TREND MICRO™

OfficeScan™ 10.6

For Enterprise and Medium Business

Installations- und Upgrade-Handbuch

Endpoint Security

Protected Cloud

Web Security

Dokument-Nr. OSEM104849/110518

Release-Datum: August 2011

Geschützt durch US-Patent-Nr. 5.623.600; 5.889.943; 5.951.698; 6.119.165

In der Benutzerdokumentation für Trend Micro OfficeScan sind die wesentlichen Funktionen der Software und Installationsanweisungen für Ihre Produktionsumgebung erläutert. Lesen Sie die Dokumentation vor der Installation und Verwendung der Software aufmerksam durch.

Ausführliche Informationen über die Verwendung bestimmter Funktionen der Software finden Sie in der Online-Hilfe und der Knowledge Base auf der Homepage von Trend Micro.

Das Trend Micro Team ist stets bemüht, die Dokumentation zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder anderen Dokumenten von Trend Micro wenden Sie sich bitte an docs@trendmicro.com.

Bitte bewerten Sie diese Dokumentation auf der folgenden Website:

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

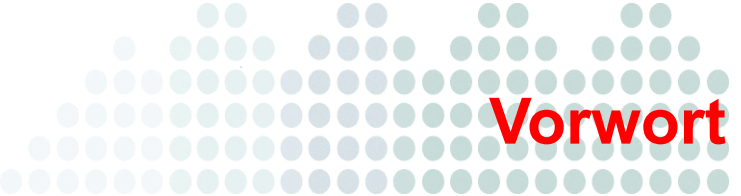
Inhalt

Vorwort

Kapitel 1: Installation und Upgrade von OfficeScan planen

Kapitel 2: OfficeScan installieren oder upgraden

Kapitel 3: Hilfe anfordern



Vorwort

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

Hinweis: Weitere Informationen zur Installation von Clients finden Sie im *Administratorhandbuch*.

Themen in diesem Kapitel:

OfficeScan Dokumentation

Die OfficeScan Dokumentation umfasst Folgendes:

TABELLE P-1. OfficeScan Dokumentation

DOKUMENTATION	BESCHREIBUNG
Installations- und Upgrade-Handbuch	Ein PDF-Dokument, in dem Anforderungen und Verfahren zum Installieren und Aktualisieren des Servers und der Clients beschrieben werden.
Administratorhandbuch	Ein PDF-Dokument mit folgenden Inhalten: Informationen über die ersten Schritte, Verfahren zur Client-Installation, OfficeScan Server und Client-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-, Client- und Policy Server 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 neuesten Versionen der PDF-Dokumente und Readme-Dateien herunterladen von:

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 Servern und Clients. Von diesen Benutzern wird erwartet, dass sie über detaillierte Kenntnisse im Zusammenhang mit der Netzwerk- und Serververwaltung verfügen.
- **Cisco NAC Administratoren:** Verantwortlich für den Entwurf und die Verwaltung von Sicherheitssystemen mit Cisco™ NAC Servern und Cisco Netzwerkausrüstung. Es wird vorausgesetzt, dass sie Erfahrung mit diesen Geräten haben.
- **Endbenutzer:** Benutzer, auf deren Computer OfficeScan Client installiert ist. Die Kenntnisse dieser Personen reichen von Anfänger bis Power-Benutzer.

Dokumentationskonventionen

Damit Sie Informationen leicht finden und einordnen können, werden in der OfficeScan Dokumentation folgende Konventionen verwendet:

TABELLE P-2. Dokumentationskonventionen

KONVENTION	BESCHREIBUNG
NUR GROSSBUCHSTABEN	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur.
Fettdruck	Menüs und Menübefehle, Schaltflächen, Registerkarten, Optionen und Aufgaben.
Kursivdruck	Verweise auf andere Dokumentation oder neue Technologiekomponenten.
TOOLS > CLIENT-TOOLS	Ein "Brotkrumen"-Pfad zu Beginn jedes Vorgangs, der dem Benutzer das Navigieren zum betreffenden Fenster der Webkonsole erleichtert. Mehrere Pfade bedeuten, dass der Zugriff auf ein Fenster über mehrere Wege möglich ist.

TABELLE P-2. Dokumentationskonventionen (Fortsetzung)

KONVENTION	BESCHREIBUNG
<Text>	Gibt an, dass der in spitze Klammern gesetzte Text durch die tatsächlichen Daten ersetzt werden sollte. Beispielsweise C:\Programme\<Dateiname> kann C:\Programme\beispiel.jpg sein.
Hinweis: Text	Stellt Konfigurationshinweise oder Empfehlungen bereit.
Tipp: Text	Stellt Best-Practice-Informationen und Trend Micro Empfehlungen bereit.
ACHTUNG! Text	Gibt Warnungen über Aktivitäten an, die die Computer im Netzwerk schädigen könnten.

