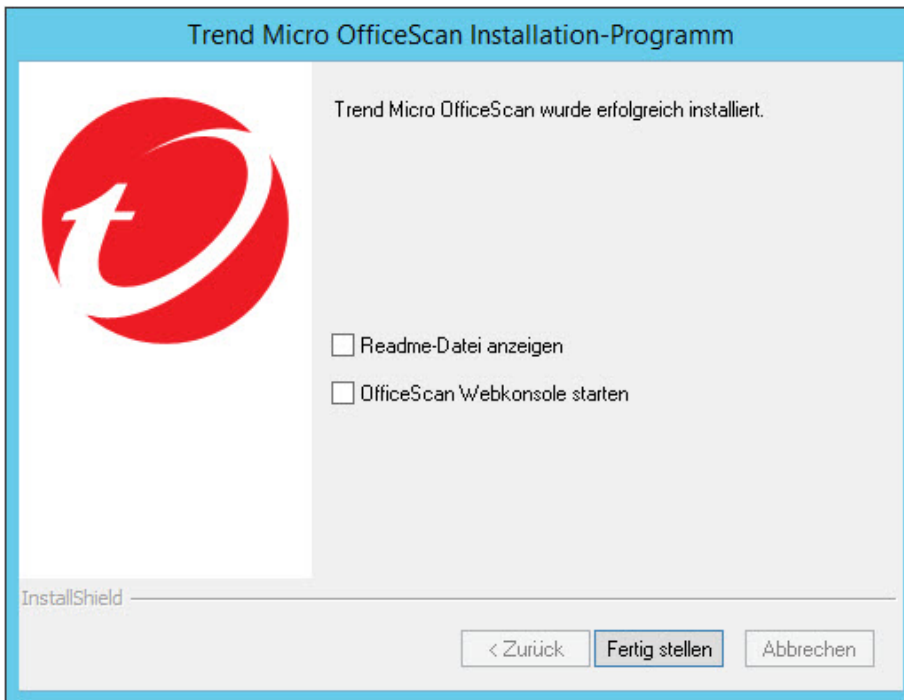


ABBILDUNG 3-12. Fenster "Der InstallShield Wizard ist abgeschlossen"

Lesen Sie nach Abschluss der Installation die Readme-Datei mit allgemeinen Informationen zum Produkt und den bekannten Problemen.

Administratoren können die Webkonsole starten, um die OfficeScan Einstellungen zu konfigurieren.

Aktualisieren von OfficeScan 10.6 SP3 mit IIS

Lizenzvereinbarung

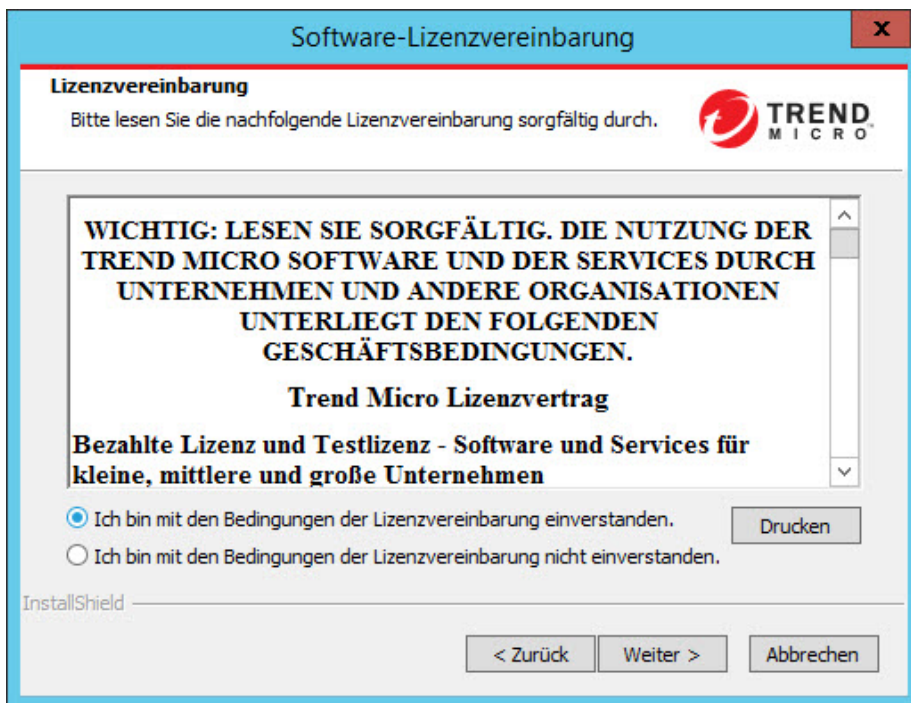


ABBILDUNG 3-13. Fenster "Lizenzvereinbarung"

Lesen Sie die Lizenzvereinbarung aufmerksam durch, und stimmen Sie den Bedingungen der Lizenzvereinbarung zu, um die Installation fortzusetzen. Die Installation kann nicht fortgesetzt werden, wenn Sie den Bedingungen der Lizenzvereinbarung nicht zustimmen.

Installationsziel

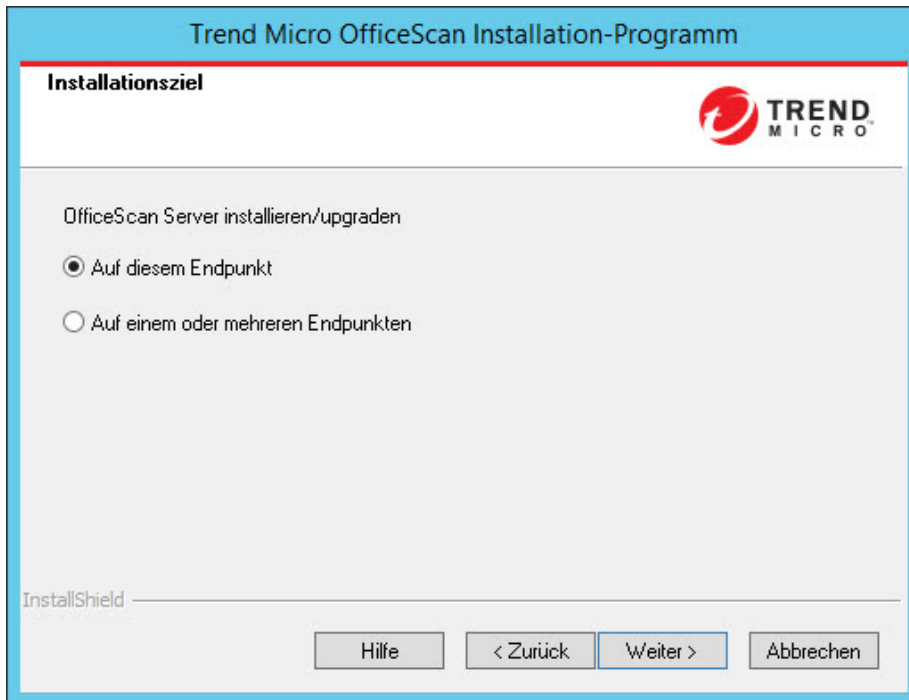


ABBILDUNG 3-14. Das Fenster "Installationsziel"

Führen Sie das Setup-Programm aus und installieren Sie den OfficeScan Server auf dem aktuellen Endpunkt oder auf anderen Endpunkten im Netzwerk. Wenn vom Setup-Programm eine frühere Version von OfficeScan auf dem Zielendpunkt erkannt wird, wird bei der Installation automatisch ein Upgrade durchgeführt. Nur die folgenden Versionen von OfficeScan können auf diese Version aktualisiert werden:

- 11.0 Service Pack 1
- 11.0
- 10.6 Service Pack 3

**Hinweis**

Trend Micro empfiehlt dringend, alle verfügbaren Patches und Hotfixes auf den aktuellen OfficeScan Server vor dem Durchführen eines Upgrades anzuwenden.

Hinweise zum Remote-Upgrade

Beim Remote-Upgrade prüft Setup, ob der Zielpunkt die Voraussetzungen für das Upgrade des Servers erfüllt. Bevor Sie den Vorgang fortsetzen:

- Sie müssen auf dem Zielpunkt über Administratorrechte verfügen.
- Notieren Sie sich den Host-Namen und die Anmeldedaten (Benutzername und Kennwort) für die Zielpunkte.
- Stellen Sie sicher, dass die Zielpunkte die Anforderungen für die Installation des OfficeScan Servers erfüllen.
- Stellen Sie sicher, dass auf dem Endpunkt Microsoft IIS Server 7.0 oder höher installiert ist, wenn er als Webserver eingesetzt wird.

Bei lokalen Upgrades behält OfficeScan die Einstellungen der früheren Installation bei, einschließlich des Servernamens, der Angaben zum Proxy-Server und der Portnummern. Es ist nicht möglich, diese Einstellungen beim Upgrade zu ändern. Ändern Sie die Einstellungen nach dem Upgrade über die OfficeScan Webkonsole.

**Wichtig**

Beim Remote-Upgrade müssen alle Einstellungen erneut vorgenommen werden. Diese Einstellungen bleiben jedoch nach dem Server-Upgrade unberücksichtigt, da der Server die Einstellungen der vorherigen Version übernimmt.

Endpoint Prescan

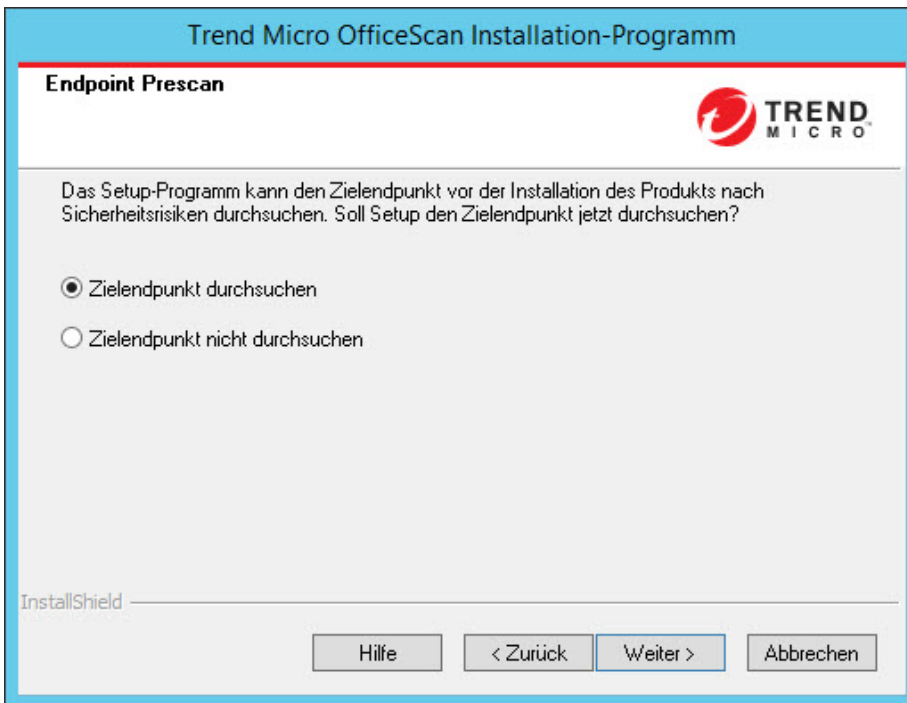


ABBILDUNG 3-15. Das Fenster "Endpoint Prescan"

Vor der Installation des OfficeScan Servers kann das Setup-Programm den Zielpunkt auf Viren und Malware überprüfen. Setup durchsucht die anfälligsten Bereiche des Endpunkts, wie beispielsweise:

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

Bei der Entdeckung von Viren/Malware und Trojanern kann Setup folgende Aktionen durchführen:

- **Löschen:** Löscht die infizierte Datei.
- **Säubern:** Eine Datei, die gesäubert werden kann, wird gesäubert, bevor der vollständige Zugriff möglich ist. Eine Datei, die nicht gesäubert werden kann, wird gemäß der festgelegten Aktion bearbeitet.
- **Umbenennen:** Die Erweiterung der infizierten Datei wird in `vir` geändert. Der Benutzer kann die 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:** Ermöglicht den vollständigen Zugriff auf die Datei, ohne sie zu verändern. Die Datei kann kopiert, gelöscht oder geöffnet werden.

Bei der lokalen Installation startet die Suche, wenn Sie auf **Weiter** klicken. Bei der Remote-Installation startet die Suche vor der eigentlichen Installation.



Wichtig

Während der lokalen Installation eines Upgrades werden Sie vom Setup-Programm aufgefordert, die Einstellungen für den Ransomware-Schutz zu aktualisieren, damit optimaler Schutz vor Ransomware-Bedrohungen gewährleistet werden kann.

Die Anwendung der aktualisierten Einstellungen wirkt sich nur auf Agents aus, die die Verhaltensüberwachung bereits aktiviert haben.

Warnung wegen Neustart des OfficeScan Agents

Das Setup-Programm bewertet die Ressourcen des Ziel-Endpunkts. Während eines Upgrade-Szenarios wird eine Warnung angezeigt, wenn das OfficeScan Agent-Programm auf dem Ziel-Endpunkt vorhanden ist.

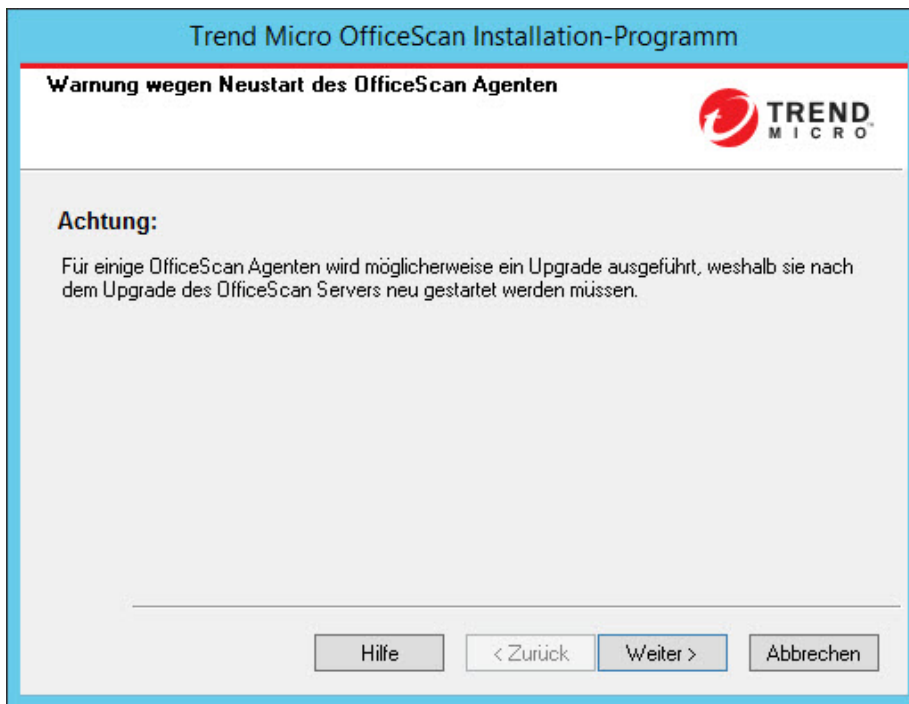


ABBILDUNG 3-16. Warnung wegen Neustart des OfficeScan Agents

Datenbanksicherung

Während Upgrades bietet das Setup-Programm die Möglichkeit, die OfficeScan Datenbank vor dem Upgrade auf die aktuelle Version zu sichern. Diese Sicherungsinformationen können Ihnen bei einem Rollback hilfreich sein.

**Hinweis**

Für das Sicherungspaket sind möglicherweise mehr als 300 MB freier Festplattenspeicher erforderlich.

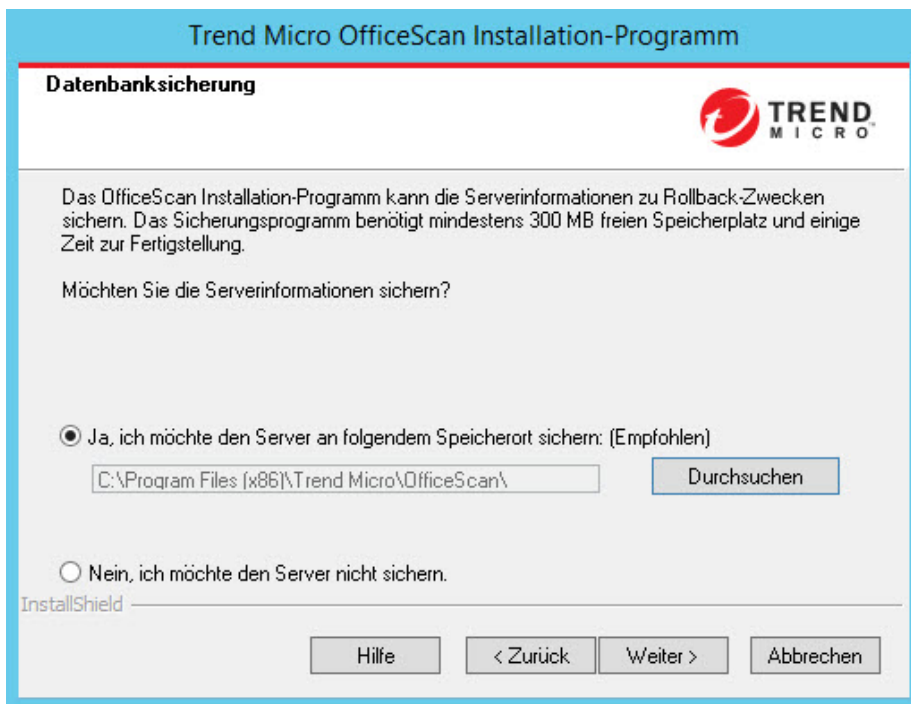


ABBILDUNG 3-17. Fenster „Datenbanksicherung“

OfficeScan Agent-Verteilung

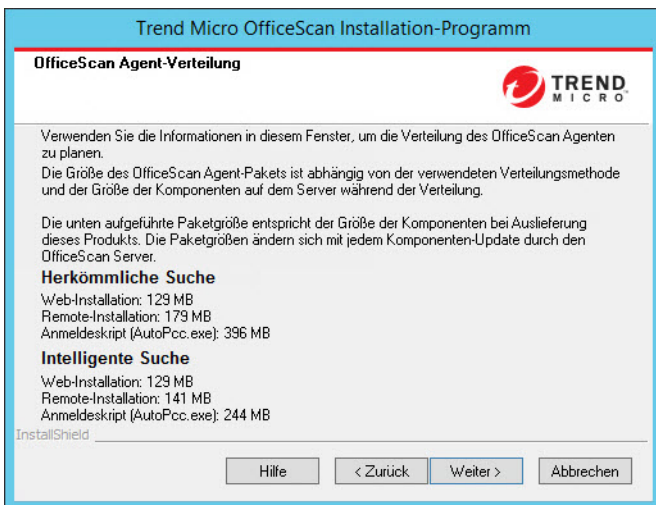


ABBILDUNG 3-18. Fenster "OfficeScan Agent-Verteilung"

Es gibt mehrere Methoden, um OfficeScan agents zu installieren oder zu aktualisieren. In diesem Fenster wird eine Liste der verschiedenen Verteilungsmethoden und der ungefähr erforderlichen Netzwerkbandbreite angezeigt.

Verwenden Sie dieses Fenster, um den auf den Servern benötigten Speicherplatz und die erforderliche Bandbreite für die Verteilung von agents auf die Ziel-Endpunkte abzuschätzen.



Hinweis

Für alle Installationsmethoden sind lokale Administrator- oder Domänenadministratorrechte auf den Ziel-Endpunkten erforderlich.

OfficeScan Firewall

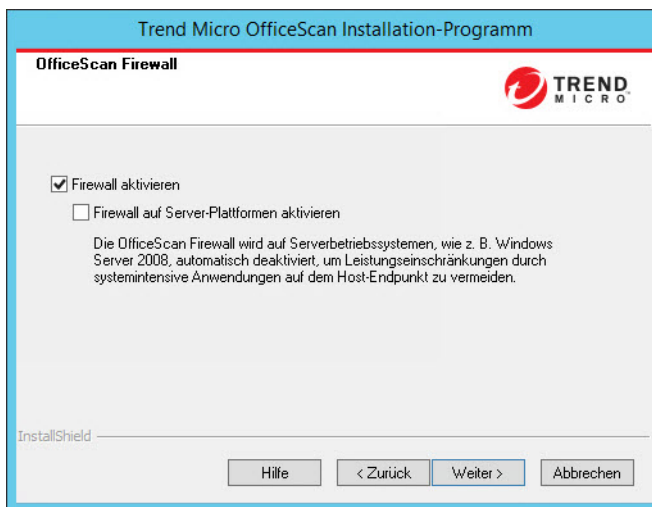


ABBILDUNG 3-19. Fenster „OfficeScan Firewall“

Dieses Fenster wird nur bei aktiviertem Virenschutz angezeigt.

OfficeScan Firewall

Die OfficeScan Firewall schützt agents und Server im Netzwerk mit Hilfe von Stateful-Inspection-Technologie und leistungsstarken Funktionen zur Virensuche und -bekämpfung. Sie können Regeln erstellen, um Verbindungen nach IP-Adresse, Portnummer oder Protokoll zu filtern, und anschließend die Regeln auf unterschiedliche Benutzergruppen anwenden.

Optional können Sie die Firewall deaktivieren und später erneut auf der Webkonsole des OfficeScan Servers aktivieren.

Optional können Sie die Firewall auf Server-Plattformen aktivieren. Wenn Sie ein Upgrade durchführen und der Firewall-Dienst bereits auf den Serverplattformen aktiviert ist, wählen Sie **Firewall auf Server-Plattformen aktivieren**, damit der Firewall-Dienst nach dem Upgrade nicht von OfficeScan deaktiviert wird.

Serverauthentifizierungszertifikat

Das Setup-Programm versucht, bisher vorhandene Authentifizierungszertifikate während der Installation zu entdecken. Ist bereits ein Zertifikat vorhanden, ordnet OfficeScan die Datei automatisch im Fenster **Serverauthentifizierungszertifikat** zu. Wenn kein Zertifikat vorhanden ist, verwendet OfficeScan standardmäßig die Option **Neues Authentifizierungszertifikat generieren**.



Hinweis

Während der Durchführung von Upgrade-Installationen über einen Remote-Standort wird das Fenster **Serverauthentifizierungszertifikat** nur angezeigt, wenn ein OfficeScan 10.6 SP3 Server aktualisiert wird.

Trend Micro OfficeScan Installation-Programm

Serverauthentifizierungszertifikat

TREND MICRO

Erlauben Sie OfficeScan, ein neues Zertifikat für die Kommunikation mit OfficeScan Agenten zu generieren, oder importieren Sie ein vorhandenes Zertifikat.
Hinweis: OfficeScan erstellt eine Sicherung des neuen oder importierten Zertifikats im Ordner <Server_installation_folder>\AuthCertBackup\.

☒ Neues Authentifizierungszertifikat generieren

Sicherungskennwort:

Kennwort bestätigen:

☐ Vorhandenes Zertifikat importieren

Hinweis: Bei dem Zertifikat handelt es sich entweder um ein ZIP-Paket, das vom Zertifikat-Manager für Serverauthentifizierung generiert wurde, oder eine korrekt formatierte PFX-Datei.

Kennwort:

InstallShield

ABBILDUNG 3-20. Fenster "Serverauthentifizierungszertifikat" für neue Zertifikate



ABBILDUNG 3-21. Fenster "Serverauthentifizierungszertifikat" für bisher vorhandene Zertifikate

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.

OfficeScan kann das Authentifizierungszertifikat während der Installation erzeugen. Alternativ können Administratoren ein bereits vorhandenes Authentifizierungszertifikat von einem anderen OfficeScan Server importieren.

**Tipp**

Trend Micro empfiehlt, das Zertifikat beim Sichern mit einem Kennwort zu verschlüsseln.

Installationsdaten

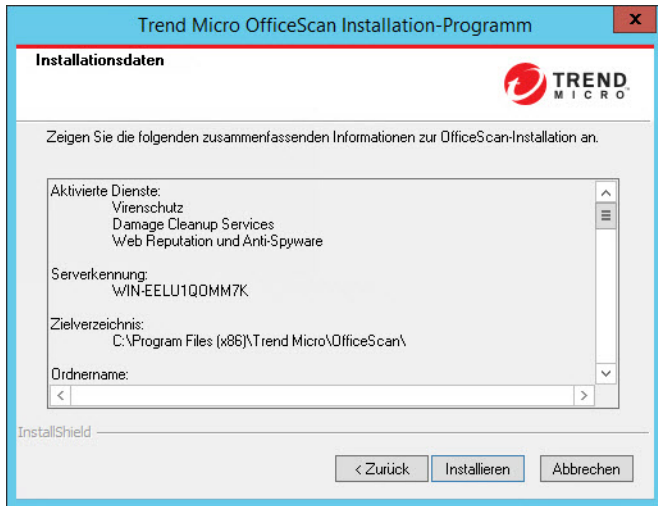


ABBILDUNG 3-22. Das Fenster mit den Installationsdaten

In diesem Fenster finden Sie eine Zusammenfassung der Installationseinstellungen. Überprüfen Sie die Installationsdaten, und klicken Sie auf **Zurück**, um Einstellungen oder Optionen zu ändern. Klicken Sie auf **Installieren**, um die Installation zu starten.

Der InstallShield Wizard ist abgeschlossen.

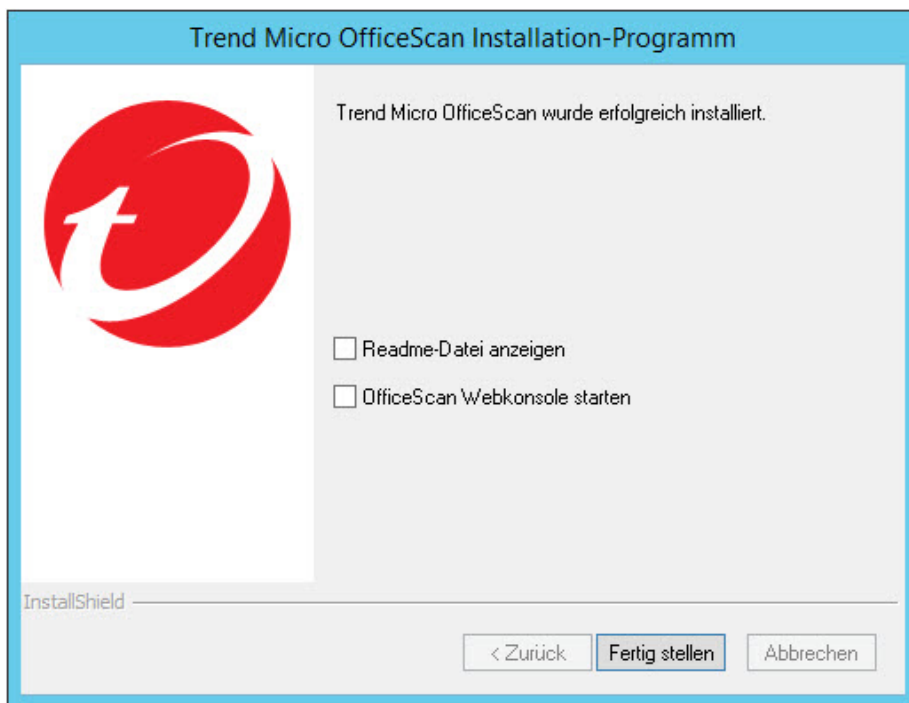


ABBILDUNG 3-23. Fenster "Der InstallShield Wizard ist abgeschlossen"

Lesen Sie nach Abschluss der Installation die Readme-Datei mit allgemeinen Informationen zum Produkt und den bekannten Problemen.

Administratoren können die Webkonsole starten, um die OfficeScan Einstellungen zu konfigurieren.

Aktualisieren von OfficeScan 11.x

Diese Version von OfficeScan bietet keine weitere Unterstützung für den Apache Webserver. Während eines Upgrades von OfficeScan 11.0, das den Apache-Server

verwendet, werden Sie von OfficeScan darüber informiert, dass das Setup-Programm die IIS Webserver-Rolle auf dem Server installiert. Nach Abschluss der Installation wird der Apache-Server von OfficeScan nicht mehr verwendet.



Wichtig

OfficeScan kann den Apache-Server nur durch den IIS-Server ersetzen, wenn Sie den Apache-Server mit Hilfe des vorherigen OfficeScan Installation-Programms installiert haben. Wenn Sie den Apache-Server manuell installiert haben, müssen Sie diesen vor dem Aktualisieren von OfficeScan deinstallieren.

Lizenzvereinbarung

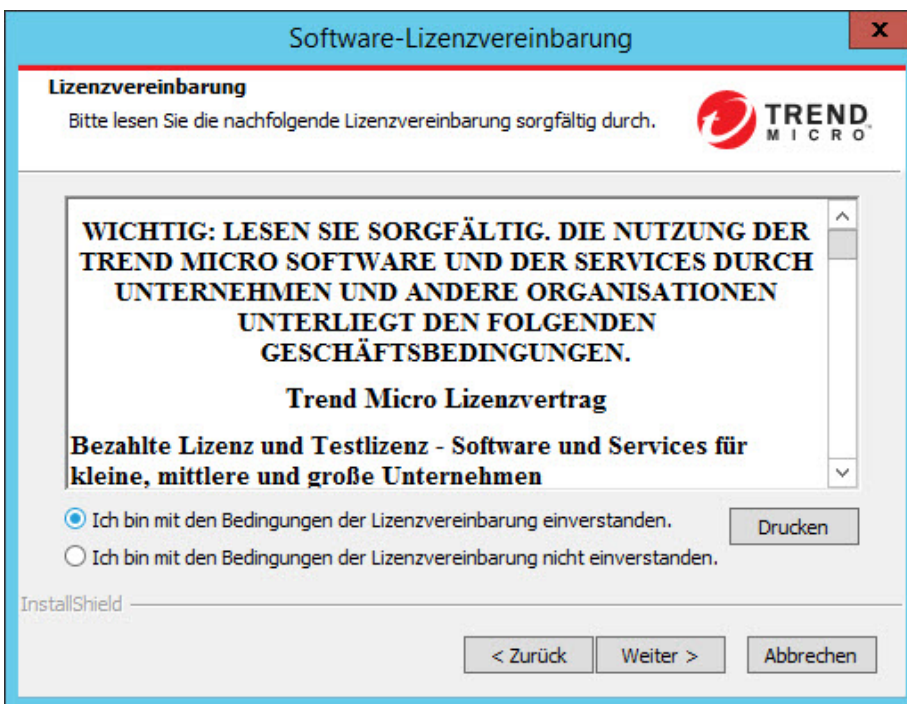


ABBILDUNG 3-24. Fenster "Lizenzvereinbarung"

Lesen Sie die Lizenzvereinbarung aufmerksam durch, und stimmen Sie den Bedingungen der Lizenzvereinbarung zu, um die Installation fortzusetzen. Die Installation kann nicht fortgesetzt werden, wenn Sie den Bedingungen der Lizenzvereinbarung nicht zustimmen.

Installationsziel

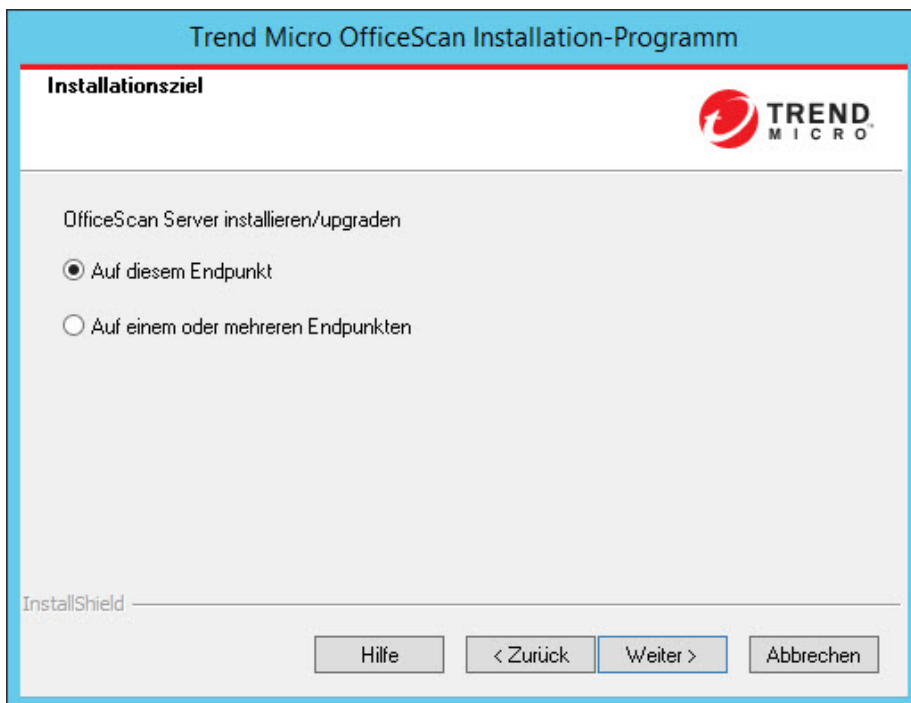


ABBILDUNG 3-25. Das Fenster "Installationsziel"

Führen Sie das Setup-Programm aus und installieren Sie den OfficeScan Server auf dem aktuellen Endpunkt oder auf anderen Endpunkten im Netzwerk. Wenn vom Setup-Programm eine frühere Version von OfficeScan auf dem Zielpunkt erkannt wird, wird bei der Installation automatisch ein Upgrade durchgeführt. Nur die folgenden Versionen von OfficeScan können auf diese Version aktualisiert werden:

- 11.0 Service Pack 1
- 11.0
- 10.6 Service Pack 3



Hinweis

Trend Micro empfiehlt dringend, alle verfügbaren Patches und Hotfixes auf den aktuellen OfficeScan Server vor dem Durchführen eines Upgrades anzuwenden.

Hinweise zum Remote-Upgrade

Beim Remote-Upgrade prüft Setup, ob der Zielendpunkt die Voraussetzungen für das Upgrade des Servers erfüllt. Bevor Sie den Vorgang fortsetzen:

- Sie müssen auf dem Zielendpunkt über Administratorrechte verfügen.
- Notieren Sie sich den Host-Namen und die Anmeldedaten (Benutzername und Kennwort) für die Zielendpunkte.
- Stellen Sie sicher, dass die Zielendpunkte die Anforderungen für die Installation des OfficeScan Servers erfüllen.
- Stellen Sie sicher, dass auf dem Endpunkt Microsoft IIS Server 7.0 oder höher installiert ist, wenn er als Webserver eingesetzt wird.

Bei lokalen Upgrades behält OfficeScan die Einstellungen der früheren Installation bei, einschließlich des Servernamens, der Angaben zum Proxy-Server und der Portnummern. Es ist nicht möglich, diese Einstellungen beim Upgrade zu ändern. Ändern Sie die Einstellungen nach dem Upgrade über die OfficeScan Webkonsole.



Wichtig

Beim Remote-Upgrade müssen alle Einstellungen erneut vorgenommen werden. Diese Einstellungen bleiben jedoch nach dem Server-Upgrade unberücksichtigt, da der Server die Einstellungen der vorherigen Version übernimmt.

Endpoint Prescan

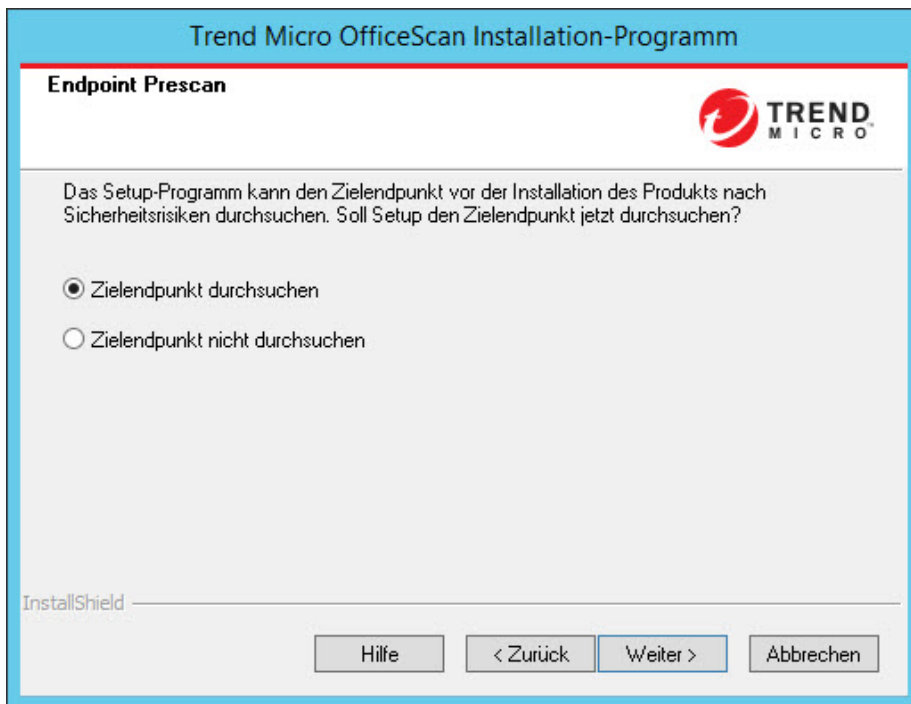


ABBILDUNG 3-26. Das Fenster "Endpoint Prescan"

Vor der Installation des OfficeScan Servers kann das Setup-Programm den Zielpunkt auf Viren und Malware überprüfen. Setup durchsucht die anfälligsten Bereiche des Endpunkts, wie beispielsweise:

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

Bei der Entdeckung von Viren/Malware und Trojanern kann Setup folgende Aktionen durchführen:

- **Löschen:** Löscht die infizierte Datei.
- **Säubern:** Eine Datei, die gesäubert werden kann, wird gesäubert, bevor der vollständige Zugriff möglich ist. Eine Datei, die nicht gesäubert werden kann, wird gemäß der festgelegten Aktion bearbeitet.
- **Umbenennen:** Die Erweiterung der infizierten Datei wird in *vir* geändert. Der Benutzer kann die 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:** Ermöglicht den vollständigen Zugriff auf die Datei, ohne sie zu verändern. Die Datei kann kopiert, gelöscht oder geöffnet werden.

Bei der lokalen Installation startet die Suche, wenn Sie auf **Weiter** klicken. Bei der Remote-Installation startet die Suche vor der eigentlichen Installation.



Wichtig

Während der lokalen Installation eines Upgrades werden Sie vom Setup-Programm aufgefordert, die Einstellungen für den Ransomware-Schutz zu aktualisieren, damit optimaler Schutz vor Ransomware-Bedrohungen gewährleistet werden kann.

Die Anwendung der aktualisierten Einstellungen wirkt sich nur auf Agents aus, die die Verhaltensüberwachung bereits aktiviert haben.

Warnung wegen Neustart des OfficeScan Agents

Das Setup-Programm bewertet die Ressourcen des Ziel-Endpunkts. Während eines Upgrade-Szenarios wird eine Warnung angezeigt, wenn das OfficeScan Agent-Programm auf dem Ziel-Endpunkt vorhanden ist.

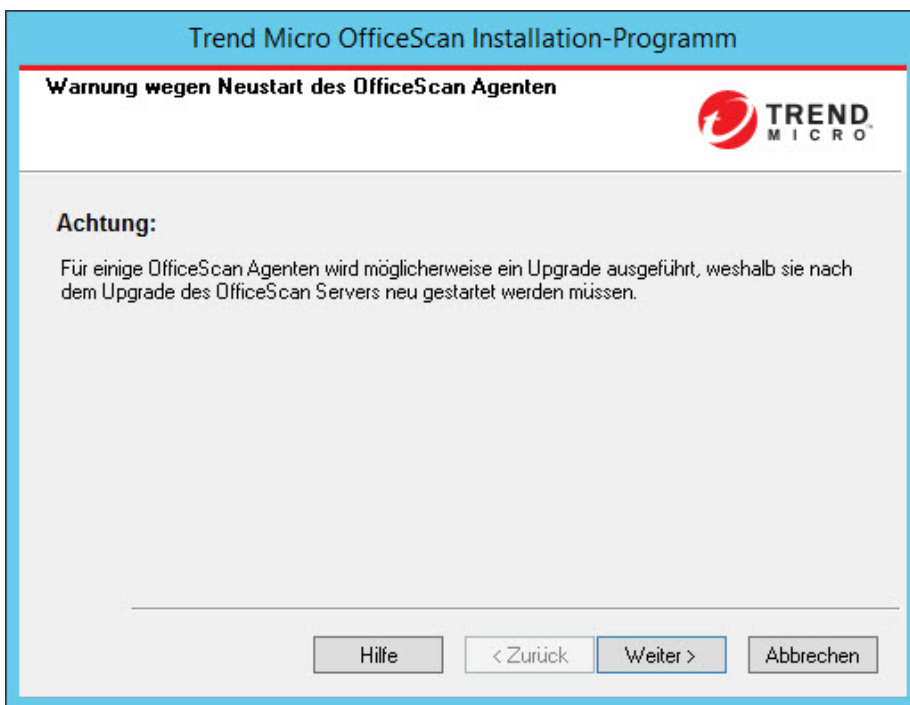


ABBILDUNG 3-27. Warnung wegen Neustart des OfficeScan Agents

Apache-Deinstallationswarnung

Beim Aktualisieren auf OfficeScan XG wird eine Warnung angezeigt, wenn der Apache Webserver für den vorherigen OfficeScan Server konfiguriert ist. OfficeScan bietet keine weitere Unterstützung für den Apache Webserver.

- Wenn Sie den Apache Webserver mit Hilfe des Setup-Programms in der Vorgängerversion von OfficeScan installiert haben, kann OfficeScan den

Webserver automatisch deinstallieren und den IIS Webserver während der Installation installieren.

- Wenn Sie den Apache Webserver vor der Installation der Vorgängerversion von OfficeScan manuell installiert haben, müssen Sie den Apache Webserver manuell deinstallieren, bevor Sie mit der Aktualisierung auf den OfficeScan Server fortfahren können.



Hinweis

Diese Warnung wird nicht angezeigt, wenn die Vorgängerversion des OfficeScan Servers mit dem IIS Webserver konfiguriert wurde.

Datenbanksicherung

Während Upgrades bietet das Setup-Programm die Möglichkeit, die OfficeScan Datenbank vor dem Upgrade auf die aktuelle Version zu sichern. Diese Sicherungsinformationen können Ihnen bei einem Rollback hilfreich sein.