Begriffe

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

TABELLE P-3. OfficeScan Terminologie

BEGRIFFE	BESCHREIBUNG
Client	Das OfficeScan Client-Programm.
Client-Computer oder Endpunkt	Der Computer, auf dem der OfficeScan Client installiert ist.
Client-Benutzer (oder Benutzer)	Die Person, die den OfficeScan Client auf dem Client-Computer verwaltet.
Server	Das OfficeScan Server-Programm.
Server computer	Der Computer, auf dem der OfficeScan Server installiert ist.
Administrator (oder OfficeScan Administrator)	Die Person, die den OfficeScan Server verwaltet.
Konsole	Die Benutzeroberfläche zur Konfiguration und Verwaltung der Einstellungen für den OfficeScan Server und die Clients. Die Konsole für das OfficeScan Server-Programm wird "Webkonsole" und die Konsole für das Client-Programm wird "Client-Konsole" genannt.
Sicherheitsrisiko	Der Oberbegriff für Viren/Malware, Spyware/Grayware und Internet-Bedrohungen.
Modul	Umfasst Antivirus, Damage Cleanup Services, Web Reputation und Anti-Spyware – alle Module werden während der Installation von OfficeScan Server aktiviert.

TABELLE P-3. OfficeScan Terminologie (Fortsetzung)

BEGRIFFE	BESCHREIBUNG
OfficeScan Dienste	Von der Microsoft Management-Konsole (MMC) verwaltete Dienste. Beispiel: ofcservice.exe, der OfficeScan Master Service.
Programm	Hierzu gehören der OfficeScan Client, der Cisco Trust Agent und der Plug-in-Manager.
Komponenten	Suchen und entdecken Sicherheitsrisiken und führen Aktionen gegen sie durch.
Installationsordner des Clients	Der Ordner auf dem Computer, in dem die OfficeScan Client-Dateien enthalten sind. Wenn Sie während der Installation die Standardeinstellungen akzeptieren, finden Sie den Installationsordner an einem der folgenden Speicherorte: **C:\Programme\Trend Micro\OfficeScan Client** **C:\Programme (x86)\Trend Micro\OfficeScan Client**
Installationsordner des Servers	Der Ordner auf dem Computer, 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:\Program Files\Trend Micro\OfficeScan\ PCCSRV\<Dateiname>.
Client der intelligenten Suche	Ein OfficeScan Client wurde so konfiguriert, dass die intelligente Suche verwendet wird.
Client der herkömmlichen Suche	Ein OfficeScan Client wurde so konfiguriert, dass die herkömmliche Suche verwendet wird.

TABELLE P-3. OfficeScan Terminologie (Fortsetzung)

BEGRIFFE	BESCHREIBUNG
Dual-Stack	Ein Gerät, das sowohl über IPv4- als auch IPv6-Adressen verfügt. Beispiel: • Ein Dual-Stack-Endpunkt ist ein Computer, der sowohl über IPv4- als auch über IPv6-Adressen verfügt. • Ein Dual-Stack-Client ist ein Client, der auf einem Dual-Stack-Endpunkt installiert ist. • Ein Dual-Stack-Update-Agent verteilt Updates an die Clients. • Ein Dual-Stack-Proxy-Server, wie etwa DeleGate, kann zwischen IPv4- und IPv6-Adressen konvertieren.
Reines IPv4	Ein Gerät, das nur über IPv4-Adressen verfügt.
Reines IPv6	Ein Gerät, das nur über IPv6-Adressen verfügt.
Plug-in-Lösungen	Native OfficeScan Funktionen und Plug-in-Programme, die über Plug-in Manager bereitgestellt werden.

Kapitel 1

Installation und Upgrade von OfficeScan planen

In diesem Kapitel wird die Vorbereitung der Installation und des Upgrades von Trend Micro™ OfficeScan™ beschrieben.

Themen in diesem Kapitel:

Systemvoraussetzungen für Erstinstallation und Upgrade

Sie können eine Erstinstallation von OfficeScan Server und Clients auf unterstützten Windows Server-Plattformen durchführen.

Außerdem unterstützt diese Version von OfficeScan Upgrades von den folgenden Versionen:

- OfficeScan 10.x
  - 10.5 Patch 1
  - 10.5
  - 10.0 Service Pack 1
  - 10.0
- OfficeScan 8.0 Service Pack 1

Besuchen Sie die folgende Webseite, um eine vollständige Liste der Systemvoraussetzungen für Erstinstallation und Upgrades zu erhalten:

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

Produktversionen und -schlüssel

Vollversion und Testversion

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, wenn Sie über keinen Aktivierungscode verfügen.

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. Falls Sie die Lizenz nach Ablauf der Übergangsfrist nicht verlängern, erhalten Sie keinen technischen Support und können keine Komponenten-Updates durchführen. Die Scan Engine durchsucht die Computer unter Verwendung nicht aktueller Komponenten weiterhin. Diese veralteten Komponenten schützen Ihre Computer möglicherweise nicht vollständig vor den aktuellen Sicherheitsrisiken. 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 Client-Funktionen.

Registrierungsschlüssel und Aktivierungscodes

Während der Installation fordert Sie das Setup-Programm zur Eingabe der Aktivierungscodes für Folgendes auf:

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

Falls Sie nicht über die Aktivierungscodes verfügen, verwenden Sie den Registrierungsschlüssel, den Sie mit dem Produkt erhalten haben. Setup leitet Sie automatisch zur Trend Micro Website, wo Sie Ihr Produkt registrieren können.

https://olr.trendmicro.com/REGISTRATION/eu/de/

Nach der Registrierung Ihres Produkts sendet Ihnen Trend Micro die Aktivierungscodes.