Hinweis

Für das Sicherungspaket sind möglicherweise mehr als 300 MB freier Festplattenspeicher erforderlich.

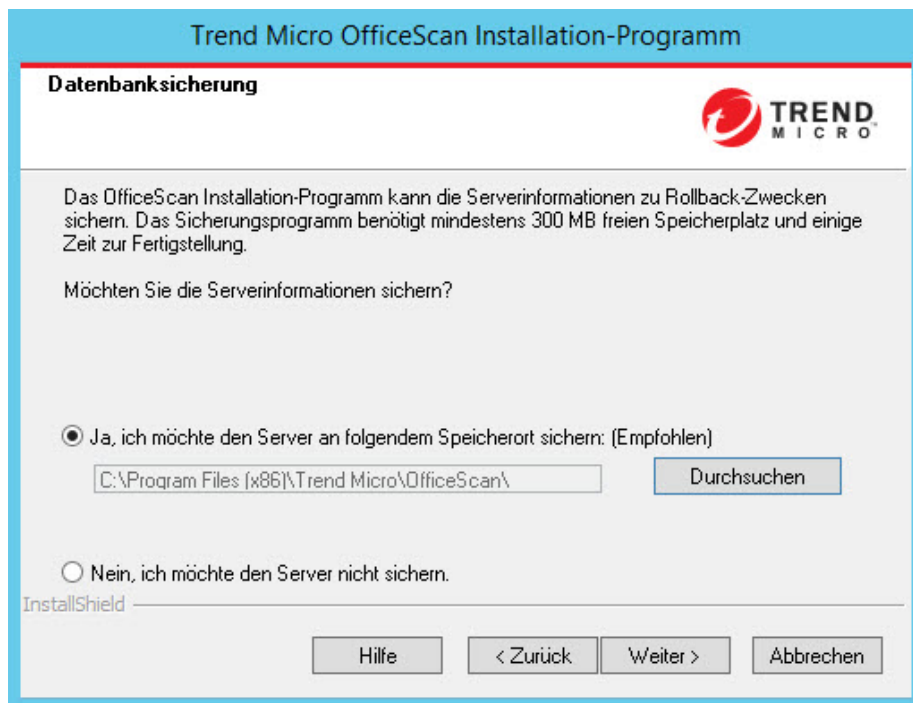


ABBILDUNG 3-28. Fenster „Datenbanksicherung“

OfficeScan Agent-Verteilung

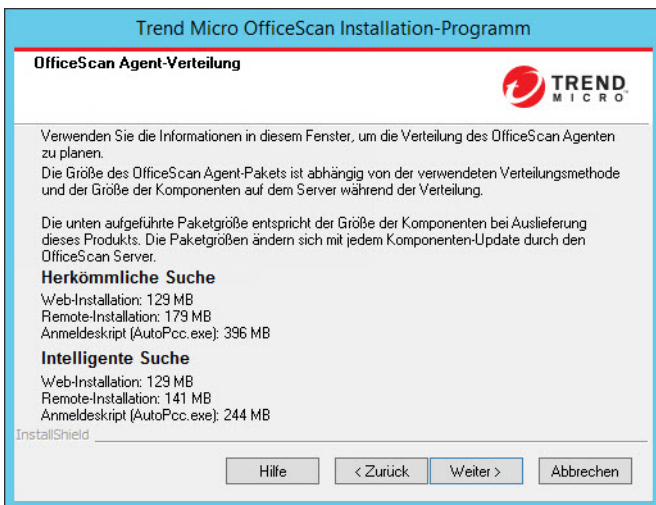


ABBILDUNG 3-29. Fenster "OfficeScan Agent-Verteilung"

Es gibt mehrere Methoden, um OfficeScan agents zu installieren oder zu aktualisieren. In diesem Fenster wird eine Liste der verschiedenen Verteilungsmethoden und der ungefähr erforderlichen Netzwerkbandbreite angezeigt.

Verwenden Sie dieses Fenster, um den auf den Servern benötigten Speicherplatz und die erforderliche Bandbreite für die Verteilung von agents auf die Ziel-Endpunkte abzuschätzen.



Hinweis

Für alle Installationsmethoden sind lokale Administrator- oder Domänenadministratorrechte auf den Ziel-Endpunkten erforderlich.

Installationsdaten

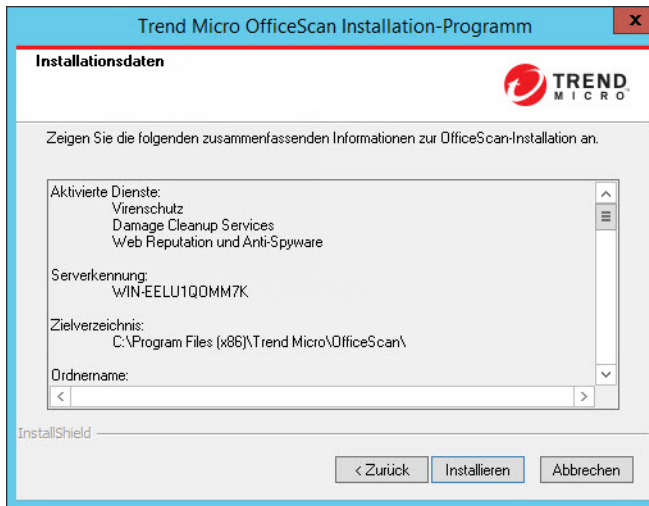


ABBILDUNG 3-30. Das Fenster mit den Installationsdaten

In diesem Fenster finden Sie eine Zusammenfassung der Installationseinstellungen. Überprüfen Sie die Installationsdaten, und klicken Sie auf **Zurück**, um Einstellungen oder Optionen zu ändern. Klicken Sie auf **Installieren**, um die Installation zu starten.

Der InstallShield Wizard ist abgeschlossen.

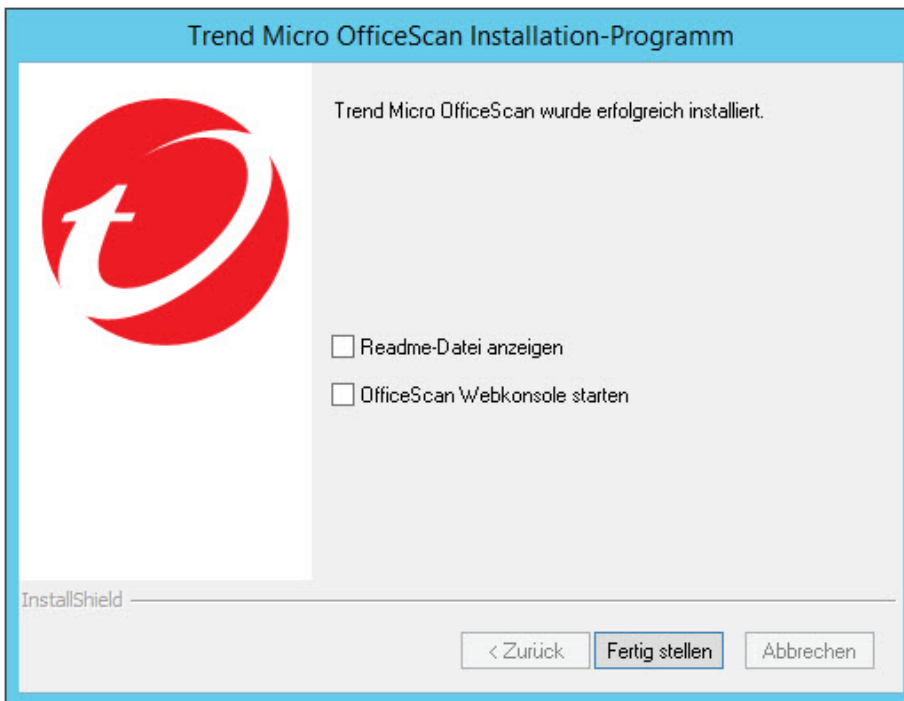


ABBILDUNG 3-31. Fenster "Der InstallShield Wizard ist abgeschlossen"

Lesen Sie nach Abschluss der Installation die Readme-Datei mit allgemeinen Informationen zum Produkt und den bekannten Problemen.

Administratoren können die Webkonsole starten, um die OfficeScan Einstellungen zu konfigurieren.

Durchführen eines Remote-Upgrades

Beim Durchführen eines Remote-Upgrades stellt OfficeScan mehrere Konfigurationsoptionen bereit, da nicht alle zuvor auf der Vorgängerversion des

OfficeScan Servers konfigurierten Einstellungen ermittelt werden können, bevor das Upgrade beginnt. Während des Upgrades überschreibt OfficeScan die Einstellungen, die Sie beim Upgrade-Setup konfigurieren, mit den Konfigurationseinstellungen der Vorgängerversion des OfficeScan Servers. Für Einstellungen, die nicht in der Vorgängerversion des OfficeScan Servers vorhanden sind, wendet OfficeScan die während des Upgrade-Setups konfigurierten Einstellungen an.



Wichtig

Das Setup-Programm unterstützt keine Remote-Upgrades von OfficeScan Servern, die den Apache Webserver verwenden. Sie müssen ein lokales Upgrade durchführen.

Lizenzvereinbarung

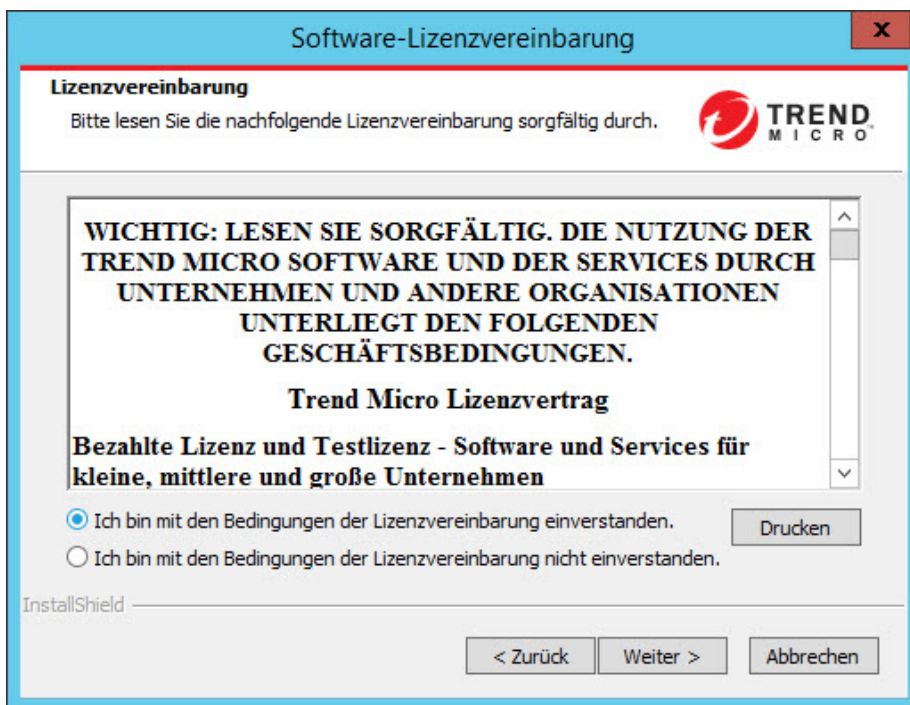


ABBILDUNG 3-32. Fenster "Lizenzvereinbarung"

Lesen Sie die Lizenzvereinbarung aufmerksam durch, und stimmen Sie den Bedingungen der Lizenzvereinbarung zu, um die Installation fortzusetzen. Die Installation kann nicht fortgesetzt werden, wenn Sie den Bedingungen der Lizenzvereinbarung nicht zustimmen.

Installationsziel

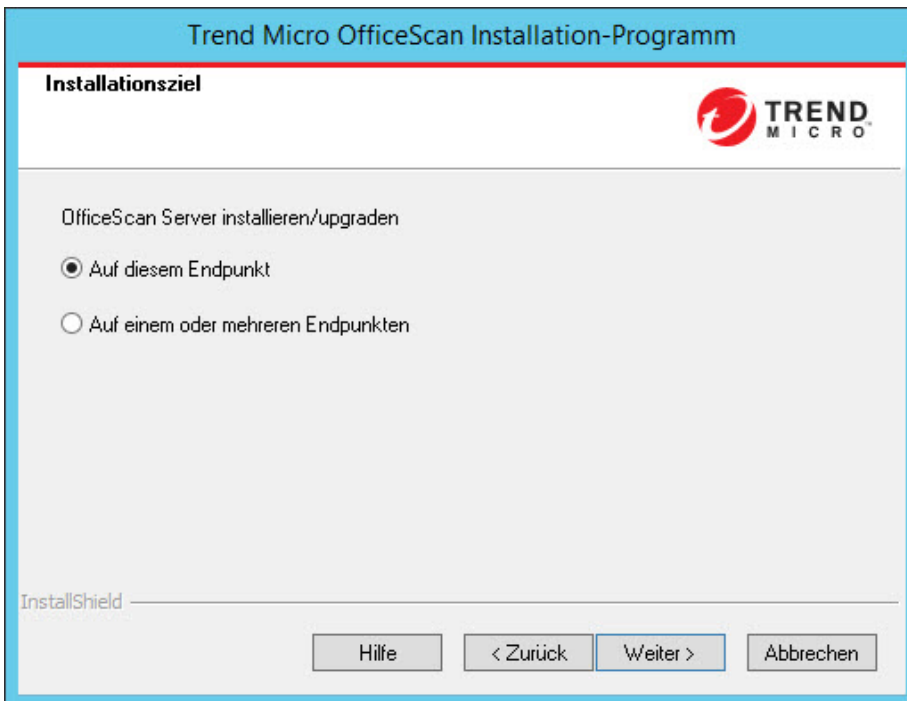


ABBILDUNG 3-33. Das Fenster "Installationsziel"

Führen Sie das Setup-Programm aus und installieren Sie den OfficeScan Server auf dem aktuellen Endpunkt oder auf anderen Endpunkten im Netzwerk. Wenn vom Setup-Programm eine frühere Version von OfficeScan auf dem Zielendpunkt erkannt wird, wird bei der Installation automatisch ein Upgrade durchgeführt. Nur die folgenden Versionen von OfficeScan können auf diese Version aktualisiert werden:

- 11.0 Service Pack 1
- 11.0
- 10.6 Service Pack 3

**Hinweis**

Trend Micro empfiehlt dringend, alle verfügbaren Patches und Hotfixes auf den aktuellen OfficeScan Server vor dem Durchführen eines Upgrades anzuwenden.

Hinweise zum Remote-Upgrade

Beim Remote-Upgrade prüft Setup, ob der Zielendpunkt die Voraussetzungen für das Upgrade des Servers erfüllt. Bevor Sie den Vorgang fortsetzen:

- Sie müssen auf dem Zielendpunkt über Administratorrechte verfügen.
- Notieren Sie sich den Host-Namen und die Anmeldedaten (Benutzername und Kennwort) für die Zielendpunkte.
- Stellen Sie sicher, dass die Zielendpunkte die Anforderungen für die Installation des OfficeScan Servers erfüllen.
- Stellen Sie sicher, dass auf dem Endpunkt Microsoft IIS Server 7.0 oder höher installiert ist, wenn er als Webserver eingesetzt wird.

Bei lokalen Upgrades behält OfficeScan die Einstellungen der früheren Installation bei, einschließlich des Servernamens, der Angaben zum Proxy-Server und der Portnummern. Es ist nicht möglich, diese Einstellungen beim Upgrade zu ändern. Ändern Sie die Einstellungen nach dem Upgrade über die OfficeScan Webkonsole.

**Wichtig**

Beim Remote-Upgrade müssen alle Einstellungen erneut vorgenommen werden. Diese Einstellungen bleiben jedoch nach dem Server-Upgrade unberücksichtigt, da der Server die Einstellungen der vorherigen Version übernimmt.

Endpoint Prescan

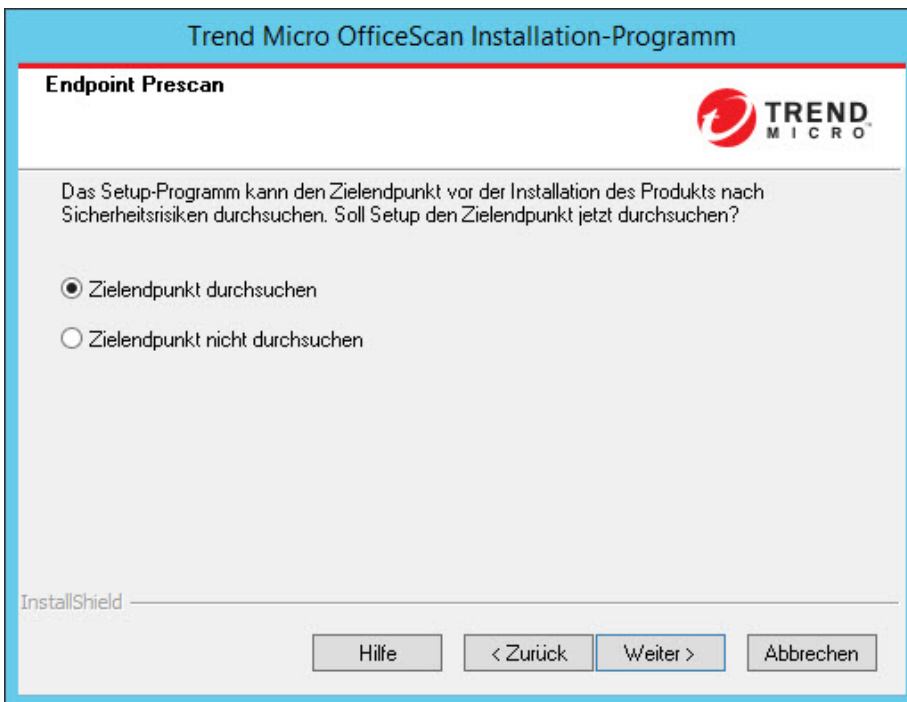


ABBILDUNG 3-34. Das Fenster "Endpoint Prescan"

Vor der Installation des OfficeScan Servers kann das Setup-Programm den Zielpunkt auf Viren und Malware überprüfen. Setup durchsucht die anfälligsten Bereiche des Endpunkts, wie beispielsweise:

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

Bei der Entdeckung von Viren/Malware und Trojanern kann Setup folgende Aktionen durchführen:

- **Löschen:** Löscht die infizierte Datei.
- **Säubern:** Eine Datei, die gesäubert werden kann, wird gesäubert, bevor der vollständige Zugriff möglich ist. Eine Datei, die nicht gesäubert werden kann, wird gemäß der festgelegten Aktion bearbeitet.
- **Umbenennen:** Die Erweiterung der infizierten Datei wird in `vir` geändert. Der Benutzer kann die 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:** Ermöglicht den vollständigen Zugriff auf die Datei, ohne sie zu verändern. Die Datei kann kopiert, gelöscht oder geöffnet werden.

Bei der lokalen Installation startet die Suche, wenn Sie auf **Weiter** klicken. Bei der Remote-Installation startet die Suche vor der eigentlichen Installation.



Wichtig

Während der lokalen Installation eines Upgrades werden Sie vom Setup-Programm aufgefordert, die Einstellungen für den Ransomware-Schutz zu aktualisieren, damit optimaler Schutz vor Ransomware-Bedrohungen gewährleistet werden kann.

Die Anwendung der aktualisierten Einstellungen wirkt sich nur auf Agents aus, die die Verhaltensüberwachung bereits aktiviert haben.

Installationspfad

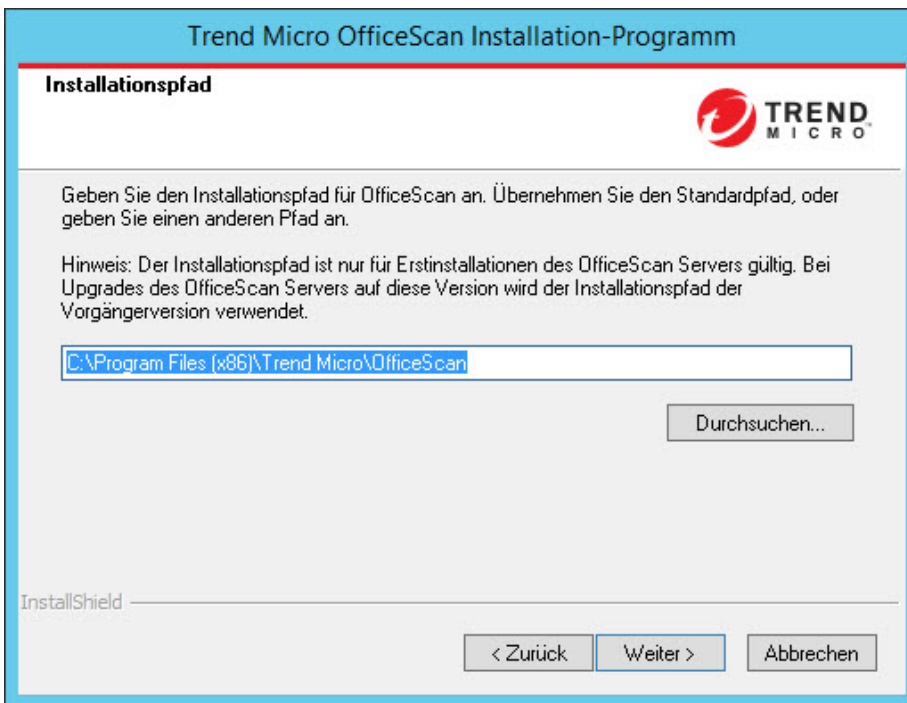


ABBILDUNG 3-35. Das Fenster "Installationspfad"

Übernehmen Sie den Standard-Installationspfad, oder geben Sie einen neuen Pfad an.