Wenn Sie weder über einen Registrierungsschlüssel noch einen Aktivierungscode verfügen, wenden Sie sich an Ihren Trend Micro Vertriebspartner. Weitere Informationen finden Sie unter *Kontaktaufnahme mit Trend Micro* auf Seite 3-8.

Hinweis: Weitere Informationen über die Registrierung finden Sie unter http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326.

Überlegungen zur Erstinstallation

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

IPv6-Unterstützung

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

- Der OfficeScan Server muss unter Windows Server 2008 installiert sein. Er darf nicht unter Windows Server 2003 installiert sein, da dieses Betriebssystem die IPv6-Adressierung nur teilweise unterstützt.
- Der Server muss einen IIS Webserver verwenden. Der Apache Webserver unterstützt keine IPv6-Adressierung.
- Wenn der Server IPv4- und IPv6-Clients verwaltet, muss er eine IPv4- wie auch eine IPv6-Adresse haben und über seinen Hostnamen identifiziert werden.
  Wenn der Server über seine IPv4-Adresse identifiziert wird, können IPv6-Clients keine Verbindung zum Server herstellen. Dasselbe Problem tritt auf, wenn reine IPv4-Clients eine Verbindung mit einem Server herstellen, der über seine IPv6-Adresse identifiziert wird.

- Wenn der Server nur IPv6-Clients 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.

- Vergewissern Sie sich, dass die IPv6- oder IPv4-Adresse des Host-Computers abgerufen werden kann. Verwenden Sie dazu z. B. den Befehl "ping" oder den Befehl "nslookup".
- Wenn Sie den OfficeScan Server auf einen reinen IPv6-Computer installieren:
  - Richten Sie einen Dual-Stack-Proxy-Server ein, der zwischen IPv4- und IPv6-Adressen konvertieren kann (wie etwa DeleGate). Platzieren Sie den Proxy-Server zwischen den OfficeScan Server und das Internet, damit der Server sich erfolgreich mit den von Trend Micro verwalteten Diensten verbinden kann, z. B. dem ActiveUpdate Server, der Online-Registrierungswebsite und Smart Protection Network.
  - Installieren Sie keinen Policy Server für Cisco NAC und Cisco Trust Agent. Diese Programme unterstützen keine IPv6-Adressierung.

Standort des OfficeScan Servers

OfficeScan kann an unterschiedlichste Netzwerkumgebungen angepasst werden. Sie können beispielsweise eine Firewall zwischen dem OfficeScan Server und den Clients positionieren, oder sowohl den Server als auch alle Clients hinter einer einzigen Netzwerk-Firewall anordnen. Falls sich zwischen dem Server und den Clients eine Firewall befindet, müssen Sie diese so konfigurieren, dass der Datenverkehr zwischen dem Client- und dem Server-Listening-Port zugelassen wird.

Hinweis: Weitere Informationen zur Lösung von Problemen, die bei der Verwaltung von OfficeScan Clients in einem Netzwerk mit NAT (Network Address Translation) auftreten können, finden Sie im *Administratorhandbuch*.

Remote-Installation

Bei einer Remote-Installation können Sie die Installation von OfficeScan auf einem bestimmten Computer von einem anderen Computer aus starten. Das Setup-Programm ermittelt bei einer Remote-Installation, ob der Zielcomputer die Voraussetzungen für die Installation des Servers erfüllt.

Sicherstellen, dass die Installation fortgesetzt werden kann:

- Starten Sie den Remote-Registrierungsdienst auf jedem Zielcomputer 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 den Host-Namen des Computers und die Anmeldedaten (Benutzername und Kennwort).
- Vergewissern Sie sich, dass der Computer 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 für den OfficeScan Server einen Computer, der über Dualprozessoren mit mindestens 2 GHz und mehr als 2 GB Arbeitsspeicher verfügt.

Wie viele vernetzte Client-Computer ein einziger OfficeScan Server verwalten kann, hängt von verschiedenen Faktoren ab, wie beispielsweise den verfügbaren Serverressourcen und der Netzwerktopologie. Bei Ihrem Trend Micro Vertriebspartner erhalten Sie Informationen, wie Sie die Anzahl der vom Server verwaltbaren Clients ermitteln.

Ein OfficeScan Server kann üblicherweise die folgende Anzahl von Clients verwalten:

- 3,000 bis 5,000 Clients bei einem OfficeScan Server mit 2-GHz-Dualprozessor und 2 GB RAM
- 5,000 bis 50,000 Clients bei einem OfficeScan Server mit 2,13-GHz-Core2Duo™-Prozessor und 4 GB RAM

Dedizierter Server

Bei der Auswahl des Computers für den OfficeScan Server muss Folgendes beachtet werden:

- Die CPU-Auslastung des Computers
- Andere Aufgaben des Computers

Falls der Zielcomputer noch andere Funktionen zu erfüllen hat, sollte es sich dabei nicht um kritische oder ressourcenintensive Anwendungen handeln.

Verteilung der Suchmethode während der Installation

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

Herkömmliche Suche

Die herkömmliche Suche ist die in allen früheren OfficeScan Versionen verwendete Suchmethode. Ein konventioneller Suchclient speichert alle OfficeScan Komponenten auf dem Clientcomputer und durchsucht die Dateien lokal.

Intelligente Suche

Bei der intelligenten Suche werden drei Signaturen verwendet, die im Internet gespeichert sind. Im intelligenten Suchmodus sucht der OfficeScan Client zunächst lokal nach Sicherheitsrisiken. Wenn der Client das Risiko der Datei während der Suche nicht ermitteln kann, stellt er 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-Definition-Updates muss lediglich ins Web und nicht zu den vielen Endpunkten 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

Bei Erstinstallationen ist die Standard-Suchmethode für Clients die intelligente Suche. Sie können nach der Installation des OfficeScan Servers die Suchmethode für jede Domäne anpassen. Beachten Sie Folgendes:

- Wenn Sie die Suchmethode nach der Installation des Servers nicht geändert haben, verwenden alle installierten Clients die intelligente Suche.
- Wenn die herkömmliche Suche auf allen Clients verwendet werden soll, ändern Sie nach der Installation der Server die Suchmethode auf Stammebene in herkömmliche Suche.
- Wenn Sie sowohl die herkömmliche als auch die intelligente Suche verwenden möchten, empfiehlt Trend Micro, die intelligente Suche aus 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 ein, wie viel Netzwerkverkehr 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 Clients zum Download aktualisierter Komponenten auf
- Benachrichtigt Clients bei Konfigurationsänderungen

Es entsteht Netzwerkverkehr, wenn der Client 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 Roaming-Modus in den Normalbetrieb
- Beim Wechsel von der herkömmlichen zur intelligenten Suche

Netzwerkverkehr während eines Komponenten-Updates

Beim Update von OfficeScan Komponenten kommt es zu erheblichem Netzwerkverkehr. Um den bei Komponenten-Updates entstehenden Netzwerkverkehr zu verringern, dupliziert OfficeScan Komponenten. 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.

Clients, die regelmäßig aktualisiert werden, laden nur die inkrementellen Pattern herunter. Anderenfalls wird die vollständige Pattern-Datei heruntergeladen.

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

Update-Agents und Netzwerkverkehr

Wenn sich zwischen den Clients und dem OfficeScan Server Netzwerkabschnitte mit geringer Bandbreite oder einem hohen Datenaufkommen befinden, können Sie ausgewählte OfficeScan Clients als Update-Agents oder Update-Adressen für andere Clients bestimmen. Dadurch wird die Verteilung von Komponenten auf alle Clients besser ausgelastet.

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

Trend Micro Control Manager und Netzwerkverkehr

Der Trend Micro Control Manager™ verwaltet Produkte und Services von Trend Micro auf Gateways, Mail-Servern, File-Servern und Unternehmensdesktops. Die webbasierte Management-Konsole des Control Managers 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, zuverlässigen Internet-Verbindung kann die Komponenten direkt vom Trend Micro ActiveUpdate Server herunterladen. Anschließend verteilt der Control Manager die Komponenten an einen oder mehrere OfficeScan Server, die über eine ungenügende oder keine Internet-Verbindung verfügen.

Weitere Informationen zum Control Manager finden Sie in der Control Manager Dokumentation.

Sicherheits-Software anderer Anbieter

Entfernen Sie Endpunkt-Sicherheitssoftware von Drittanbietern von dem Computer, auf dem Sie den OfficeScan Server installieren möchten. Das Vorhandensein solcher Anwendungen kann die erfolgreiche Installation von OfficeScan Server verhindern oder dessen Leistung beeinträchtigen. Installieren Sie den OfficeScan Server und den Client unverzüglich, nachdem Sie die Sicherheitssoftware von Drittanbietern entfernt haben, um den Computer keinen Sicherheitsrisiken auszusetzen.

Hinweis: OfficeScan kann nur die Client-, nicht jedoch die Serverkomponente anderer Antiviren-Produkte automatisch deinstallieren. Weitere Informationen finden Sie im *Administratorhandbuch*.

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.

Webserver

Die Funktionen des OfficeScan Webservers sind Folgende:

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

Sie können einen IIS oder einen Apache Webserver verwenden. Stellen Sie bei Verwendung eines IIS Webservers sicher, dass auf dem Server-Computer keine Anwendungen ausgeführt werden, die IIS nicht unterstützen. Setup beendet den IIS Dienst automatisch während der Installation und startet ihn erneut.

Wenn Sie einen Apache Webserver verwenden, wird auf diesem als einziges Konto das Administratorkonto erstellt. Erstellen Sie ein anderes Konto, über das der Webserver ausgeführt wird, um die Sicherheit des OfficeScan Servers nicht zu gefährden, falls ein Hacker die Kontrolle über den Apache Webserver übernimmt.