Der angegebene Installationspfad wird nur bei einer remote durchgeführten Erstinstallation angewendet. Bei remote durchgeführten Upgrades verwendet OfficeScan die Einstellungen aus der Vorgängerversion.

Proxy-Server

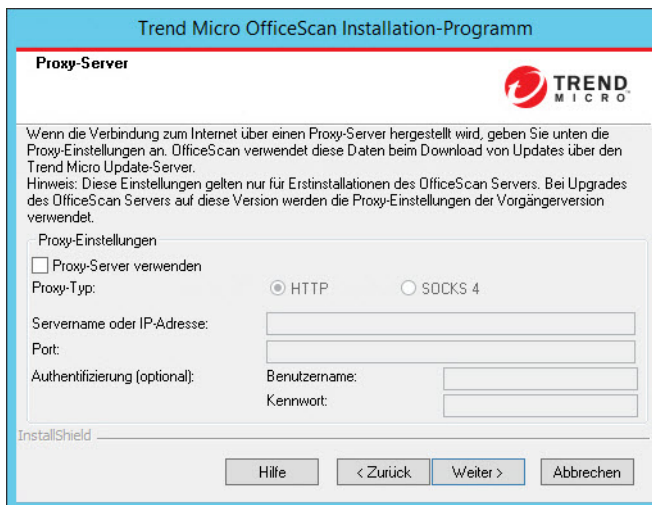


ABBILDUNG 3-36. Das Fenster "Proxy-Server"

Der OfficeScan Server verwendet für die Kommunikation zwischen agent und Server, für die Verbindung mit dem Trend Micro ActiveUpdate Server und für das Herunterladen von Updates das HTTP-Protokoll. Wenn Sie im Netzwerk den Zugriff auf das Internet über einen Proxy-Server steuern, benötigt OfficeScan die Proxy-Einstellungen zum Herunterladen von Updates vom ActiveUpdate Server.

Der Administrator kann die Proxy-Einstellungen auch nach der Installation über die OfficeScan Webkonsole eingeben.

Die Proxy-Einstellungen betreffen nur eine Remote-Erstinstallation. Bei remote durchgeführten Upgrades verwendet OfficeScan die Einstellungen aus der früheren Version.

**Hinweis**

Wenn Sie den OfficeScan Server auf einem reinen IPv6-Endpoint installieren, richten Sie einen Dual-Stack-Proxy-Server ein, der IP-Adressen umwandeln kann. Auf diese Weise kann der Server erfolgreich eine Verbindung zum ActiveUpdate Server herstellen.

Webserver

Trend Micro OfficeScan Installation-Programm

Webserver

Konfigurieren Sie den Webserver, der für den OfficeScan Server verwendet werden soll. OfficeScan verwendet SSL als Übertragungsprotokoll für die Webkonsole.

Hinweis: Die Einstellungen des Webserverns gelten nur für Erstinstallationen des OfficeScan Servers. Bei Upgrades des OfficeScan Servers auf diese Version werden die Einstellungen der Vorgängerversion verwendet.

IIS-Server:

HTTP-Port:

SSL-Einstellungen

Gültigkeitsdauer des Zertifikats: Jahr(e)

SSL-Port:

InstallShield

ABBILDUNG 3-37. Das Fenster "Webserver"

Der OfficeScan Webserver hostet die Webkonsole, nimmt Befehle von den agents entgegen und ermöglicht dem Administrator, CGI-Skripte (Common Gateway Interface) auszuführen. Der Webserver konvertiert diese Befehle in agent-CGI-Skripte und leitet sie an den OfficeScan Master Service weiter.

Die Webserver-Einstellungen betreffen nur eine Remote-Erstinstallation. Bei einem remote durchgeführten Upgrade verwendet OfficeScan die Einstellungen aus der Vorgängerversion.

IPv6-Unterstützung

Wählen Sie für Neuinstallationen den IIS-Server zum Aktivieren der IPv6-Unterstützung.

Wenn ein Upgrade auf diese OfficeScan Version durchgeführt wird, muss der zu aktualisierende OfficeScan Server bereits IIS verwenden.



Wichtig

Wenn Sie Apache mit Hilfe des Installationspakets des vorherigen OfficeScan Servers installiert haben, installiert und konfiguriert OfficeScan den IIS Webserver automatisch während des Upgrades. Wenn Sie den Apache-Server manuell installiert haben, müssen Sie diesen vor dem Aktualisieren des OfficeScan Servers manuell entfernen.

IIS-Unterstützung für Webserver

- Die folgenden Versionen von Microsoft Internet Information Server (IIS) sind erforderlich:
 - Version 7.0 unter Windows Server 2008
 - Version 7.5 unter Windows Server 2008 R2
 - Version 8.0 unter Windows Server 2012
 - Version 8.5 unter Windows Server 2012 R2
 - Version 10.0 unter Windows Server 2016

Der Webserver sollte auf keinem Endpunkt installiert werden, auf dem Anwendungen den IIS blockieren, da die Installation sonst fehlschlagen könnte. Weitere Informationen finden Sie in der Dokumentation des IIS.

HTTP-Port

Der Webserver hört den HTTP-Port auf agent-Anfragen ab und leitet diese an den OfficeScan Master Service weiter. Der Dienst sendet Informationen an agents auf dem

festgelegten agent-Kommunikationsport. Das Setup-Programm erzeugt bei der Installation eine zufällige Portnummer für die agent-Kommunikation.

SSL-Unterstützung

OfficeScan verwendet SSL (Secure Sockets Layer) für eine sichere Kommunikation zwischen der Webkonsole und dem Server. SSL bietet eine zusätzliche Schutzebene vor Hacker-Angriffen. Obwohl OfficeScan die in der Webkonsole festgelegten Kennwörter vor dem Versenden an den OfficeScan Server verschlüsselt, können Hacker das Paket auskundschaften und es ohne Entschlüsselung erneut senden, um Zugriff auf die Konsole zu erlangen. Im SSL-Tunnel ist das Paket bei der Weiterleitung über das Netzwerk vor Hacker-Übergriffen geschützt.

Die verwendete SSL-Version hängt von der Version ab, die der Webserver unterstützt.

Wenn Sie SSL auswählen, erstellt Setup automatisch ein für SSL-Verbindungen erforderliches SSL-Zertifikat. Das Zertifikat enthält Server-Angaben sowie einen öffentlichen und einen privaten Schlüssel.

Das SSL-Zertifikat sollte einen Gültigkeitszeitraum zwischen 1 und 20 Jahren haben. Der Administrator kann das Zertifikat auch nach Ablauf dieses Zeitraums verwenden. Es wird jedoch bei jedem Verbindungsaufbau mit diesem SSL-Zertifikat eine Warnmeldung angezeigt.

Der Ablauf einer SSL-Kommunikation:

1. Der Administrator sendet über die Webkonsole Daten per SSL-Verbindung an den Webserver.
2. Der Webserver antwortet der Webkonsole mit dem erforderlichen Zertifikat.
3. Der Browser führt die Schlüsselübergabe per RSA-Verschlüsselung durch.
4. Die Webkonsole sendet per RC4-Verschlüsselung Daten an den Webserver.

Die RSA-Verschlüsselung bietet zwar einen besonders wirksamen Schutz, verlangsamt jedoch den Kommunikationsfluss. Daher wird sie nur bei der Schlüsselübergabe eingesetzt. Die Datenweiterleitung wird über die schnellere Alternative RC4 verschlüsselt.

Webserver-Ports

Die folgende Tabelle enthält eine Liste der Standard-Portnummern für den Webserver.

TABELLE 3-2. Portnummern für den OfficeScan Webserver

WEBSERVER UND EINSTELLUNGEN	PORTS:	
	HTTP	HTTPS (SSL)
IIS Standard-Website mit aktiviertem SSL	80 (not configurable)	443 (not configurable)
IIS virtuelle Website mit aktiviertem SSL	8080 (configurable)	4343 (configurable)

Servererkennung

Trend Micro OfficeScan Installation-Programm

Servererkennung

Geben Sie an, ob OfficeScan Agents den Server über den Domänennamen oder die IP-Adresse ermitteln.

Trend Micro empfiehlt die Verwendung der IP-Adresse, wenn auf dem Server mehrere Netzwerkkarten vorhanden sind, und die Verwendung des vollqualifizierten Domänennamens (FQDN) oder Hostnamens, wenn es sich bei der IP-Adresse um eine dynamisch zugewiesene Adresse handelt.

☒ Vollqualifizierter Domänenname (FQDN) oder Hostname:

☐ IP-Adresse:

Tipp: Überprüfen Sie, ob der Domänenname aufgelöst werden kann, bevor Sie den Vorgang fortsetzen.

InstallShield

Hilfe < Zurück Weiter > Abbrechen

ABBILDUNG 3-38. Das Fenster "Servererkennung"

Die in diesem Fenster gewählte Option betrifft nur eine remote durchgeführte Erstinstallation. Bei einem remote durchgeführten Upgrade verwendet OfficeScan die Einstellungen aus der Vorgängerversion.

Legen Sie fest, ob OfficeScan agents den Server über den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN), Host-Namen (Domäne) oder die IP-Adresse identifizieren.

Die Kommunikation zwischen dem Server und den agents ist von der angegebenen IP-Adresse abhängig. Wenn Sie die IP-Adresse ändern, können die agents nicht mehr mit dem OfficeScan Server kommunizieren. Die Kommunikation kann dann nur durch eine erneute Verteilung aller agents wiederhergestellt werden. Dasselbe gilt für den Fall, dass der Server-Computer über einen Host-Namen ermittelt und dieser Host-Name dann geändert wird.

In den meisten Netzwerken ändert sich eher die IP-Adresse als der Hostname des Server-Computers. Der Server-Computer sollte deshalb vorzugsweise über den Hostnamen identifiziert werden.



Tip

Administratoren, die anstelle des Host-Namens die IP-Adresse verwenden, empfiehlt Trend Micro, die IP-Adresse (die vom DHCP-Server bezogen wurde) nach der Installation nicht zu ändern. Administratoren können weitere Kommunikationsprobleme mit OfficeScan Agents vermeiden, indem sie mit Hilfe derselben vom DHCP-Server bezogenen IP-Adressinformationen die IP-Adresskonfiguration (auf dem DHCP-Server) auf "Statisch" setzen.

Eine weitere Methode zur Beibehaltung der IP-Adresskonfiguration ist die ausschließliche Reservierung der IP-Adresse für den OfficeScan Server. Dadurch wird der DHCP-Server gezwungen, OfficeScan dieselbe IP-Adresse auch bei aktiviertem DHCP zuzuweisen.

Wenn Sie statische IP-Adressen verwenden, identifizieren Sie den Server über seine IP-Adresse. Sind außerdem mehrere Netzwerk-Schnittstellenkarten (NICs) auf dem Server vorhanden, sollte anstelle des Host-Namens eine entsprechende IP-Adresse verwendet werden, um eine erfolgreiche Kommunikation zwischen agent und Server zu gewährleisten.

IPv6-Unterstützung

Wenn der Server IPv4- und IPv6-agents verwaltet, muss er eine IPv4- und eine IPv6-Adresse aufweisen. Darüber hinaus müssen Administratoren den Server über seinen Host-Namen identifizieren. Wenn Administratoren den Server über seine IPv4-Adresse

identifizieren, können IPv6-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 Host-Namen oder seine IPv6-Adresse identifiziert werden. Wenn der Administrator den Server über seinen Host-Namen identifiziert, sollte er vorzugsweise den vollqualifizierten Domännennamen (FQDN) verwenden. Der Grund hierfür ist, dass ein WINS Server in einer reinen IPv6-Umgebung einen Hostnamen nicht in seine entsprechende IPv6-Adresse übersetzen kann.



Hinweis

Geben Sie den FQDN nur bei einer lokalen Installation des Servers an. Der FQDN wird für Remote-Installationen nicht unterstützt.

Registrierung und Aktivierung

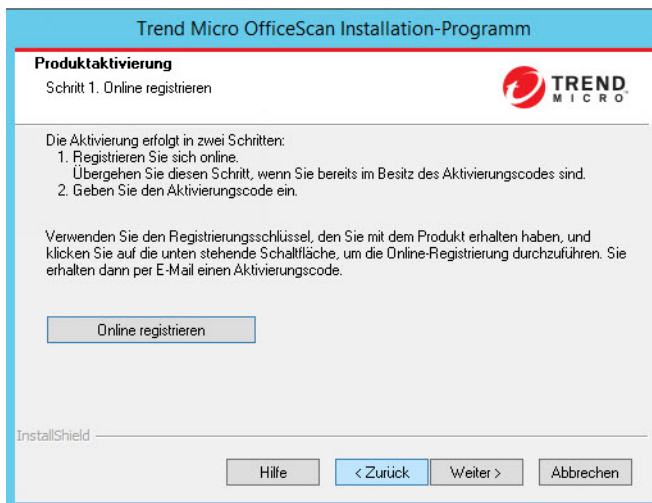


ABBILDUNG 3-39. Fenster "Produktaktivierung - Schritt 1"

Registrieren Sie OfficeScan über den Registrierungsschlüssel, den Sie mit dem Produkt erhalten haben. Die AktivierungsCodes werden Ihnen anschließend zugesendet. Überspringen Sie diesen Schritt, falls die AktivierungsCodes bereits zur Verfügung stehen.

Um die AktivierungsCodes anzufordern, klicken Sie auf **Online-Registrierung**. Das Setup-Programm öffnet die Registrierungswebsite von Trend Micro. Nachdem Sie das Registrierungsformular ausgefüllt haben, erhalten Sie von Trend Micro eine E-Mail mit den AktivierungsCodes. Fahren Sie nach dem Erhalt der Codes mit dem Installationsvorgang fort.

Wenn Sie den OfficeScan Server auf einem reinen IPv6-Endpunkt installieren, richten Sie einen Dual-Stack-Proxy-Server ein, der IP-Adressen umwandeln kann. Auf diese Weise kann der Server erfolgreich eine Verbindung zur Registrierungswebsite von Trend Micro herstellen.

ABBILDUNG 3-40. Fenster "Produktaktivierung - Schritt 2"

Geben Sie die AktivierungsCodes ein. Achten Sie bei der Eingabe auf Groß- und Kleinschreibung.

Wenn der Aktivierungscode für alle Dienste gültig ist:

1. Geben Sie im Textfeld **Antivirus** den Aktivierungscode ein.
2. Wählen Sie **Verwenden Sie den gleichen Aktivierungscode für Damage Cleanup Services, für Web Reputation und für Anti-Spyware** aus.
3. Klicken Sie auf **Weiter**, und überprüfen Sie die Lizenzdaten.

OfficeScan Agent-Verteilung

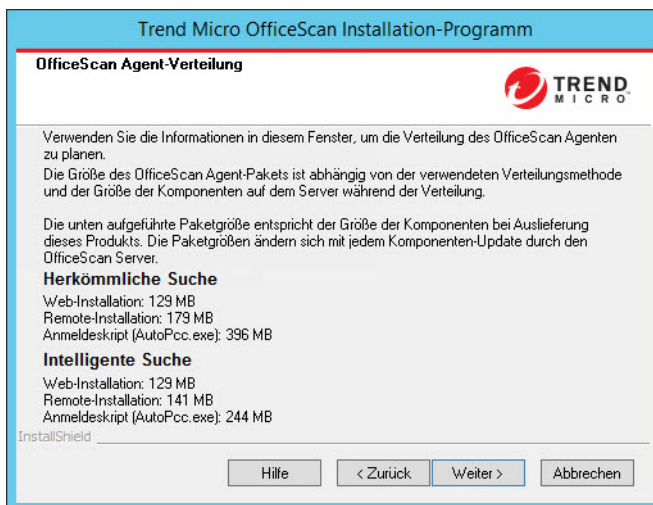


ABBILDUNG 3-41. Fenster "OfficeScan Agent-Verteilung"

Es gibt mehrere Methoden, um OfficeScan agents zu installieren oder zu aktualisieren. In diesem Fenster wird eine Liste der verschiedenen Verteilungsmethoden und der ungefähr erforderlichen Netzwerkbandbreite angezeigt.

Verwenden Sie dieses Fenster, um den auf den Servern benötigten Speicherplatz und die erforderliche Bandbreite für die Verteilung von agents auf die Ziel-Endpunkte abzuschätzen.

**Hinweis**

Für alle Installationsmethoden sind lokale Administrator- oder Domänenadministratorrechte auf den Ziel-Endpunkten erforderlich.

Integrierten Smart Protection Server installieren

**Hinweis**

Dieses Fenster wird nicht angezeigt, wenn Sie eine virtuelle IIS-Website während der Updateinstallationen verwenden.



ABBILDUNG 3-42. Das Fenster "Integrierten Smart Protection Server installieren"

Das Setup-Programm kann den integrierten Smart Protection Server auf dem Ziel-Endpunkt installieren. Der integrierte Server bietet File-Reputation-Dienste für agents mit intelligenter Suche sowie Web-Reputation-Dienste für agents, die den Web-Reputation-Richtlinien unterliegen. Sie können den integrierten Server über die OfficeScan Webkonsole verwalten.

Trend Micro empfiehlt die Installation des eigenständigen Smart Protection Servers, der über die gleichen Funktionen wie der integrierte Server verfügt, aber mehreren agents

dienen kann. Der eigenständige Server wird separat installiert und hat eine eigene Management-Konsole. Weitere Informationen zum eigenständigen Server finden Sie im *Trend Micro Smart Protection Server Administratorhandbuch*.

**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. Weitere Informationen zum Konfigurieren von Smart Protection Quellen für Agents finden Sie im *Administratorhandbuch*.

Agent-Verbindungsprotokolle für File-Reputation-Dienste

OfficeScan Agents können sich über HTTP und HTTPS mit den File-Reputation-Diensten des integrierten Smart Protection Servers verbinden. HTTPS ermöglicht eine sicherere Verbindung, während HTTP weniger Bandbreite benötigt.

**Hinweis**

Wenn Endpunkte die Verbindung zum integrierten Server über einen Proxy-Server aufbauen, müssen die internen Proxy-Einstellungen über die Webkonsole konfiguriert werden. Weitere Informationen zum Konfigurieren von Proxy-Einstellungen finden Sie im *Administratorhandbuch*.

Die für File-Reputation-Dienste verwendeten Portnummern richten sich nach dem Webserver, den der OfficeScan Server verwendet. Weitere Informationen finden Sie unter *Webserver auf Seite 2-15*.

Der HTTP-Port wird im Installationsfenster nicht angezeigt. Der HTTPS-Port wird angezeigt; seine Konfiguration ist jedoch optional.

TABELLE 3-3. Ports für die File-Reputation-Dienste des integrierten Smart Protection Servers

WEBSERVER UND EINSTELLUNGEN	PORTS FÜR FILE-REPUTATION-DIENSTE	
	HTTP	HTTPS (SSL)
IIS-Standard-Website	80	443
Virtuelle IIS-Website	8080	4343

Integrierter Server nicht installiert

Wenn Sie eine Erstinstallation durchführen und nicht ausgewählt haben, den integrierten Server zu installieren:

- Die herkömmliche Suche wird zur standardmäßigen Suchmethode.
- Wenn Sie die Web-Reputation-Richtlinien in einem separaten Installationsfenster aktivieren (ausführliche Hinweise finden Sie unter [Web-Reputation-Funktion auf Seite 2-39](#)), können agents keine Web-Reputation-Abfragen senden, da OfficeScan davon ausgeht, dass kein Smart Protection Server installiert wurde.

Falls ein eigenständiger Server nach der Installation von OfficeScan verfügbar ist, führen Sie die folgenden Aufgaben über die OfficeScan Webkonsole durch:

- Ändern Sie die Suchmethode in die intelligente Suche.
- Fügen Sie den eigenständigen Server zur Liste der Smart Protection Quellen hinzu, sodass agents File- und Web-Reputation-Abfragen an den Server senden können.

Bei der Aktualisierung von OfficeScan Servern der Version 10.x, bei denen der integrierte Server deaktiviert ist, wird der integrierte Server nicht installiert. OfficeScan Agents behalten die Suchmethoden und die Smart Protection Quellen bei, an die sie Abfragen senden.

Installationsziel

ABBILDUNG 3-43. Das Fenster "Installationsziel"

Geben Sie den Zielendpunkt an, auf dem OfficeScan installiert wird. Geben Sie manuell den Hostnamen oder die IP-Adresse des Endpunkts ein. Klicken Sie auf **Durchsuchen**, um nach Endpunkten im Netzwerk zu suchen.

Importieren Sie die Endpunktnamen aus einer Textdatei, indem Sie auf **Liste importieren** klicken. Wenn der OfficeScan Server auf mehreren Endpunkten gleichzeitig installiert wird und alle Endpunkte die Analyse erfolgreich durchlaufen, erfolgt die Installation nach der Reihenfolge der Endpunkte in der Textdatei.

In der Textdatei:

- Tragen Sie pro Zeile einen Endpunktnamen ein.
- Verwenden Sie das UNC-Format (Unified Naming Convention) (z. B. \\test).
- Verwenden Sie nur die folgenden Zeichen: a-z, A-Z, 0-9, Punkte (.) und Gedankenstriche (-).

Beispiel:

\\domäne1\test-abc

\\domain2\test-123

Hinweise zur Durchführung der Remote-Installation:

- Sie müssen auf dem Zielendpunkt über Administratorrechte verfügen.
- Notieren Sie sich den Host-Namen und die Anmeldedaten des Endpunkts (Benutzername und Kennwort).
- Stellen Sie sicher, dass die Zielendpunkte die Systemanforderungen für die Installation des OfficeScan Servers erfüllen.
- Stellen Sie sicher, dass auf dem Endpunkt Microsoft IIS Server 7.0 oder höher installiert ist, wenn er als Webserver eingesetzt wird.
- Der Endpunkt, auf dem Setup ausgeführt wird, darf nicht als Zielendpunkt angegeben werden. Starten Sie stattdessen die lokale Installation auf dem Endpunkt.

Klicken Sie nach der Angabe der Zielendpunkte auf **Weiter**. Das Setup-Programm überprüft, ob die angegebenen Endpunkte die Installationsvoraussetzungen von OfficeScan erfüllen.

Analyse des Zielpunkts

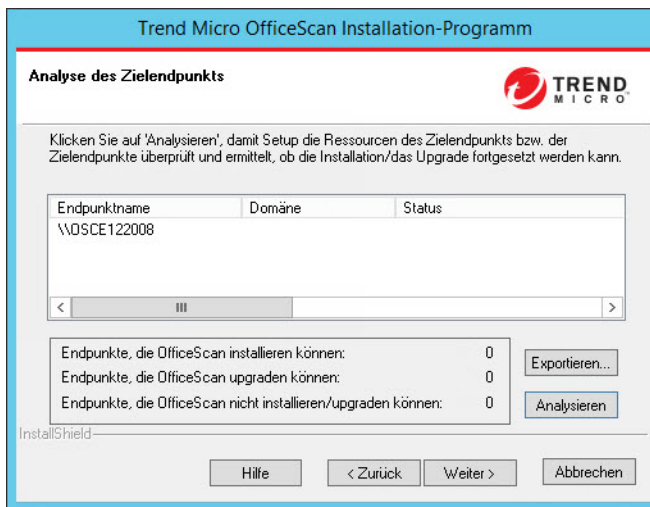


ABBILDUNG 3-44. Das Fenster "Analyse des Zielpunkts"



Wichtig

Das Setup-Programm unterstützt keine Remote-Upgrades von OfficeScan Servern, die den Apache Webserver verwenden. Sie müssen den Apache Webserver manuell deinstallieren, bevor Sie ein Remote-Upgrade von OfficeScan durchführen.

Vor der Durchführung der Remote-Installation muss das Setup-Programm überprüfen, ob der OfficeScan Server auf den ausgewählten Zielpunkten installiert werden kann. Starten Sie die Überprüfung durch Klicken auf **Analysieren**. Setup fordert Sie möglicherweise zur Eingabe des Administrator-Benutzernamens und -kennworts zur Anmeldung beim Zielpunkt auf. Nach der Analyse zeigt Setup das Ergebnis auf dem Bildschirm an.



Wichtig

Während der Serveranalyse werden Sie vom Setup-Programm aufgefordert, die Einstellungen für den Ransomware-Schutz zu aktualisieren, damit optimaler Schutz vor Ransomware-Bedrohungen gewährleistet ist.

Die Anwendung der aktualisierten Einstellungen wirkt sich nur auf Agents aus, die die Verhaltensüberwachung bereits aktiviert haben.

Bei der Installation auf mehreren Endpunkten wird die Installation fortgesetzt, wenn mindestens einer der Endpunkte die Voraussetzungen erfüllt. Das Setup-Programm installiert den OfficeScan Server auf diesem Endpunkt und ignoriert die Endpunkte, die die Analyse nicht erfolgreich durchlaufen haben.

Der Fortschritt der Remote-Installation wird nur auf dem Endpunkt angezeigt, auf dem Setup ausgeführt wird, und nicht auf den Zielpunkten.

Warnung wegen Neustart des OfficeScan Agents

Das Setup-Programm bewertet die Ressourcen des Ziel-Endpunkts. Während eines Upgrade-Szenarios wird eine Warnung angezeigt, wenn das OfficeScan Agent-Programm auf dem Ziel-Endpunkt vorhanden ist.

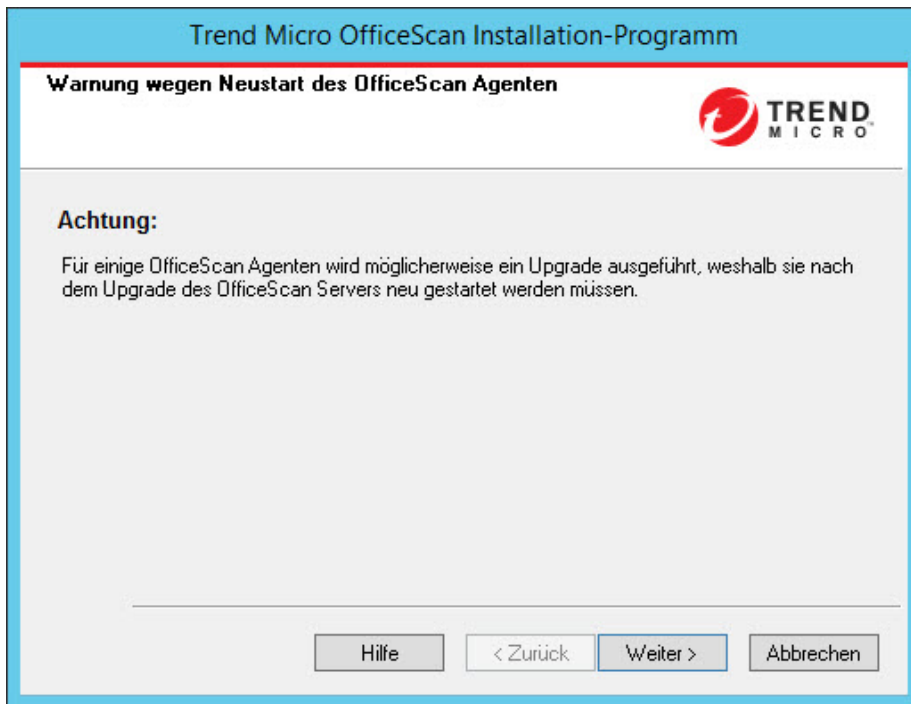


ABBILDUNG 3-45. Warnung wegen Neustart des OfficeScan Agents

Datenbanksicherung

Während Upgrades bietet das Setup-Programm die Möglichkeit, die OfficeScan Datenbank vor dem Upgrade auf die aktuelle Version zu sichern. Diese Sicherungsinformationen können Ihnen bei einem Rollback hilfreich sein.

**Hinweis**

Für das Sicherungspaket sind möglicherweise mehr als 300 MB freier Festplattenspeicher erforderlich.

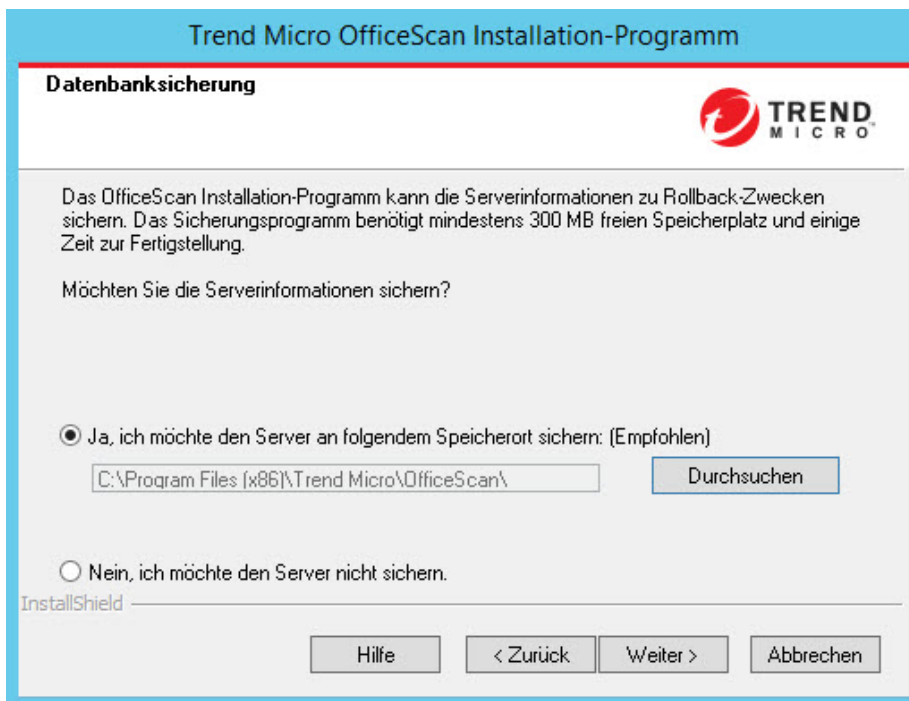


ABBILDUNG 3-46. Fenster „Datenbanksicherung“

Serverauthentifizierungszertifikat

Das Setup-Programm versucht, bisher vorhandene Authentifizierungszertifikate während der Installation zu entdecken. Ist bereits ein Zertifikat vorhanden, ordnet OfficeScan die Datei automatisch im Fenster **Serverauthentifizierungszertifikat** zu. Wenn kein Zertifikat vorhanden ist, verwendet OfficeScan standardmäßig die Option **Neues Authentifizierungszertifikat generieren**.



Hinweis

Während der Durchführung von Upgrade-Installationen über einen Remote-Standort wird das Fenster **Serverauthentifizierungszertifikat** nur angezeigt, wenn ein OfficeScan 10.6 SP3 Server aktualisiert wird.

Trend Micro OfficeScan Installation-Programm

Serverauthentifizierungszertifikat

TREND MICRO

Erlauben Sie OfficeScan, ein neues Zertifikat für die Kommunikation mit OfficeScan Agenten zu generieren, oder importieren Sie ein vorhandenes Zertifikat.
Hinweis: OfficeScan erstellt eine Sicherung des neuen oder importierten Zertifikats im Ordner <Server_installation_folder>\AuthCertBackup\.

☒ Neues Authentifizierungszertifikat generieren

Sicherungskennwort:

Kennwort bestätigen:

☐ Vorhandenes Zertifikat importieren

Hinweis: Bei dem Zertifikat handelt es sich entweder um ein ZIP-Paket, das vom Zertifikat-Manager für Serverauthentifizierung generiert wurde, oder eine korrekt formatierte PFX-Datei.

Kennwort:

InstallShield

ABBILDUNG 3-47. Fenster "Serverauthentifizierungszertifikat" für neue Zertifikate

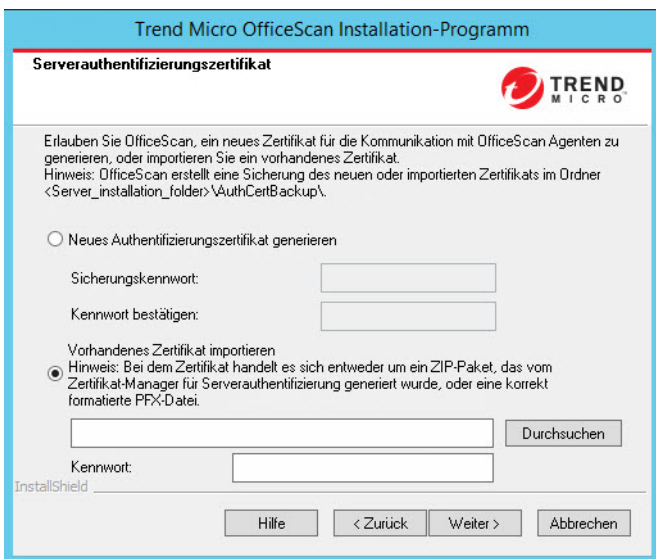


ABBILDUNG 3-48. Fenster "Serverauthentifizierungszertifikat" für bisher vorhandene Zertifikate

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.

OfficeScan kann das Authentifizierungszertifikat während der Installation erzeugen. Alternativ können Administratoren ein bereits vorhandenes Authentifizierungszertifikat von einem anderen OfficeScan Server importieren.



Tipp

Trend Micro empfiehlt, das Zertifikat beim Sichern mit einem Kennwort zu verschlüsseln.

Installationsdaten

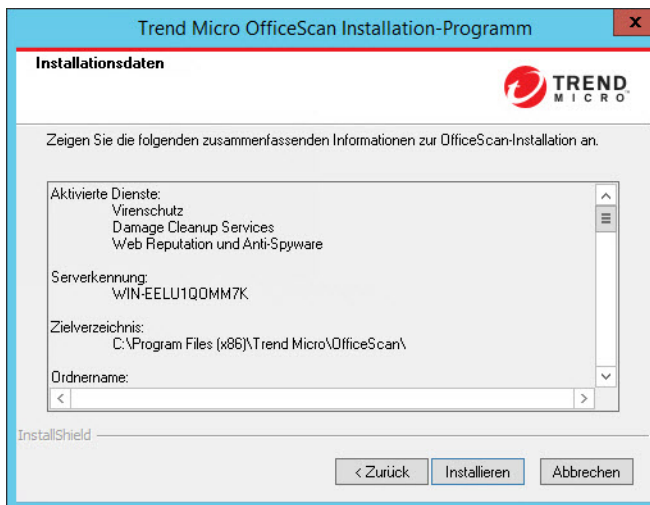


ABBILDUNG 3-49. Das Fenster mit den Installationsdaten

In diesem Fenster finden Sie eine Zusammenfassung der Installationseinstellungen. Überprüfen Sie die Installationsdaten, und klicken Sie auf **Zurück**, um Einstellungen oder Optionen zu ändern. Klicken Sie auf **Installieren**, um die Installation zu starten.

Der InstallShield Wizard ist abgeschlossen.

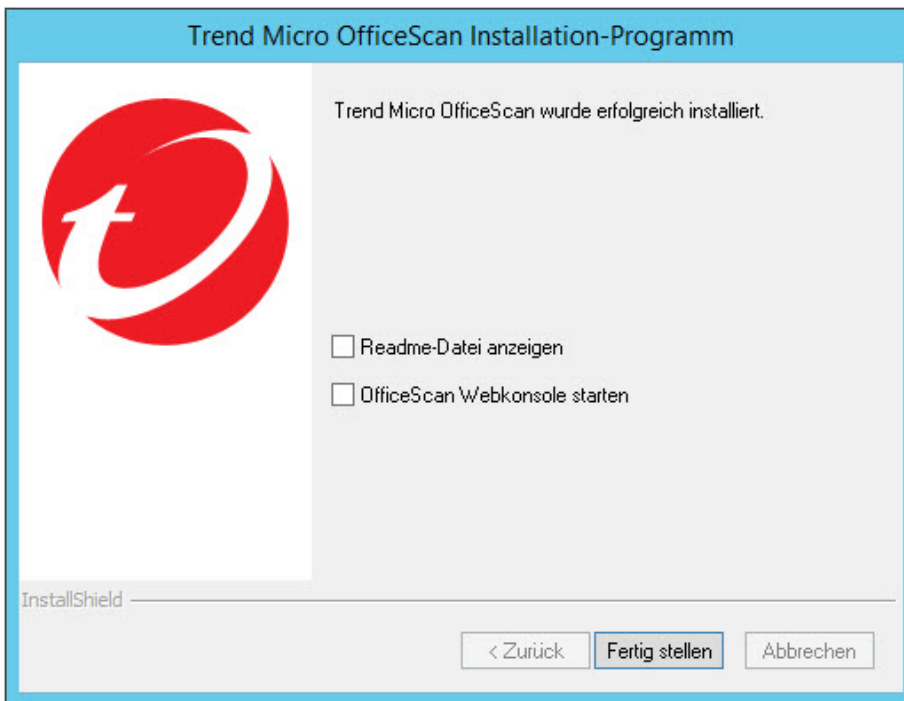


ABBILDUNG 3-50. Fenster "Der InstallShield Wizard ist abgeschlossen"

Lesen Sie nach Abschluss der Installation die Readme-Datei mit allgemeinen Informationen zum Produkt und den bekannten Problemen.

Administratoren können die Webkonsole starten, um die OfficeScan Einstellungen zu konfigurieren.

Kapitel 4

Aufgaben nach der Installation

Führen Sie nach Abschluss der Installation des OfficeScan Servers folgende Aufgaben durch:

Themen in diesem Kapitel:

- *Die Installation oder das Upgrade des Servers überprüfen auf Seite 4-2*
- *Aktualisieren von OfficeScan Komponenten auf Seite 4-5*
- *Standardeinstellungen überprüfen auf Seite 4-5*
- *OfficeScan beim Control Manager registrieren auf Seite 4-6*

Die Installation oder das Upgrade des Servers überprüfen

Überprüfen Sie nach Abschluss der Installation oder der Aktualisierung Folgendes:

TABELLE 4-1. Nach der Installation von OfficeScan zu überprüfende Elemente

ZU ÜBERPRÜFENDES ELEMENT	DETAILS
Tastenkombinationen des OfficeScan Servers	Die Tastenkombinationen für den Trend Micro OfficeScan Server werden im Windows-Menü Start des Servers angezeigt.
Programmliste	Der Trend Micro OfficeScan Server wird in der Systemsteuerung des Servers in der Liste Software aufgeführt.
OfficeScan Webkonsole	Geben Sie die folgende URL im Internet Explorer ein: • HTTPS-Verbindung: <code>https://<OfficeScan Server-Name>:<Portnummer>/OfficeScan</code> Wobei <OfficeScan Server-Name> für den Namen oder die IP-Adresse des OfficeScan Servers steht. Das Anmeldefenster der OfficeScan Webkonsole wird angezeigt.

ZU ÜBERPRÜFENDES ELEMENT	DETAILS
OfficeScan Server-Dienste	Folgende OfficeScan Server-Dienste werden in der Microsoft Management-Konsole aufgeführt: • OfficeScan Active Directory Integration Service: Dieser Dienst zeigt an, ob die Active Directory Integration und die rollenbasierte Administration korrekt funktionieren. • OfficeScan Control Manager Agent: Der Status dieses Dienstes sollte "Gestartet" lauten, wenn der OfficeScan Server bei Control Manager registriert wurde. • OfficeScan Deep Discovery Service: Der Status dieses Dienstes sollte "Gestartet" lauten. • OfficeScan Master Service: Der Status dieses Dienstes sollte "Gestartet" lauten. • OfficeScan Log Receiver Service: Der Status dieses Dienstes sollte "Gestartet" lauten. • OfficeScan Plug-in Manager: Der Status dieses Dienstes sollte "Gestartet" lauten. • Trend Micro Smart Scan Server: Der Status dieses Dienstes sollte "Gestartet" lauten. • Trend Micro Local Web Classification Server: Der Status dieses Dienstes sollte "Gestartet" lauten, wenn während der Installation "Web-Reputation-Dienste" aktiviert wurde.
OfficeScan Server-Prozesse	Wenn Sie den Windows Task-Manager öffnen, wird "DBServer.exe" ausgeführt.
Server-Installationsprotokoll	Das Protokoll der Server-Installation, OFCMAS.LOG, befindet sich im Verzeichnis %windir%.

ZU ÜBERPRÜFENDES ELEMENT	DETAILS
Registrierungsschlüssel	Es sind folgende Registrierungsschlüssel vorhanden: - Für 32-Bit-Plattformen: <code>HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan</code> - Für 64-Bit-Plattformen: <code>HKEY_LOCAL_MACHINE\Software\Wow6432Node\TrendMicro\OfficeScan</code>
Programmordner	Die OfficeScan Server-Dateien befinden sich im <Installationsordner des Servers>.

Überprüfen der Installation des integrierten Smart Protection Servers

OfficeScan installiert automatisch den integrierten Smart Protection Server während einer Erstinstallation.

Prozedur

1. Navigieren Sie in der Webkonsole des Servers zu **Administration > Smart Protection > Smart Protection Quellen**.
2. Klicken Sie auf den Link **Standardliste**.
3. Klicken Sie im daraufhin angezeigten Fenster auf **Integrierter Smart Protection Server**.
4. Klicken Sie im nächsten Fenster auf **Verbindung testen**.

Die Verbindung mit dem integrierten Server sollte hergestellt werden.

Aktualisieren von OfficeScan Komponenten

Aktualisieren Sie nach der Installation von OfficeScan die Komponenten auf dem Server.



Hinweis

In diesem Abschnitt wird ein manuelles Update erläutert. Informationen über das zeitgesteuerte Update und Update-Konfigurationen finden Sie in der *Hilfe zum OfficeScan Server*.

Den OfficeScan Server aktualisieren

Prozedur

1. Melden Sie sich an der Webkonsole an.
 2. Klicken Sie im Hauptmenü auf **Updates > Server > Manuelles Update**.

Das Fenster **Manuelles Update** wird angezeigt. Es enthält eine Übersicht über die aktuellen Komponenten, Versionsnummern und das Datum des letzten Updates.
 3. Wählen Sie die zu aktualisierenden Komponenten aus.
 4. Klicken Sie auf **Aktualisieren**. Der Server sucht auf dem Update-Server nach aktualisierten Komponenten. Der Verlauf und der Status des Updates werden angezeigt.
-

Standardeinstellungen überprüfen

OfficeScan wird mit Standardeinstellungen installiert. Falls diese Einstellungen nicht Ihren Sicherheitsanforderungen entsprechen, ändern Sie die Einstellungen auf der Webkonsole. Weitere Informationen zu den Einstellungen, die Sie auf der Webkonsole vornehmen können, finden Sie in der *OfficeScan Server-Hilfe* und im *Administratorhandbuch*.