Weitere Informationen über Upgrades, Patches und Sicherheitsfragen im Zusammenhang mit dem Apache Webserver finden Sie unter http://www.apache.org.

Überlegungen zum Upgrade

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

IPv6-Unterstützung

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

- Der zu aktualisierende OfficeScan Server muss unter Windows Server 2008 installiert sein. OfficeScan Server unter Windows Server 2003 können nicht aktualisiert werden, da Windows Server 2003 die IPv6-Adressierung nur teilweise unterstützt.
- Der zu aktualisierende OfficeScan Server muss in der Version 10.x oder 8.0 SP1 vorliegen.
- Der Server muss bereits einen IIS Webserver verwenden. Der Apache Webserver unterstützt keine IPv6-Adressierung.
- Weisen Sie dem Server eine IPv6-Adresse zu. Zusätzlich muss der Server über seinen Hostnamen identifiziert werden, vorzugsweise seinen vollqualifizierten Domänennamen (FQDN). Wenn der Server über seine IPv6-Adresse identifiziert wird, verlieren alle aktuell vom Server verwalteten Clients ihre Verbindung mit dem Server. Wenn der Server über seine IPv4-Adresse identifiziert wird, kann der Server den Client nicht an reine IPv6-Computer verteilen.
- Vergewissern Sie sich, dass die IPv6- oder IPv4-Adresse des Host-Computers abgerufen werden kann. Verwenden Sie dazu z. B. den Befehl "ping" oder den Befehl "nslookup".

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 von OfficeScan 10.x/8.0 SP1 aus ein Upgrade auf diese Version durchführen möchten und wenn Sie OfficeScan 10.x/8.0 SP1 Clients mit diesen Betriebssystemen haben:

- Führen Sie kein Upgrade aller 10.x/8.0 SP1 Server auf diese OfficeScan Version durch.
- Bestimmen Sie mindestens einen OfficeScan 10.x oder OfficeScan 8.0 SP1 Server (übergeordneten Server) für die Verwaltung der Clients, auf denen nicht unterstützte Betriebssysteme laufen.
- Vor dem Upgrade der anderen Server:
  - Öffnen Sie die Webkonsole, und klicken Sie im Hauptmenü auf **Netzwerkcomputer > Client-Verwaltung**.
  - Wählen Sie in der Client-Hierarchie die Clients aus, die Sie verschieben möchten, 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 Computernamen oder die IP-Adresse des Servers sowie den Server-Listening-Port an.
  - Klicken Sie auf **Verschieben**.

Wenn Sie den OfficeScan Server upgegradet, jedoch die nicht unterstützten Clients nicht verschoben haben, verwenden Sie das Tool Client Mover für veraltete Plattformen, um die Clients auf einen übergeordneten Server zu verschieben, die diese verwalten können. Detaillierte Hinweise zum Tool finden Sie unter *Client Mover für veraltete Plattformen verwenden* auf Seite 2-73.

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 Programmordners.

Die OfficeScan Datenbank und die Konfigurationsdateien sichern und wiederherstellen:

1. Sichern Sie die Datenbank über die Webkonsole von OfficeScan 10.x/8.0 SP1, indem Sie zu **Administration > Datenbanksicherung navigieren**.

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

   ACHTUNG! **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. Sichern Sie manuell folgende Dateien und Ordner unter <Installationsordner des Servers>\PCCSRV:

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

   - **ofcscan.ini:** Diese Datei enthält allgemeine Client-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. Führen Sie ein Upgrade des OfficeScan Servers durch.

Hinweis: Kopieren Sie in einem solchen Fall die Sicherungsdateien aus Schritt 3 in den Ordner <Installationsordner des Servers>\PCCSRV auf dem Zielcomputer, und starten Sie den OfficeScan Master Service neu.

Verteilung der Suchmethode während des Upgrades

In dieser OfficeScan Version können Sie Clients so konfigurieren, dass sie entweder die intelligente suche oder die herkömmliche suche verwenden.

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

Upgrade von OfficeScan 10.x:

- Wenn Sie ein Upgrade von OfficeScan 10.x Server direkt auf dem Server-Computer planen, brauchen Sie keine Änderungen an der Suchmethode über die Webkonsole vornehmen, weil die Clients nach dem Upgrade ihre Einstellungen für die Suchmethode beibehalten.
- Wenn Sie ein Upgrade von OfficeScan 10.x Clients durch Verschieben auf einen OfficeScan 10.6 Server planen:
  - Wählen Sie auf dem OfficeScan 10.6 Server die manuelle Client-Gruppierung. Bei dieser Methode zur Client-Gruppierung können Sie neue Domänen erstellen.

Hinweis: Wenn Sie planen, die automatische Client-Gruppierung zu verwenden, aktivieren Sie diese erst, nachdem alle Clients das Upgrade erhalten haben, um sicherzustellen, dass während des Client-Upgrade die Einstellungen für die Suchmethode beibehalten werden.

- Kopieren Sie die Einstellungen für die Domänenstruktur und die Suchmethode auf dem OfficeScan 10.x Server auf den OfficeScan 10.6 Server. Wenn die Einstellungen für die Domänenstruktur und die Suchmethode auf beiden Servern nicht identisch sind, werden auf einigen Clients, die auf die OfficeScan 10.6 Server verschoben wurden, nicht die ursprünglichen Einstellungen für die Suchmethode angewendet.

Upgraden von OfficeScan 8.0 SP1

- Wenn Sie ein Upgrade von OfficeScan 8.0 SP1 Server direkt auf dem Server-Computer planen:

  Alle Clients verwenden die intelligente Suche:

  i. Verhindern Sie automatische Updates und Upgrades der Clients.

  Weitere Informationen finden Sie unter *Teil 1: Konfigurieren der Update-Einstellungen auf dem OfficeScan Server der Version 10.x oder 8.0 SP1* auf Seite 2-4.

  ii. Führen Sie ein Upgrade des OfficeScan Servers durch.

  Weitere Informationen finden Sie unter *Teil 2: Upgrade des OfficeScan Servers durchführen* auf Seite 2-5.

  iii. Ändern Sie die Suchmethode auf Stammebene in die intelligente Suche.

  iv. Führen Sie Upgrades der Clients durch.

  Weitere Informationen finden Sie unter *Teil 3: Upgrade der OfficeScan Clients durchführen* auf Seite 2-5.

  Alle Clients verwenden die herkömmliche Suche:

  i. Führen Sie ein Upgrade des OfficeScan Servers durch.

  Einzelheiten zum ausschließlichen Upgrade des Servers und anschließender Staffelung des Client-Upgrades finden Sie unter *Teil 2: Upgrade des OfficeScan Servers durchführen* auf Seite 2-5.

  Einzelheiten zum automatischen Upgrade der Server und Clients finden Sie unter *Teil 2: Upgrade des OfficeScan Servers durchführen* auf Seite 2-16.

ii. Client-Upgrades

Weitere Informationen finden Sie unter *Teil 3: Upgrade der OfficeScan Clients durchführen* auf Seite 2-5.

Die meisten Clients verwenden die intelligente Suche:

Trend Micro empfiehlt, die folgenden Aufgaben durchzuführen:

i. Verhindern Sie automatische Updates und Upgrades der Clients.

Weitere Informationen finden Sie unter *Teil 1: Konfigurieren der Update-Einstellungen auf dem OfficeScan Server der Version 10.x oder 8.0 SP1* auf Seite 2-4.

ii. Führen Sie ein Upgrade des OfficeScan Servers durch.

Weitere Informationen finden Sie unter *Teil 2: Upgrade des OfficeScan Servers durchführen* auf Seite 2-5.

iii. Ändern Sie die Suchmethode auf Stammebene in die intelligente Suche.

iv. Führen Sie ein Upgrade der Clients durch (alle Clients verwenden die intelligente Suche).

Weitere Informationen finden Sie unter *Teil 3: Upgrade der OfficeScan Clients durchführen* auf Seite 2-5.

v. Ändern Sie die Suchmethode der Clients, die die herkömmliche Suche verwenden sollen.

- Wenn Sie planen, ein Upgrade der Clients durchzuführen, indem Sie sie auf einen OfficeScan 10.6 Server verschieben:

Alle Clients verwenden die intelligente Suche:

i. Verschieben Sie auf dem OfficeScan 8.0 SP1 Server die Clients auf den OfficeScan 10.6 Server.

Weitere Informationen finden Sie unter *Upgrade-Methode 3: Clients auf einen OfficeScan 10.6 Server verschieben* auf Seite 2-14.

Alle Clients verwenden die herkömmliche Suche:

i. Ändern Sie auf dem OfficeScan 10.6 Server die Suchmethode auf Stammebene in die herkömmliche Suche.

ii. Verschieben Sie auf dem OfficeScan 8.0 SP1 Server die Clients auf den OfficeScan 10.6 Server.

Weitere Informationen finden Sie unter *Teil 2: Upgrade der OfficeScan Clients durchführen* auf Seite 2-15.

Die meisten Clients verwenden die intelligente Suche:

i. Auf dem OfficeScan 8.0 SP1 Server:

- Identifizieren Sie, welche Domänen die intelligente Suche und welche die herkömmliche Suche anwenden. Beispiel: Auf den Domänen A1, A2 und A3 wird die intelligente Suche und auf den Domänen A4, A5 und A6 die herkömmliche Suche angewendet.
- Vergewissern Sie sich, dass die OfficeScan 8.0 SP1 Clients, die die intelligente Suche verwenden sollen, unter den Domänen A1, A2 oder A3 gruppiert sind.
- Vergewissern Sie sich, dass die OfficeScan 8.0 SP1 Clients, die die herkömmliche Suche verwenden sollen, unter den Domänen A4, A5 oder A6 gruppiert sind.

ii. Auf dem OfficeScan 10.6 Server:

- Wählen Sie die manuelle Client-Gruppierung. Bei dieser Methode zur Client-Gruppierung können Sie neue Domänen erstellen.
- Erstellen Sie die Domänen A1, A2, A3, A4, A5 und A6. Verwenden Sie die genauen Domänennamen.
- Ändern Sie die Suchmethode der Domänen A4, A5 und A6 in die herkömmliche Suche.

iii. Auf dem OfficeScan 8.0 SP1 Server:

- Verschieben Sie Clients auf den OfficeScan 10.6 Server.