Sucheinstellungen

OfficeScan stellt verschiedene Suchtypen bereit, mit denen Sie Endpunkte vor Sicherheitsrisiken schützen können. Ändern Sie die Sucheinstellungen über die Webkonsole, indem Sie zu **Agents > Agent-Verwaltung** navigieren und auf **Einstellungen > {Suchtyp}** klicken.

Agent Einstellungen

In OfficeScan stehen verschiedene Einstellungsarten zur Verfügung, die für alle beim Server registrierten agents oder für alle agents mit einer bestimmten Berechtigung gelten. Ändern Sie agent-Einstellungen über die Webkonsole, indem Sie zu **Agents > Globale Agent-Einstellungen** wechseln.

Agent-Berechtigungen

Zu den Standardberechtigungen eines agents gehören das Anzeigen des Taskleistensymbols auf dem OfficeScan Agent-Endpunkt. Ändern Sie Standardberechtigungen für den agent über die Webkonsole.

1. Navigieren Sie zu **Agents > Agent-Verwaltung**.
2. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**.

OfficeScan beim Control Manager registrieren

Wenn ein Control Manager Server neu installierte OfficeScan Server verwaltet, registrieren Sie OfficeScan nach der Installation bei Control Manager.



Hinweis

Control Manager Registrierung gilt nur für neu installierte OfficeScan Server.

Navigieren Sie auf der OfficeScan Webkonsole zu **Administration > Einstellungen > Control Manager**.

Weitere Informationen zu diesem Verfahren finden Sie in der *OfficeScan Server-Hilfe* oder im *OfficeScan Administratorhandbuch*.

Kapitel 5

Deinstallieren und Rollback von OfficeScan

In diesem Kapitel werden die Schritte beschrieben, die für Deinstallation oder das Rollback von Trend Micro™ OfficeScan™ notwendig sind.

Themen in diesem Kapitel:

- *Überlegungen zu Deinstallation und Rollback auf Seite 5-2*
- *Vor der Deinstallation des OfficeScan Servers auf Seite 5-2*
- *OfficeScan Server deinstallieren auf Seite 5-5*
- *Durchführen eines Rollbacks des OfficeScan Servers und der OfficeScan Agenten mit dem Serversicherungspaket auf Seite 5-10*
- *Durchführen eines manuellen Rollbacks zu früheren OfficeScan Versionen auf Seite 5-16*

Überlegungen zu Deinstallation und Rollback

Wenn bei der Verwendung von OfficeScan Probleme auftreten, gehen Sie wie folgt vor:

- Verwenden Sie das Deinstallationsprogramm, um den OfficeScan Server sicher vom Endpunkt zu entfernen. Verschieben Sie vor der Deinstallation des Servers die von ihm verwalteten agents auf einen anderen OfficeScan Server.
- Führen Sie ein Rollback der agents auf frühere OfficeScan Versionen durch, anstatt den OfficeScan Server zu deinstallieren. Weitere Informationen finden Sie unter *Durchführen eines Rollbacks des OfficeScan Servers und der OfficeScan Agenten mit dem Serverversicherungspaket auf Seite 5-10*.

Vor der Deinstallation des OfficeScan Servers

Verwenden Sie das Deinstallationsprogramm, um den OfficeScan Server sicher zu entfernen.

Verschieben Sie vor der Deinstallation des Servers die von ihm verwalteten agents auf einen anderen OfficeScan Server mit derselben Version. Ziehen Sie in Betracht, die Server-Datenbank und die Konfigurationsdateien zu sichern, falls Sie vorhaben, den Server später neu zu installieren.

Verschieben von Agents auf einen anderen OfficeScan Server

Die OfficeScan Webkonsole stellt eine Option bereit, mit der vom Server verwaltete agents auf einen anderen OfficeScan Server verschoben werden können.

Prozedur

1. Notieren Sie sich folgende Informationen für den anderen OfficeScan Server. Sie benötigen diese Informationen, wenn die agents verschoben werden.
 - Endpunktname oder IP-Adresse

- Server-Listening-Port

Um den Server-Listening-Port anzuzeigen, navigieren Sie zu **Administration > Einstellungen > Agent-Verbindung**. Die Portnummer wird auf dem Bildschirm angezeigt.

2. Navigieren Sie in der Webkonsole des zu deinstallierenden Servers zu **Agents > Agent-Verwaltung**.
3. Wählen Sie in der agent-Hierarchie die agents aus, die Sie aktualisieren möchten, und klicken Sie anschließend auf **Agent-Hierarchie verwalten > Agent verschieben**.
4. Geben Sie unterhalb von **Ausgewählte(n) Agent(s) auf einen anderen OfficeScan Server verschieben** den Computernamen oder die IP-Adresse des Servers sowie den Server-Listening-Port des anderen OfficeScan Servers an.
5. Klicken Sie auf **Verschieben**.

Wenn alle agents verschoben wurden und bereits von dem anderen OfficeScan Server verwaltet werden, kann der ursprüngliche OfficeScan Server ohne Bedenken deinstalliert werden.

OfficeScan Datenbank und Konfigurationsdateien sichern und wiederherstellen

Sichern Sie die OfficeScan Datenbank und wichtige Konfigurationsdateien, bevor Sie den OfficeScan Server deinstallieren. Sichern Sie die OfficeScan Server-Datenbank in einem Speicherort außerhalb des OfficeScan Programmverzeichnis.

Prozedur

1. Sichern Sie die Datenbank über die Webkonsole, indem Sie zu **Administration > Einstellungen > Datenbanksicherung** navigieren. Anweisungen hierzu finden Sie im *Administratorhandbuch* oder in der *OfficeScan Server-Hilfe*.



Warnung!

Verwenden Sie kein anderes Tool oder keine andere Anwendung zur Datenbanksicherung.

2. Beenden Sie den OfficeScan Master Service von der Microsoft Management-Konsole aus.
3. Führen Sie eine manuelle Datensicherung der folgenden Dateien und Ordner durch, die sich im Verzeichnis <Installationsordner des Servers> \PCCSRV befinden:
 - ofcscan.ini: Diese Datei enthält globale agent-Einstellungen.
 - ous.ini: Diese Datei enthält die Liste der Update-Adressen für die Verteilung von Antiviren-Komponenten.
 - Persönlicher Ordner: Dieser Ordner enthält die Einstellungen der Firewall und der Update-Adressen.
 - Ordner Web\tmOPP: Dieser Ordner enthält die Einstellungen der Ausbruchsprävention.
 - Pccnt\Common\OfcPfw*.dat: Diese Datei enthält die Einstellungen der Firewall.
 - Download\OfcPfw.dat: Diese Datei enthält die Einstellungen zur Verteilung der Firewall.
 - Ordner "Log": Dieser Ordner enthält Systemereignisse und das Verbindungsprotokoll.
 - Ordner "Virus": Dieser Ordner enthält die in Quarantäne verschobenen Dateien.
 - HTTPDB-Ordner: Dieser Ordner enthält die OfficeScan Datenbank.
4. Deinstallieren Sie den OfficeScan Server. Weitere Informationen finden Sie unter *OfficeScan Server deinstallieren auf Seite 5-5*.
5. Führen Sie eine Erstinstallation durch. Weitere Informationen finden Sie unter *Durchführen einer Erstinstallation des OfficeScan Servers auf Seite 2-2*.

6. Öffnen Sie nach beendetem Setup die Microsoft Management-Konsole (`services.msc`).
 7. Klicken Sie mit der rechten Maustaste auf **OfficeScan Master Service** und anschließend auf **Beenden**.
 8. Kopieren Sie die Sicherungsdateien in den Speicherort <Installationsordner des Servers>\PCCSRV auf dem Ziel-Endpunkt. Hierdurch werden die OfficeScan Server-Datenbank und die entsprechenden Dateien und Ordner überschrieben.
 9. Starten Sie den OfficeScan Master Service neu.
-

OfficeScan Server deinstallieren

Verwenden Sie das Deinstallationsprogramm, um den OfficeScan Server und den integrierten Smart Protection Server zu deinstallieren.

Sollten bei der Verwendung des Deinstallationsprogramms Probleme auftreten, führen Sie eine manuelle Deinstallation durch.



Hinweis

Anweisungen zur Deinstallation von OfficeScan Agent finden Sie im Administratorhandbuch.

Den OfficeScan Server mit Hilfe des Deinstallationsprogramms deinstallieren

Prozedur

1. Führen Sie das Deinstallationsprogramm aus. Es gibt zwei Möglichkeiten, auf das Deinstallationsprogramm zuzugreifen.
 - Methode A

- a. Klicken Sie auf dem OfficeScan Server auf **Start > Programme > Trend Micro OfficeScan Server > OfficeScan deinstallieren**. Ein Bestätigungsfenster wird angezeigt.
 - b. Klicken Sie auf **Ja**. Das Programm zum Deinstallieren der Server-Software fordert Sie zur Eingabe des Administratorkennworts auf.
 - c. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**. Die Serverdateien werden nun entfernt. Eine Bestätigungsmeldung wird angezeigt.
 - d. Klicken Sie zum Schließen des Deinstallationsprogramms auf **OK**.
 - Methode B
 - a. Doppelklicken Sie im Windows-Fenster **Software** auf das OfficeScan Server-Programm.
 - b. Klicken Sie auf **Systemsteuerung > Software**. Suchen Sie "Trend Micro OfficeScan Server", und doppelklicken Sie darauf. Befolgen Sie die Anweisungen im Fenster, bis Sie aufgefordert werden, das Administrator-Kennwort einzugeben.
 - c. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**. Die Serverdateien werden nun entfernt. Eine Bestätigungsmeldung wird angezeigt.
 - d. Klicken Sie zum Schließen des Deinstallationsprogramms auf **OK**.
-

Den OfficeScan Server manuell deinstallieren

Teil 1: Deinstallation des integrierten Smart Protection Servers

Prozedur

1. Öffnen Sie die Microsoft Management-Konsole, und beenden Sie den OfficeScan Master Service.
2. Öffnen Sie die Eingabeaufforderung, und navigieren Sie zum Ordner <Installationsordner des Servers>\PCCSRV.

3. Führen Sie den folgenden Befehl aus:

```
SVRSVCSETUP.EXE -uninstall
```

Mit diesem Befehl werden auf OfficeScan bezogene Dienste deinstalliert. Konfigurationsdateien oder die OfficeScan Datenbank werden jedoch nicht entfernt.

4. Navigieren Sie zum <Installationsordner des Servers>\PCCSRV\private, und öffnen Sie die Datei ofcserver.ini.
5. Ändern Sie die folgenden Einstellungen:

TABELLE 5-1. ofcserver.ini-Einstellungen

EINSTELLUNG	ANWEISUNG
WSS_INSTALL	Ändern Sie 1 in 0
WSS_ENABLE=1	Löschen Sie diese Zeile
WSS_URL=https://<computer_name>:4345/tmcss/	Löschen Sie diese Zeile

6. Navigieren Sie zum Ordner <Installationsordner des Servers>\PCCSRV, und öffnen Sie die Datei OfUninst.ini. Löschen Sie die folgenden Zeilen:

```
[WSS_WEB_SERVER]

ServerPort=8082

IIS_VhostName=Smart Protection Server (integriert)

IIS_VHostIdx=5
```



Hinweis

Der Wert für IIS_VHostidx sollte derselbe sein, wie der in der folgenden Zeile angegebene "isapi"-Wert:

```
ROOT=/tmcss,C:\Programme\Trend Micro\OfficeScan\PCCSRV\WSS
\isapi,,<Wert>
```

[WSS_SSL]

SSLPort=<SSL-Port>

7. Öffnen Sie die Eingabeaufforderung, und navigieren Sie zum Ordner <Installationsordner des Servers>\PCCSRV.

8. Führen Sie die folgenden Befehle aus:

```
Svrsvcsetup -install
```

```
Svrsvcsetup -enablessl
```

```
Svrsvcsetup -setprivilege
```

9. Vergewissern Sie sich, dass die folgenden Elemente entfernt wurden:
 - Trend Micro Smart Protection Server-Dienst von der Microsoft Management-Konsole
 - Leistungszähler des Smart Protection Servers
 - Smart Protection Server (integriert) Website

Teil 2: Deinstallation des OfficeScan Servers

Prozedur

1. Öffnen Sie den Registrierungseditor, und führen Sie folgende Schritte aus:



Warnung!

Die nächsten Schritte erfordern das Löschen von Registrierungsschlüsseln. 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.

- a. Navigieren Sie zu HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.

- b. Vergewissern Sie sich, dass der Registrierungsschlüssel ofcservice gelöscht wurde.
 - c. Navigieren Sie zu HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\OfficeScan\, und löschen Sie den Registrierungsschlüssel OfficeScan.

Für 64-Bit-Endpunkte lautet der Pfad HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfficeScan\.
 - d. Navigieren Sie zu HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\. Löschen Sie den Ordner OfficeScan Management Console-<Servername>.
 2. Navigieren Sie zum <Installationsordner des Servers>\PCCSRV und heben Sie die Freigabe des Ordners PCCSRV auf.
 3. Starten Sie den Server-Computer neu.
 4. Navigieren Sie zum <Installationsordner des Servers>\PCCSRV und löschen Sie den Ordner PCCSRV.
 5. Löschen Sie die OfficeScan Website über die IIS-Konsole (Internet Information Services, Internetinformationsdienste).
 - a. Öffnen Sie die IIS Konsole.
 - b. Erweitern Sie Servername.
 - c. Falls Sie OfficeScan auf einer separaten Website installiert haben, navigieren Sie zum Ordner websites und löschen Sie OfficeScan.
 - d. Falls Sie unter der Standard-Website virtuelle OfficeScan Verzeichnisse installiert haben, navigieren Sie zur Standard-Website und löschen Sie anschließend das virtuelle OfficeScan Verzeichnis.
-

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

Der Vorgang des OfficeScan Rollbacks umfasst das Rollback von OfficeScan Agents und anschließend das Rollback des OfficeScan Servers.



Wichtig

- Administratoren können das Rollback des OfficeScan Servers und der Agents nur durchführen, indem sie folgendermaßen vorgehen, wenn der Administrator den Server während des Installationsvorgangs sichern möchte. Wenn die Server-Sicherungsdateien nicht verfügbar sind, finden Sie im *Installations- und Upgrade-Handbuch* der zuvor installierten OfficeScan-Version weitere Informationen zum manuellen Rollback.
 - Diese Version von OfficeScan unterstützt Rollbacks nur für die folgenden OfficeScan Versionen:
 - OfficeScan 11.0 Service Pack 1 mit kritischem Patch
 - OfficeScan 11.0 Service Pack 1
 - OfficeScan 11.0
 - OfficeScan 10.6 Service Pack 3
-

Durchführen eines Rollbacks des OfficeScan Agentens

OfficeScan kann für OfficeScan Agents nur ein Rollback auf die Version des wiederherzustellenden Servers durchführen. Ein Rollback von OfficeScan Agents auf eine ältere Version als die des Servers ist nicht möglich.



Wichtig

Stellen Sie sicher, dass Sie das Rollback zuerst für die OfficeScan Agents und erst dann für den OfficeScan Server durchführen.

Prozedur

1. Stellen Sie sicher, dass OfficeScan Agents das Agent-Programm nicht aktualisieren können.
 - a. Navigieren Sie in der OfficeScan XG 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 **OfficeScan Agents können Komponenten aktualisieren, aber kein Upgrade des Agents durchführen oder Hotfixes verteilen**.

2. Navigieren Sie in der OfficeScan XG 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.

9. Fordern Sie den Benutzer nach der Installation der vorherigen Version des OfficeScan Agents auf, den Endpunkt neu zu starten.

Nachdem der Rollback-Vorgang beendet wurde, berichtet der OfficeScan Agent weiterhin an denselben OfficeScan Server.



Hinweis

Nach dem Rollback des OfficeScan Agent wird ein Rollback aller Komponenten, einschließlich des Viren-Patterns, auf die Vorgängerversion durchgeführt. Wenn Administratoren das Rollback des OfficeScan Servers nicht durchführen, kann der OfficeScan Agent, für den ein Rollback durchgeführt wurde, keine Komponenten aktualisieren. Administratoren müssen die Update-Adresse des OfficeScan Agents, für den ein Rollback durchgeführt wurde, in die Standard-Update-Adresse ändern, um weitere Komponenten-Updates zu erhalten.

Wiederherstellen der Vorgängerversion des OfficeScan Servers

Für den Vorgang zur Wiederherstellung des OfficeScan Servers müssen die Administratoren den OfficeScan XG Server deinstallieren, die ältere Serverversion erneut installieren, die Windows-Dienste manuell beenden, die Systemregistrierung aktualisieren und die OfficeScan Server-Dateien im OfficeScan Installationsverzeichnis ersetzen.



Wichtig

Stellen Sie sicher, dass Sie zuerst das Rollback für die OfficeScan Agents durchführen, bevor Sie den OfficeScan Server wiederherstellen.

Prozedur

1. Deinstallieren Sie den OfficeScan XG Server.
2. Installieren Sie die Vorgängerversion des OfficeScan Servers.



Tipp

Trend Micro empfiehlt, den Host-Namen bzw. die IP-Adresse beim Wiederherstellen des Servers nicht zu ändern.

Sie können die Vorgängerversion des Servers wie folgt überprüfen: Öffnen Sie den *<Installationsordner des Servers>* und überprüfen Sie den Wiederherstellungsordner, der bei der Installation des OfficeScan XG Servers erstellt wurde. Der Ordner hat einen der folgenden Namen (als *<Restore_folder_version>* bezeichnet):

- OSCE11_SP1: OfficeScan 11.0 Service Pack 1
- OSCE11: OfficeScan 11.0
- OSCE106_SP3: OfficeScan 10.6 Service Pack 3

3. Beenden Sie die folgenden Dienste auf dem OfficeScan Server-Computer.

- Intrusion Defense Firewall (wenn installiert)
- Trend Micro Local Web Classification Server
- Trend Micro Smart Scan Server
- OfficeScan Active Directory Integration Service
- OfficeScan Control Manager Agent
- OfficeScan Plug-in Manager
- OfficeScan Master Service
- World Wide Web Publishing Dienst

4. Kopieren Sie alle Dateien und Verzeichnisse aus dem Verzeichnis *<Server_installation_folder>\<Restore_folder_version>* in das Verzeichnis *<Server_installation_folder>\PCCSRV* und ersetzen Sie sie dort.

5. Stellen Sie die OfficeScan Registrierung wieder her.

- a. Öffnen Sie den **Registrierungseditor** (*regedit.exe*).
- b. Wählen Sie im linken Navigationsbereich einen der folgenden Registrierungsschlüssel aus:

- Für 32-Bit-Systeme: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service
 - Für 64-Bit-Systeme: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Officescan\service
- c. Wechseln Sie zu **Datei > Importieren...**
- d. Wählen Sie die allgemeine .reg-Datei für den OfficeScan Server aus, die sich im Verzeichnis <Server_installation_folder>\<Restore_folder_version>\ befindet.
- Der Name der Registrierungsdatei hat das folgende Format:
- RegBak_<Restore_folder_version>.reg
- e. Klicken Sie auf **Ja**, um alle vorherigen Versionsschlüssel von OfficeScan wiederherzustellen.
6. Sie können optional den Zeitplan für die Datenbanksicherung wiederherstellen.
- a. Öffnen Sie den **Registrierungseditor** (`regedit.exe`).
- b. Wählen Sie im linken Navigationsbereich einen der folgenden Registrierungsschlüssel aus:
- Für 32-Bit-Systeme: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Database Backup
 - Für 64-Bit-Systeme: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Database Backup
- c. Wechseln Sie zu **Datei > Importieren...**
- d. Wählen Sie die .reg-Datei der Datenbank aus, die sich im Verzeichnis <Server_installation_folder>\<Restore_folder_version>\ befindet.
- Der Name der Registrierungsdatei hat das folgende Format:
- RegBak_DBBak_<Restore_folder_version>.reg
- e. Klicken Sie auf **Ja**, um alle vorherigen Versionsschlüssel von OfficeScan wiederherzustellen.

7. Öffnen Sie einen Befehlszeilen-Editor (**cmd.exe**) und geben Sie die folgenden Befehle ein, um den Leistungszähler des Local Web Classification Servers zurückzusetzen:

```
cd <Installationsordner des Servers>\PCCSRV\LWCS  
regsvr32.exe /u /s perflWCSPerfMonMgr.dll  
regsvr32.exe /s perflWCSPerfMonMgr.dll
```

8. Starten Sie die folgenden Dienste neu:

- Intrusion Defense Firewall (wenn installiert)
- Trend Micro Local Web Classification Server
- Trend Micro Smart Scan Server
- OfficeScan Active Directory Integration Service
- OfficeScan Control Manager Agent
- OfficeScan Plug-in Manager
- OfficeScan Master Service
- Apache 2 (bei Verwendung des Apache Webservers)
- World Wide Web Publishing Dienst (bei Verwendung des IIS-Webservers)

9. Säubern Sie den Zwischenspeicher des Internet Explorers und entfernen Sie manuell die ActiveX-Steuerelemente. Weitere Informationen zum Entfernen von ActiveX-Steuerelementen im Internet Explorer 9 finden Sie unter <http://windows.microsoft.com/en-us/internet-explorer/manage-add-ons#ie=ie-9>.