Weitere Informationen finden Sie unter *Teil 2: Upgrade der OfficeScan Clients durchführen* auf Seite 2-15.

Installations- und Upgrade-Checkliste

Während der Installation oder des Upgrades des OfficeScan Servers fordert Sie das Setup-Programm zur Eingabe folgender Informationen auf:

TABELLE 1-1. Installations-Checkliste

INSTALLATIONSDATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAUFSICHTIGTE ERSTINSTALLATION	REMOTE-ERSTINSTALLATION	LOKAL/ UNBEAUFSICHTIGTES UPGRADE	REMOTE-UPGRADE
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, falls Sie nicht den Standardpfad verwenden möchten. Wenn der Pfad nicht vorhanden ist, erstellt Setup ihn.	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

TABELLE 1-1. Installations-Checkliste (Fortsetzung)

INSTALLATIONSDATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAUFSICHTIGTE ERSTINSTALLATION	REMOTE-ERSTINSTALLATION	LOKAL/ UNBEAUFSICHTIGTES UPGRADE	REMOTE-UPGRADE
Web-Server-Einstellungen Der Webserver (Apache oder IIS Webserver) führt CGI-Skripte für die Webkonsole aus und nimmt Befehle von den Clients entgegen. Geben Sie Folgendes ein: • HTTP-Port: Der Standardport ist 8080. Falls Sie die Standard-IIS-Website verwenden, prüfen Sie den TCP-Port des HTTP-Servers. **ACHTUNG! 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 Sie derzeit die Standardports nutzen.** *Falls sichere Verbindungen aktiviert werden:* • Gültigkeitsdauer des SSL-Zertifikats • SSL-Port (Standard: 4343)	Ja	Ja	Nein	Ja

TABELLE 1-1. Installations-Checkliste (Fortsetzung)

INSTALLATIONSDATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAUFSICHTIGTE ERSTINSTALLATION	REMOTE-ERSTINSTALLATION	LOKAL/ UNBEAUFSICHTIGTES UPGRADE	REMOTE-UPGRADE
Registrierung Registrieren Sie das Produkt, um die Aktivierungscodes zu erhalten. Für die Registrierung benötigen Sie Folgendes: *Für Benutzer mit Benutzerkonto* • Online-Registrierungskonto (Anmeldename und -Kennwort) *Für Benutzer ohne Benutzerkonto* • Registrierungsschlüssel	Ja	Ja	Ja	Ja
Aktivierung Beziehen Sie die Aktivierungscodes für folgende Produkt-Dienste: • Virenschutz • Damage Cleanup Services • Web Reputation und Anti-Spyware	Ja	Ja	Ja	Ja
Installation des integrierten Smart Protection Servers Wenn Sie die Installation des integrierten Servers wählen, geben Sie Folgendes an: • Gültigkeitsdauer des SSL-Zertifikats • SSL-Port	Ja	Ja	Ja	Ja

TABELLE 1-1. Installations-Checkliste (Fortsetzung)

INSTALLATIONSDATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAUFSICHTIGTE ERSTINSTALLATION	REMOTE-ERSTINSTALLATION	LOKAL/ UNBEAUFSICHTIGTES UPGRADE	REMOTE-UPGRADE

Ziel der Remote-Installation
Geben Sie die Computer an, auf denen Sie den OfficeScan Server installieren bzw. upgraden möchten. Bereiten Sie Folgendes vor:
• Eine Liste der Computernamen oder IP-Adressen
• (Optional) Eine Textdatei mit einer Liste der Namen oder IP-Adressen der Zielcomputer
Beispiel der Textdatei:
`Benutzer_01`
`Admin_01`
`123.12.12.123`
	Nein	Ja	Nein	Ja

Remote-Installation – Computeranalyse Vor der Analyse des Zielcomputers fordert Sie das Setup-Programm zur Eingabe folgender Informationen auf: • Benutzername und Kennwort eines Administratorkontos auf dem Zielcomputer mit der Berechtigung "Anmeldung als Dienst"	Nein	Ja	Nein	Ja
Andere OfficeScan Programme installieren Falls Sie Cisco Trust Agent installieren, bereiten Sie Folgendes vor: • Zertifikatsdatei für Cisco Trust Agent	Ja	Nein	Nein	Nein

TABELLE 1-1. Installations-Checkliste (Fortsetzung)

INSTALLATIONSDATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAUFSICHTIGTE ERSTINSTALLATION	REMOTE-ERSTINSTALLATION	LOKAL/ UNBEAUFSICHTIGTES UPGRADE	REMOTE-UPGRADE
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 unberechtigte Deinstallieren oder Beenden des OfficeScan Clients, indem Sie Folgendes angeben: • Kennwort für das Deinstallieren/Beenden des Clients	Ja	Ja	Nein	Nein
Client-Installationspfad Geben Sie das Verzeichnis auf dem Client-Computer an, in dem der OfficeScan Client installiert wird. Geben Sie Folgendes ein: • Installationspfad: Der Standardpfad für die Client-Installation lautet $ProgramFiles\Trend Micro\ OfficeScan Client. Geben Sie den Installationspfad an, falls Sie nicht den Standardpfad verwenden möchten. Falls der Pfad nicht vorhanden ist, erstellt Setup ihn während der Client-Installation. • Client-Kommunikationsport: OfficeScan generiert die Portnummer über einen Zufallsgenerator. Übernehmen Sie die generierte Portnummer, oder geben Sie eine neue an.	Ja	Ja	Nein	Nein