Die Einstellungen der Vorgängerversion des OfficeScan Servers wurden wiederhergestellt.

**Tipp**

Administratoren können einen erfolgreichen Rollback bestätigen, indem sie die OfficeScan Versionsnummer im **Info**-Fenster (**Hilfe > Info**) überprüfen.

10. Optional können Sie den OfficeScan Server mithilfe der Webkonsole beim Control Manager Server registrieren.
11. Optional können Sie den OfficeScan Server mithilfe der Webkonsole beim Deep Discovery Server registrieren.



Hinweis

Die Integration von Deep Discovery mit dem OfficeScan Server ist seit OfficeScan 10.6 Service Pack 2 möglich.

12. Nachdem Sie das erfolgreiche Rollback von OfficeScan bestätigt haben, löschen Sie alle Dateien im Verzeichnis `<Server_installation_folder>\<Restore_folder_version>\`.
-

Durchführen eines manuellen Rollbacks zu früheren OfficeScan Versionen

Wenn Probleme beim Upgrade von OfficeScan Agents auftreten, können Sie ein Rollback der Agents auf ihre frühere Version durchführen.



Hinweis

Führen Sie ein manuelles Rollback aus, wenn Sie die Serverinformationen während der Installation nicht gesichert haben. Wenn Sie die Serverinformationen während der Serverinstallation gesichert haben, führen Sie das in [Durchführen eines Rollbacks des OfficeScan Servers und der OfficeScan Agenten mit dem Serversicherungspaket auf Seite 5-10](#) beschriebene Rollback-Verfahren aus.

Um ein erfolgreiches Rollback durchzuführen, bereiten Sie Folgendes vor:

- Den OfficeScan Server zur Verwaltung der Agents, für die ein Rollback durchgeführt wird. Die Serverversion sollte eine der folgenden sein:
 - 11.0 (einschließlich aller Service Pack-Versionen)
 - 10.6 (einschließlich aller Service Pack-Versionen)

- Den Endpunkt, der als Update-Quelle verwendet werden soll. Diese Update-Quelle enthält die Dateien und Komponenten des Rollbacks. Wird ein Agent, für den ein Rollback ausgeführt werden soll, von dieser Quelle aus aktualisiert, wird der OfficeScan Agent deinstalliert. Anschließend wird die vorherige Version des Agents installiert.
- Den OfficeScan XG Server zur Verwaltung der Agents, für die ein Rollback ausgeführt werden soll
- Die OfficeScan XG Agents, für die ein Rollback ausgeführt werden soll

Teil 1: Vorgängerversion des OfficeScan Servers vorbereiten

Prozedur

1. Bereiten Sie einen Server mit einer installierten Vorgängerversion von OfficeScan Server vor.
2. Wenden Sie die letzten Hotfixes, Patches oder Service Packs für die frühere Version von OfficeScan Server an.
3. Replizieren Sie die folgenden Einstellungen des OfficeScan XG Servers auf die Vorgängerversion von OfficeScan Server.
 - a. Agent-Einstellungen
 - Durchsuchen
 - Update-Agents
 - Berechtigungen
 - Liste der zugelassenen Spyware/Grayware (für OfficeScan 8.0 SP1 oder höher)
 - Ausnahmeliste der Verhaltensüberwachung (für OfficeScan 10.0 SP1 oder höher)
 - b. Allgemeine OfficeScan Agent-Einstellungen

- c. Web-Reputation-Einstellungen (für OfficeScan 8.0 SP1 oder höher)
 - Endpunktstandort
 - Richtlinien
 - Proxy
 - d. OfficeScan Firewall-Einstellungen
 - Richtlinie
 - Profile
 - e. Zeitplan der Verbindungsüberprüfung
 - f. Web-Reputation-Einstellungen (für OfficeScan 8.0 SP1 oder höher)
 - Zeitgesteuertes Serverupdate
 - Server-Update-Adresse
 - Zeitgesteuertes Agent-Update
 - Update-Adresse des Agents
 - g. Einstellungen der Protokollwartung
 - h. Benachrichtigungen - alle Benachrichtigungseinstellungen
 - i. Administrationseinstellungen
 - Quarantäne-Manager
 - Control Manager
 - Datenbanksicherung
4. Führen Sie Client Packager auf der Vorgängerversion von OfficeScan Server zweimal aus, um zwei OfficeScan Agent-Installationspakete zu erstellen: ein Paket für x86-Endpunkte und ein weiteres für x64-Endpunkte.
- Einstellungen im OfficeScan Agent-Installationspaket für x86-Endpunkte:
- Packettyp: Setup

- Windows Betriebssystem: 32 Bit
- Ausgabedatei: `InstNTPkg.exe`

Einstellungen im OfficeScan Agent-Installationspaket für x64-Endpunkte:

- Packettyp: Setup
- Windows Betriebssystem: 64 Bit
- Ausgabedatei: `InstNTPkg.exe`

Da die beiden Ausgabedateien denselben Dateinamen aufweisen, speichern Sie sie in verschiedenen Verzeichnissen, damit die Dateien sich nicht gegenseitig überschreiben.

Teil 2: Vorbereiten einer Update-Adresse für Agents, für die ein Rollback durchgeführt werden soll

Prozedur

1. Bereiten Sie den Endpunkt vor, der als Update-Adresse verwendet werden soll.
2. Navigieren Sie auf dem OfficeScan XG Server zu <Installationsordner des Servers>\PCCSRV und kopieren Sie den Ordner Download (einschließlich seiner Unterordner) auf den Endpunkt der Update-Adresse (der im vorherigen Schritt vorbereitete Endpunkt).

Kopieren Sie den Ordner Download beispielsweise in das folgende Verzeichnis auf dem Endpunkt der Update-Adresse:

`C:\OfficeScanUpdateSource`

3. Auf dem OfficeScan XG Server:
 - a. Erstellen Sie einen temporären Ordner.
 - b. Navigieren Sie zu <Installationsordner des Servers>\PCCSRV\Admin, und kopieren Sie die folgenden Dateien in den temporären Ordner:

`RollbackAgent.dll`

RollbackAgent_64x.dll

ClientRollback.exe

- c. Komprimieren Sie im temporären Ordner die Datei RollbackAgent.dll zu RollbackAgent.zip.
- d. Komprimieren Sie im temporären Ordner die Datei RollbackAgent_64x.dll zu RollbackAgent_64x.zip.
- e. Erstellen Sie einen Unterordner im temporären Ordner, und benennen Sie diesen RollBackNTPkg.
- f. Kopieren Sie folgende Dateien in den Unterordner RollBackNTPkg:

ClientRollback.exe

Das in Teil 1, Schritt 4 erstellte OfficeScan Agent-Installationspaket für x86-Endpunkte (InstPkg.exe)

- g. Komprimieren Sie den Unterordner RollbackNTPkg zu RollbackNTPkg.zip.
- h. Erstellen Sie einen Unterordner im temporären Ordner, und benennen Sie diesen RollBackNTPkgx64.
- i. Kopieren Sie folgende Dateien in den Unterordner RollBackNTPkgx64:

ClientRollback.exe

Das in Teil 1, Schritt 4 erstellte agent-Installationspaket für x64-Endpunkte (InstPkg.exe)

- j. Komprimieren Sie den Unterordner RollbackNTPkgx64 zu RollbackNTPkgx64.zip.
- k. Kopieren Sie die folgenden komprimierten Dateien aus dem temporären Ordner auf den Endpunkt der Update-Adresse:

RollbackAgent.zip

RollbackAgent_64x.zip

RollbackNTPkg.zip

RollbackNTPkgx64.zip



Hinweis

Kopieren Sie die Dateien in den Ordner \Download\Product auf dem Endpunkt der Update-Adresse. Kopieren Sie die Dateien z. B. nach C:\OfficeScanUpdateSource\Download\Product.

4. Auf dem Endpunkt der Update-Adresse:
 - a. Stellen Sie sicher, dass das "Internet-Gastkonto" über Lesezugriff auf die folgenden komprimierten Dateien unter \Download\Product verfügt (z. B. C:\OfficeScanUpdateSource\Download\Product):

RollbackAgent.zip

RollbackAgent_64x.zip

RollbackNTPkg.zip

RollbackNTPkgx64.zip



Tipp

Klicken Sie mit der rechten Maustaste auf jede Datei, und klicken Sie dann auf "Eigenschaften", um die Zugriffsberechtigung zu prüfen. Auf der Registerkarte "Sicherheit" sollte als Berechtigung für das Internet-Gastkonto "Lesen" angegeben sein.

5. Öffnen Sie im Ordner \Download\Product die Datei server.ini mit einem Texteditor, z. B. Notepad.
6. Ändern Sie die folgenden Zeilen in der Datei server.ini, und speichern Sie die Datei:



Warnung!

Ändern Sie keine anderen Einstellungen in der Datei server.ini.

```
[All_Product]
```

```
MaxProductID=109
```

Product.109=OfficeScan Rollback, 3.5, <Aktuelle OfficeScan Version>

[Info_109_35000_1_5633]

Version=<Vorherige OfficeScan Version>

Update_Path=product/RollbackAgent_64x.zip,
<RollbackAgent64-Dateigröße>

Path=product/RollBackNTPkgx64.zip, <RollBackNTPkg64-
Dateigröße>

Wobei gilt:

<RollbackAgent-Dateigröße>: Dateigröße von
"RollbackAgent.zip" in Byte. Beispiel: 90517.

<RollBackNTPkg-Dateigröße>: Dateigröße von
"RollbackNTPkg.zip" in Byte. Beispiel: 32058256.

<RollbackAgent64-Dateigröße>: Dateigröße von
"RollbackAgent_64x.zip" in Byte. Beispiel: 90517.

<RollBackNTPkg64-Dateigröße>: Dateigröße von
"RollbackNTPkgx64.zip" in Byte. Beispiel: 36930773.



Tipp

Um die Dateigröße zu ermitteln, klicken Sie mit der rechten Maustaste auf die ZIP-Datei, und klicken Sie dann auf **Eigenschaften**. Notieren Sie die Größe der Datei, nicht die Größe auf der Festplatte.

<Aktuelle OfficeScan Version>: Aktuelle OfficeScan Version
(XG)

<Vorherige OfficeScan Version>: Vorherige OfficeScan
Version. Beispiel: 10.0.

Teil 3: Durchführen eines Rollbacks des OfficeScan Agents

Prozedur

1. Navigieren Sie auf der OfficeScan XG Webkonsole zu **Updates > Agents > Update-Adresse**:
 - a. Wählen Sie **Benutzerdefinierte Update-Adresse** aus.
 - b. Klicken Sie in der **Liste der benutzerdefinierten Update-Quelle** auf **Hinzufügen**. Es öffnet sich ein neues Fenster.
 - c. Geben Sie die IP-Adressen der agents ein, für die das Rollback ausgeführt werden soll.
 - d. Geben Sie die URL der Update-Quelle an. Geben Sie z. B. Folgendes ein:
`http://<IP-Adresse der Update-Quelle>/OfficeScanUpdateSource/`
 - e. Klicken Sie auf **Speichern**.
Das Fenster wird geschlossen.
 - f. Klicken Sie auf **Alle Agents benachrichtigen**.
Wenn agents, für die ein Rollback ausgeführt werden soll, von der Update-Adresse aus aktualisiert werden, wird der OfficeScan Agent deinstalliert und die vorherige Client-Version wird installiert.
 2. Fordern Sie den Benutzer nach der Installation der vorherigen Client-Version auf, den Endpunkt neu zu starten. Nach dem Neustart sendet der OfficeScan Agent einen Bericht an den in Teil 1 vorbereiteten OfficeScan Server.
-

Kapitel 6

OfficeScan Ressourcen zur Fehlerbehebung

In diesem Kapitel werden Ressourcen beschrieben, die zum Beheben möglicher Probleme mit dieser Version von OfficeScan verwendet werden können.

Themen in diesem Kapitel:

- *Support-Informationssystem auf Seite 6-2*
- *Case Diagnostic Tool auf Seite 6-2*
- *Trend Micro Performance Tuning Tool auf Seite 6-2*
- *Installationsprotokolle auf Seite 6-5*
- *Debug-Protokolle für den Server auf Seite 6-5*
- *Agent-Debug-Protokolle auf Seite 6-7*

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 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.

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 sollte während der Pilotphase auf einem herkömmlichen Workstation-Image und/oder einiger weniger Ziel-Workstations ausgeführt werden, um Leistungsprobleme in der tatsächlichen Bereitstellung der Verhaltensüberwachung und Gerätesteuerung vorwegzunehmen.



Hinweis

Das Trend Micro Performance Tuning Tool unterstützt nur 32-Bit-Plattformen.

Systemintensive Anwendungen identifizieren

Prozedur

1. Trend Micro Performance Tuning Tool herunterladen:
http://solutionfile.trendmicro.com/solutionfile/1054312/EN/TMPerfTool_2_90_1131.zip
2. Entpacken Sie die Datei TMPerfTool.zip, um TMPerfTool.exe zu extrahieren.
3. Platzieren Sie die Datei TMPerfTool.exe in den <Installationsordner des Clients> oder in denselben Ordner wie die Datei TMBMCLI.dll.
4. Klicken Sie mit der rechten Maustaste auf TMPerfTool.exe, und wählen Sie **Als Administrator ausführen**.
5. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung, und klicken Sie dann auf **OK**.
6. Klicken Sie auf **Analysieren**. Das Tool startet die Überwachung der CPU-Nutzung und das Laden der Ereignisse.

Ein systemintensiver Prozess erscheint rot markiert.

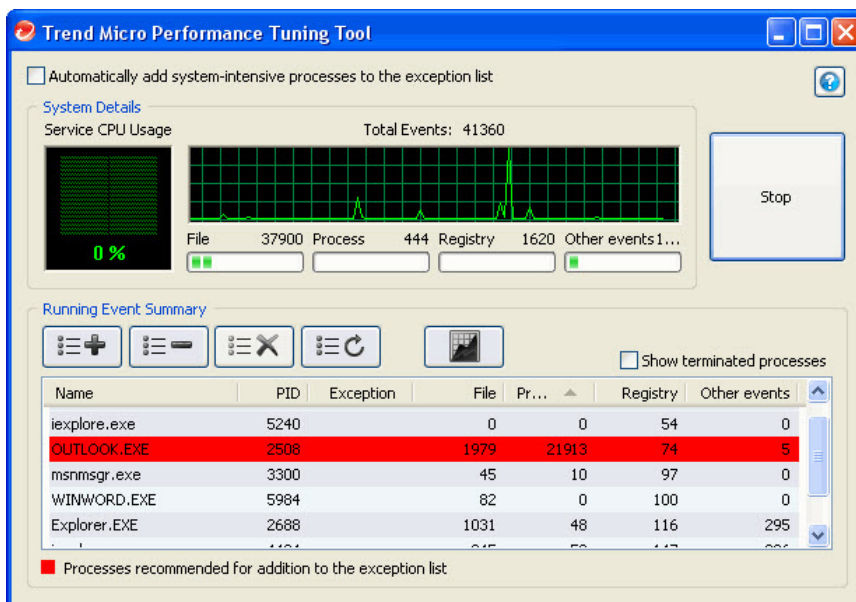


ABBILDUNG 6-1. Markierter systemintensiver Prozess

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 dann 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 im *Administratorhandbuch*.

Installationsprotokolle

Verwenden Sie zur Behebung von Problemen bei der Installation die von OfficeScan automatisch erstellten Installationsprotokolldateien.

TABELLE 6-1. Installationsprotokolldateien

PROTOKOLLDATTEI	DATEINAME	SPEICHERORT
Installations-/Upgrade-Protokoll des Servers	OFCMAS.LOG	%windir%
Remote-Installations-/Upgrade-Protokoll des Servers	OFCMAS.LOG (auf dem Endpunkt, auf dem das Setup-Programm gestartet wurde) OFCMAS.LOG (auf dem Ziel-Endpunkt)	%windir%
Installationsprotokoll von OfficeScan Agent	OFCNT.LOG	%windir% (für alle Installationsmethoden außer mit MSI Paket) %temp% (für die Installation mit MSI Paket)

Debug-Protokolle für den Server

Sie können die Debug-Protokollierung aktivieren, bevor Sie folgende Aufgaben im Hinblick auf den Server 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-Programm ausgeführt wird, und nicht auf dem Remote-Endpunkt).



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. Löschen Sie die Protokolldatei, wenn sie zu groß wird.

Aktivieren der Debug-Protokollierung auf dem OfficeScan Server-Computer

Möglichkeit 1:

Prozedur

1. Melden Sie sich an der Webkonsole an.
 2. Klicken Sie auf dem Banner der Webkonsole auf das erste "O" in "OfficeScan". Dadurch wird das Fenster **Einstellungen des Fehlersuchprotokolls** geöffnet.
 3. Geben Sie die Debug-Protokolleinstellungen an.
 4. Klicken Sie auf **Speichern**.
 5. Überprüfen Sie die Protokolldatei (`ofcdebug.log`) am Standardspeicherort:
<Installationsordner des Servers>\PCCSRV\Log.
-

Möglichkeit 2:

Prozedur

1. Kopieren Sie den Ordner "LogServer" im Ordner <Installationsordner des Servers>\PCCSRV\Private nach C:\.

2. Erstellen Sie eine Datei mit dem Namen `ofcdebug.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 erneut installieren, auf eine neue Version upgraden oder eine Remote-Installation/ein Remote-Upgrade durchführen).
5. Überprüfen Sie `ofcdebug.log` unter `C:\LogServer`.

**Hinweis**

Wenn der OfficeScan Agent auf dem OfficeScan Server vorhanden ist, gibt der Agent seine Debug-Protokolle auch in den Debug-Protokollen des Servers aus.

Agent-Debug-Protokolle

Aktivieren Sie die Debug-Protokollierung vor der Installation des OfficeScan Agents.

**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.

Aktivieren der Debug-Protokollierung auf dem OfficeScan Agent

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 agent-Benutzer und weisen Sie sie an, die Datei auf Laufwerk `C:\` zu speichern.

`LogServer.exe` wird automatisch bei jedem Start des agent-Endpunkts ausgeführt.

3. Laden Sie zum Starten der Debug-Protokollierung den OfficeScan Agent erneut oder starten Sie den Endpunkt erneut.

Weisen Sie die Benutzer an, das Befehlsfenster von `LogServer.exe`, das beim Start des Endpunkts geöffnet wird, NICHT zu schließen, da OfficeScan in diesem Fall die Debug-Protokollierung beendet. Schließt der Benutzer das Befehlsfenster, kann die Debug-Protokollierung erneut gestartet werden, indem der Prozess `LogServer.exe` im Ordner `\OfficeScan Client` ausgeführt wird.

4. Überprüfen Sie für jeden agent-Endpunkt die Datei `ofcdebug.log` auf Laufwerk `C:\`.

5. Löschen Sie zum Deaktivieren der Debug-Protokollierung für den OfficeScan Agent die Datei `ofcdebug.ini`.
-

Kapitel 7

Technischer Support

Erfahren Sie mehr über die folgenden Themen:

- *Ressourcen zur Fehlerbehebung auf Seite 7-2*
- *Kontaktaufnahme mit Trend Micro auf Seite 7-3*
- *Verdächtige Inhalte an Trend Micro senden auf Seite 7-4*
- *Sonstige Ressourcen auf Seite 7-6*

Ressourcen zur Fehlerbehebung

Vor der Kontaktaufnahme mit dem technischen Support sollten Sie die folgenden Online-Ressourcen zu Trend Micro heranziehen.

Support-Portal verwenden

Über das Trend Micro Support-Portal können Sie rund um die Uhr online auf die aktuellsten Informationen über allgemeine und ungewöhnliche Probleme zugreifen.

Prozedur

1. Gehen Sie zu [http://docs.trendmicro.com/de-de/enterprise/trend-micro-security-\(for-mac\).aspx](http://docs.trendmicro.com/de-de/enterprise/trend-micro-security-(for-mac).aspx).
2. Wählen Sie unter den verfügbaren Produkten aus oder klicken Sie auf die entsprechende Schaltfläche, um nach Lösungen zu suchen.
3. Mit dem Feld **Support durchsuchen** können Sie nach verfügbaren Lösungen suchen.
4. Falls Sie keine Lösung finden, klicken Sie auf **Contact Support** und wählen Sie den gewünschten Support aus.



Tipp

Um online eine Supportanfrage zu senden, besuchen Sie die folgende URL:

<http://esupport.trendmicro.com/srf/srfmain.aspx>

Das Problem wird von einem Support-Mitarbeiter von Trend Micro untersucht, der innerhalb von 24 Stunden oder weniger auf Ihre Anfrage reagiert.

Bedrohungszyklopädie

Die meiste Malware besteht heutzutage aus komplexen Bedrohungen, bei denen zwei oder mehr Technologien miteinander kombiniert werden, um Computer-

Sicherheitsprotokolle zu umgehen. Trend Micro bekämpft diese komplexe Malware mit Produkten, die eine benutzerdefinierte Verteidigungsstrategie verfolgen. Die 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 Irving, Texas 75062 U.S.A.
Telefon	Telefon: +1 (817) 569-8900 Gebührenfrei in den USA: (888) 762-8736
Website	http://www.trendmicro.de/ueber-uns/kontakt/index.html
E-Mail-Adresse	sales@trendmicro.de

- Weltweite Support-Büros:
<http://www.trendmicro.de/ueber-uns/kontakt/index.html>
- Trend Micro Produktdokumentation:
<http://www.trendmicro.de/ueber-uns/kontakt/index.html>

Problemlösung beschleunigen

Sie sollten die folgenden Informationen zur Hand haben, um die Problemlösung zu beschleunigen:

- Schritte, um das Problem nachvollziehen zu können
- Informationen zur Appliance und zum Netzwerk
- Marke und Modell des Computers sowie zusätzlich angeschlossene Hardware oder Geräte
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Betriebssystem- und Service Pack-Version
- Version des installierten Agents
- Seriennummer oder Aktivierungscode
- Ausführliche Beschreibung der Installationsumgebung
- Genauer Wortlaut eventueller Fehlermeldungen

Verdächtige Inhalte an Trend Micro senden

Es gibt mehrere Optionen, um verdächtige Inhalte an Trend Micro zur weiteren Analyse zu senden.

E-Mail-Reputation-Dienste

Fragen Sie die Reputation einer bestimmten IP-Adresse ab, und geben Sie einen Message Transfer Agent zum Hinzufügen zur Liste der allgemein zulässigen Adressen an:

<https://ers.trendmicro.com/>

Informationen zum Senden von Nachrichten an Trend Micro finden Sie im folgenden Knowledge Base-Artikel:

<http://esupport.trendmicro.com/solution/en-US/1112106.aspx>

File-Reputation-Dienste

Sammeln Sie Systeminformationen, und senden Sie verdächtige Dateiinhalte an Trend Micro:

<http://esupport.trendmicro.com/solution/en-us/1059565.aspx>

Notieren Sie sich die Anfragenummer für die weitere Bearbeitung Ihrer Anfrage.

Web-Reputation-Dienste

Sie können die Sicherheitsbewertung und den Inhaltstyp einer URL abfragen, hinter der Sie eine Phishing-Website oder einen Infektionsüberträger vermuten, d. h. eine Quelle von Internet-Bedrohungen, wie z. B. Spyware und Viren:

<http://global.sitesafety.trendmicro.com/>

Falls die zugewiesene Bewertung nicht zutrifft, senden Sie eine Neuklassifizierungsanforderung an Trend Micro.

Sonstige Ressourcen

Neben Lösungen und Support sind online viele zusätzliche hilfreiche Ressourcen verfügbar, damit Sie immer auf dem neuesten Stand sind, Innovationen kennenlernen und mit den neuesten Sicherheitstrends vertraut sind.

Download Center

Trend Micro veröffentlicht in bestimmten Abständen Patches für gemeldete bekannte Probleme oder Upgrades zu bestimmten Produkten oder Diensten. Auf folgender Seite können Sie feststellen, ob Patches verfügbar sind:

<http://www.trendmicro.com/download/emea/?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.

Anregungen und Kritik

Das Trend Micro Team ist stets bemüht, die Dokumentationen zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder einem anderen Dokument von Trend Micro besuchen Sie diese Website:

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

Anhang A

Verteilungsbeispiel

In diesem Abschnitt wird erläutert, wie OfficeScan ausgehend von der Netzwerktopologie und den verfügbaren Netzwerkressourcen verteilt wird. Verweisen Sie auf diesen Abschnitt, wenn Sie die Bereitstellung von OfficeScan in Ihrem Unternehmen planen.

Basisnetzwerk

In Abbildung 1 wird ein Basisnetzwerk dargestellt, in dem der OfficeScan Server und die agents direkt miteinander verbunden sind. In den meisten Unternehmensnetzwerken wird diese Konfiguration bei einer LAN- (und/oder WAN-) Zugriffsgeschwindigkeit von 10 Mb/s, 100 Mb/s oder 1 Gb/s eingesetzt. In diesem Szenario eignet sich der

Endpunkt, der die OfficeScan Systemvoraussetzungen erfüllt und über die entsprechenden Ressourcen verfügt, optimal für die Installation des OfficeScan Servers.

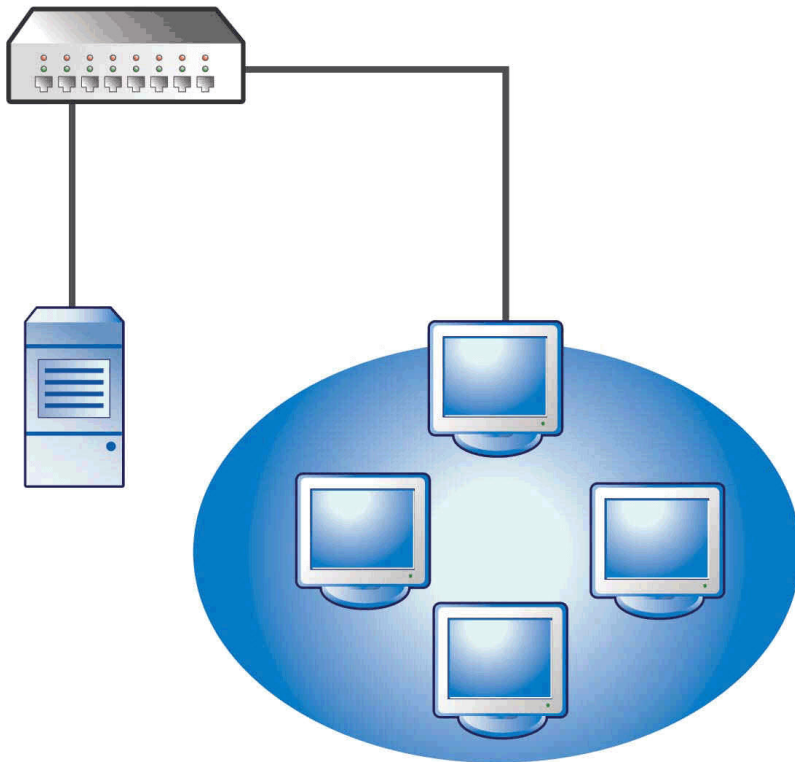


ABBILDUNG A-1. Topologie eines Basisnetzwerks

Netzwerk mit mehreren Standorten

Bei einem Netzwerk mit mehreren Zugriffspunkten und Remote-Standorten mit unterschiedlichen Bandbreiten:

- Analysieren Sie die Konsolidierungspunkte bezüglich der Büros und der Netzwerkbandbreite.
- Ermitteln Sie die aktuelle Bandbreitenauslastung für jedes Büro.

Dadurch erhalten Sie mehr Aufschluss über die ideale Verteilung von OfficeScan. Abbildung 1 stellt eine Netzwerktopologie mit mehreren Standorten dar.

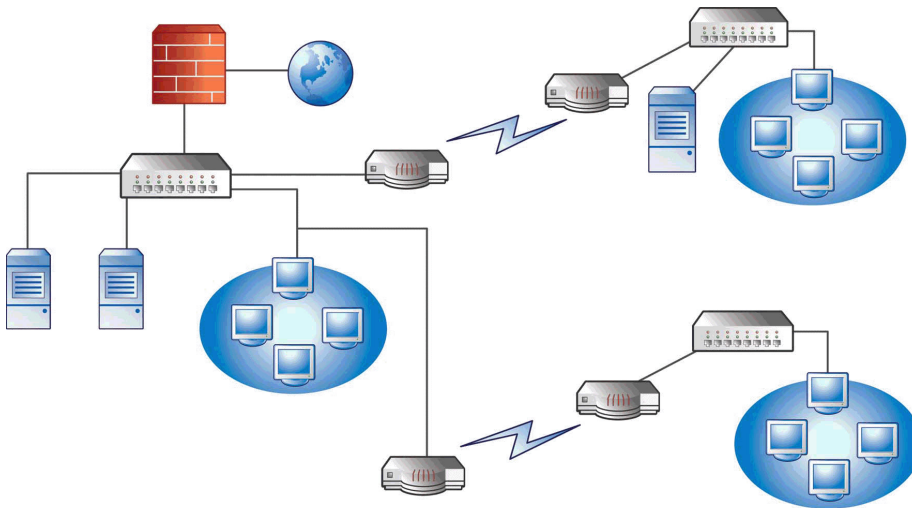


ABBILDUNG A-2. Netzwerktopologie mit mehreren Standorten

Angaben zum Netzwerk:

- Die durchschnittliche Auslastung der WAN-Verbindung von Remote-Standort 1 beträgt während der Geschäftszeiten 70 Prozent. An diesem Standort befinden sich 35 Agent-Endpunkte.
- Die durchschnittliche Auslastung der WAN-Verbindung von Remote-Standort 2 beträgt während der Geschäftszeiten 40 Prozent. An diesem Standort befinden sich 9 Agent-Endpunkte.
- Server 3 fungiert lediglich als Datei- oder Druckserver für die Gruppe an Remote-Standort 1. Dieser Endpunkt eignet sich für die Installation des OfficeScan Servers,

ist aber den zusätzlichen Verwaltungsaufwand nicht wert. Auf allen Servern wird Windows Server 2012 ausgeführt. Im Netzwerk wird Active Directory eingesetzt, dient jedoch hauptsächlich zur Authentifizierung im Netzwerk.

- Auf allen Agent-Endpunkten in der Zentrale sowie an Remote-Standort 1 und 2 wird Windows Server 2012 oder Windows 7 ausgeführt.

Netzwerk mit mehreren Standorten vorbereiten

Prozedur

1. Geben Sie den Endpunkt an, auf dem der OfficeScan Server installiert werden soll. Informationen über das Installationsverfahren finden Sie unter *Durchführen einer Erstinstallation des OfficeScan Servers auf Seite 2-2*.
2. Ermitteln Sie die verfügbaren Installationsmethoden für den agent und schließen Sie Methoden aus, die die Voraussetzungen nicht erfüllen. Weitere Informationen zu den agent-Installationsmethoden finden Sie im *Administratorhandbuch*.

Mögliche Installationsmethoden:

- Anmeldeskript-Setup

Das Anmeldeskript-Setup ist geeignet, wenn kein WAN vorhanden ist, da der lokale Datenverkehr hierfür unerheblich ist. Sofern jedoch mehr als 50 MB Daten auf die einzelnen Endpunkte übertragen werden, kann diese Option nicht verwendet werden.

- Remote-Installation über die Webkonsole

Diese Methode eignet sich für alle über das LAN verbundenen Endpunkte im Hauptbüro. Da auf all diesen Endpunkten Windows Server 2012 ausgeführt wird, lässt sich das Paket ganz einfach auf die Endpunkte verteilen.

Aufgrund der geringen Verbindungsgeschwindigkeit zwischen zwei Remote-Standorten kann sich diese Verteilungsmethode negativ auf die verfügbare Bandbreite auswirken, wenn die Bereitstellung von OfficeScan während der Geschäftszeiten erfolgt. Außerhalb der Geschäftszeiten, wenn die meisten Mitarbeiter nicht mehr im Büro sind, steht Ihnen die gesamte Verbindungskapazität für die Installation von OfficeScan zur Verfügung. Auf

ausgeschalteten Endpunkten kann OfficeScan jedoch nicht erfolgreich installiert werden.

- OfficeScan Agent-Paketbereitstellung

Die Verteilung mit dem OfficeScan Agent-Paket eignet sich am besten für die Bereitstellung an einem Remote-Standort. Am Remote-Standort 2 ist jedoch kein lokaler Server vorhanden, der diese Option ausreichend unterstützt.

Nach eingehender Betrachtung aller Möglichkeiten eignet sich diese Option für die meisten Endpunkte am besten.

Verteilung im Hauptbüro

Am Hauptsitz lässt sich der agent am einfachsten in Form einer Remote-Installation über die OfficeScan Webkonsole verteilen. Weitere Informationen zu dem Verfahren finden Sie im *Administratorhandbuch*.

Verteilung am Remote-Standort 1

Bei der Verteilung auf den Remote-Standort 1 muss das verteilte Dateisystem (DFS) von Microsoft konfiguriert werden. Weitere Informationen über DFS finden Sie unter <http://support.microsoft.com/?kbid=241452>. Nach der Konfiguration des verteilten Dateisystems muss dieses auf dem Server 3 am Remote-Standort 1 aktiviert werden, wobei die vorhandene DFS-Umgebung repliziert oder eine neue Umgebung erstellt wird.

Eine geeignete Verteilungsmethode besteht in der Erstellung eines agent-Pakets im MSI-Format (Microsoft Installer Package) und der Bereitstellung des agent-Pakets auf dem verteilten Dateisystem. Weitere Informationen zu dem Verfahren finden Sie im *Administratorhandbuch*. Da das Paket beim nächsten zeitgesteuerten Update auf Server 3 repliziert wird, wirkt sich die Verteilung des agent-Pakets nur geringfügig auf die Bandbreite aus.

Sie können ein agent-Paket auch über Active Directory verteilen. Weitere Informationen finden Sie im *Administratorhandbuch*.

Auswirkungen von Komponenten-Updates im WAN möglichst gering halten

Prozedur

1. Bestimmen Sie einen agent, der an Remote-Standort 1 die Funktion des Update-Agents übernimmt.
 - a. Melden Sie sich bei der Webkonsole an und navigieren Sie zu **Agents > Agent-Verwaltung**.
 - b. Wählen Sie in der agent-Hierarchie den agent aus, der die Funktion des Update-Agents übernehmen soll, und klicken Sie auf **Einstellungen > Update-Agent-Einstellungen**.
 2. Wählen Sie an Remote-Standort 1 die agents aus, deren Komponenten über den Update-Agent aktualisiert werden.
 - a. Navigieren Sie zu **Updates > Server > Update-Adresse**.
 - b. Wählen Sie **Benutzerdefinierte Update-Adresse**, und klicken Sie auf **Hinzufügen**.
 - c. Geben Sie im angezeigten Fenster den IP-Adressbereich der Endpunkte an Remote-Standort 1 an.
 - d. Wählen Sie **Update-Adresse** aus, und wählen Sie anschließend den designierten Update-Agent im Listenfeld aus.
-

Verteilung am Remote-Standort 2

Das Hauptproblem beim Remote-Standort 2 ist die geringe Bandbreite. 60 Prozent der Bandbreite sind jedoch während der Geschäftszeiten frei, wenn eine Bandbreite von ca. 154 Kb/s zur Verfügung steht.

Am besten installieren Sie den OfficeScan Agent, indem Sie dasselbe agent-Paket in dem an Remote-Standort 1 verwendeten MSI-Format verwenden. Da jedoch kein Server verfügbar ist, können Sie kein verteiltes Dateisystem (Distributed File System, DFS) verwenden.

Eine Möglichkeit besteht in der Verwendung von Management-Tools anderer Hersteller, mit denen der Administrator freigegebene Verzeichnisse auf Remote-Endpunkten erstellen oder konfigurieren kann, ohne physisch auf diese Endpunkte zuzugreifen. Nachdem das freigegebene Verzeichnis auf einem einzelnen Endpunkt erstellt wurde, ist für das Kopieren des agent-Pakets in das Verzeichnis weniger Aufwand erforderlich als für die Installation des agents auf neun Endpunkten.

Verwenden Sie eine weitere Active Directory Richtlinie, geben Sie die DFS Freigabe jedoch wieder nicht als Adresse an.

Mit diesen Methoden verbleibt der durch die Installation entstehende Datenverkehr innerhalb des lokalen Netzwerks. Das WAN ist durch den Datenverkehr nur in geringem Maß betroffen.

Um die Auswirkung von Komponenten-Updates im WAN möglichst zu minimieren, bestimmen Sie einen agent als Update-Agent. Weitere Informationen finden Sie unter *Verteilung am Remote-Standort 1 auf Seite A-6*.

Stichwortverzeichnis

A

Active Directory, 1-11, A-6
Agent-Installationspfad, 1-22, 2-35
Aktivierung, 1-19, 2-21, 3-76
Aktivierungscode, 1-3, 2-21, 3-76
Anmeldeskript-Setup, A-5
Anregungen und Kritik, 7-6
Antwortdatei, 2-2
Ausnahmen
 Performance Tuning Tool, 6-2
automatisches Agent-Upgrade, 3-4, 3-13, 3-18

B

Begriffe, x
Bewertungsmodus, 2-38

C

Case Diagnostic Tool, 6-2
Client Mover, 5-2
Client Packager, A-6
Control Manager, 1-10

D

Datenbanksicherung, 1-13, 1-23, 5-3
Debug-Protokolle
 Server, 6-5
Deinstallation
 Verwenden des
 Deinstallationsprogramms, 5-5
Dokumentation, viii

E

Erstinstallation, 2-2
 Checkliste, 1-16
 Systemvoraussetzungen, 1-2

Überlegungen, 1-4
Überprüfung, 4-2
Zusammenfassung, 2-44, 3-37, 3-50, 3-61,
3-89

F

Fehlerbehebung, 6-1
firewall, 2-37, 3-47

H

Herkömmliche Suche, 1-8
HTTP-Port, 1-18, 2-16, 3-71

I

Inkrementelles Pattern, 1-9
Installation
 Aufgaben nach der Installation, 4-1
 Protokolle, 6-5
Installationspfad
 agent, 1-22, 2-35
 server, 1-17
 Server, 2-13, 3-68
Installationsziel, 2-9, 3-23, 3-40, 3-53, 3-64
Integrierter Smart Protection Server, 1-8, 5-5
 Agent-Verbindungsprotokolle, 2-24, 3-32,
3-79
 Deinstallation, 5-6
 installation, 2-23, 3-31, 3-78
Intelligente Suche, 1-8
IPv6-Unterstützung, 1-4

K

Kennwörter, 1-21, 2-33
Kompatibilitätsprobleme, 1-24
Komponenten, 4-5

Komponentenduplizierung, 1-9

Komponenten-Updates, 1-9

M

Manuelles Agent-Upgrade, 3-13

Manuelles Update, 4-5

Microsoft Exchange Server, 1-25

MSI Paket, Verteilung, A-6

N

Nach der Installation, 4-1

Netzwerkverkehr, 1-9

Nicht unterstützte Betriebssysteme, 1-12

O

OfficeScan

Dokumentation, viii

OfficeScan Agent

Beenden, 2-34

Sicherheitsstufe, 2-36

OfficeScan firewall, 2-37, 3-47

OfficeScan server

Debug-Protokolle, 6-5

Dienste, 4-3

Erstinstallation, 2-2

Funktionen, 1-7

Installationsprotokolle, 4-3

Installationszusammenfassung, 2-44,
3-37, 3-50, 3-61, 3-89

Leistung, 1-7

Manuelles Update, 4-5

Master-Dienst, 2-15, 3-70, 4-3

Mit Control Manager verwalten, 1-10

Produktmodule, 1-3

Prozesse, 4-3

Registrierungsschlüssel, 4-4

Speicherort, 1-5

Standardeinstellungen, 4-5

P

Performance Tuning Tool, 6-2

port

Port für die Agent-Kommunikation,
2-36

Proxy-Server-Port, 1-17

Server-Listening-Port, 1-13

Port

HTTP-Port, 1-18, 2-16, 3-71

Port für die Agent-Kommunikation,
1-22

Server-Listening-Port, 1-13, 3-16

SSL-Port, 1-18

Programmeinstellungen, 5-3

Proxy-Server, 1-17

R

Readme-Datei, 2-45, 3-38, 3-51, 3-62, 3-90

Registrierung, 1-19, 2-21, 3-76

Registrierungsschlüssel, 1-3

Remote-Installation, 1-6, 1-20, 2-10, 2-26, 2-28,
3-81, 3-83, A-5

Remote-Upgrade, 3-24, 3-41, 3-54, 3-65

Root-Konto, 1-21, 2-34

RSA-Verschlüsselung, 2-17, 3-72

S

server

Identifikation, 2-18, 2-19, 3-73, 3-74

Serverauthentifizierungszertifikat, 1-23

Sicherheits-Software anderer Anbieter, 1-11

Sichern

OfficeScan Datenbank, 5-3

OfficeScan Server-Dateien und -
Ordner, 5-4

Smart Protection Network, 2-31
Smart Protection Server, 1-8, 2-23, 2-24, 3-31,
3-32, 3-78, 3-79, 5-5, 5-6
SQL-Server, 1-26
SSL-Port, 1-18, 2-17, 3-72
SSL-Tunnel, 2-17, 3-72
Standardeinstellungen
 Agent-Berechtigungen, 4-6
 Globale Agent-Einstellungen, 4-6
 Sucheinstellungen, 4-6
Suchmethode, 1-7
support
 Probleme schneller beheben, 7-4
Support-Informationssystem, 6-2
Systemvoraussetzungen
 Erstinstallation, 1-2

T

Testversion, 1-3
Testverteilung
 Auswertung, 1-24
 Rollback-Plan, 1-24
 Teststandort, 1-24
TMPerftool, 6-2

U

Überlegungen
 Erstinstallation, 1-4
 Upgrade, 1-12
Update-Agent, 1-10
Updates, 1-9
upgrade
 agents, 3-13
 Checkliste, 1-16
 summary, 2-44, 3-37, 3-50, 3-61, 3-89
 Überlegungen, 1-12
 Überprüfung, 4-2

Upgrade

 Agents, 3-17
 Überprüfung, 4-2

V

Verknüpfung mit Programmordner, 1-23,
2-43, 4-2
Verteiltes Dateisystem (DFS), A-6
Virensuche vor der Installation, 2-11, 3-25,
3-42, 3-55, 3-66
Vollversion, 1-3

W

Webkonsole, 2-34, 2-45, 3-38, 3-51, 3-62, 3-90, 4-2
webserver, 1-11, 1-18, 2-15, 3-70



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: OSGMXG7614/161028