TABELLE 1-1. Installations-Checkliste (Fortsetzung)

INSTALLATIONSDATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAUFSICHTIGTE ERSTINSTALLATION	REMOTE-ERSTINSTALLATION	LOKAL/ UNBEAUFSICHTIGTES UPGRADE	REMOTE-UPGRADE
Verknüpfung mit Programmordner Die Verknüpfung zum Installationsordner für den OfficeScan Server wird im Windows Startmenü angezeigt. Der Standardname der Verknüpfung lautet **Trend Micro OfficeScan Server-<Servername>**. Geben Sie einen anderen Namen an, falls Sie nicht den Standardnamen verwenden möchten.	Ja	Nein	Nein	Nein

TABELLE 1-1. Installations-Checkliste (Fortsetzung)

INSTALLATIONSDATEN	BENÖTIGTE INFORMATIONEN WÄHREND			
	LOKAL/ UNBEAUFSICHTIGTE ERSTINSTALLATION	REMOTE-ERSTINSTALLATION	LOKAL/ UNBEAUFSICHTIGTES UPGRADE	REMOTE-UPGRADE

Installation des Policy Servers
Bereiten Sie folgende Informationen vor, wenn Sie den Policy Server für Cisco NAC installieren möchten:
• Installationspfad: Wenn Sie den Standard-Installationspfad nicht übernehmen möchten, geben Sie einen Speicherort auf dem lokalen Computer an, auf dem der Policy Server installiert werden soll.
• Webserver-Konfiguration: Geben Sie die folgenden Einstellungen für den ausgewählten Webserver an:
  • HTTP-Port (Standard: 8081)
  • Falls sichere Verbindungen aktiviert werden:
  • Gültigkeitsdauer des SSL-Zertifikats
• SSL-Port (Standard: 4344)
• Kennwort der Webkonsole: Geben Sie das Kennwort für die Anmeldung an der Policy Server Konsole an.
• Authentifizierung des ACS-Servers: Der ACS Server empfängt über das Netzzugangsgerät Antiviren-Daten vom OfficeScan Client und leitet sie zur Überprüfung an eine externe Benutzerdatenbank weiter.
Geben Sie die Anmeldedaten an (Benutzername und Kennwort).
	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 Sie nach der vollständigen Verteilung Support benötigen werden. Sie ermöglicht Ihrem Installationsteam, den Verteilungsprozess zu proben und zu verfeinern. Außerdem können Sie feststellen, ob der Verteilungsplan den Sicherheitsanforderungen Ihres Unternehmens entspricht.

Weitere Informationen über eine OfficeScan Testverteilung 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 dem gleichen Computer installieren. Weitere Informationen zu Anwendungen von anderen Herstellern finden Sie in der Dokumentation.

Microsoft Small Business Server

Notieren Sie vor der Installation von OfficeScan Server auf einem Computer mit Microsoft Small Business Server™ und Microsoft Internet Security Acceleration Server (ISA) den von ISA verwendeten Serverport. Standardmäßig verwenden der OfficeScan Server und ISA den Port 8080.

Wählen Sie daher bei der Installation des OfficeScan Servers einen anderen Server-Listening-Port aus.

Microsoft Lockdown Tool und URLScan

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

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

URLScan daran hindern, in die Client-Server-Kommunikation einzugreifen:

1. Beenden Sie den Dienst "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 Client installieren möchten, benötigt OfficeScan Zugriff auf alle Dateien, die der Client durchsuchen soll. 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. Diese Einstellung kann auf der Webkonsole festgelegt werden (**Netzwerkcomputer > Allgemeine Client-Einstellungen > Einstellungen der Suche nach Viren/Malware**). Bei Verwendung von Microsoft Exchange 2007 finden Sie weitere Informationen über den Suchausschluss unter http://technet.microsoft.com/en-us/library/bb332342(EXCHG.80).aspx.

SQL-Server

SQL Server™-Datenbanken können nach Viren durchsucht werden. Dies kann jedoch bei Anwendungen, die auf die Datenbanken zugreifen, zu Leistungseinbußen führen. Daher sollten SQL-Server-Datenbanken und deren Backup-Ordner von der Echtzeitsuche ausgeschlossen werden. Erforderliche Virensuchen in einer Datenbank sollten bei geringem Netzaufkommen manuell durchgeführt werden, um die Leistung des Systems so wenig wie möglich zu beeinträchtigen.

Internet Connection Firewall (ICF)

Windows Server 2003 verfügt über eine integrierte Internet Connection Firewall (ICF). Wenn ICF verwendet werden soll, tragen Sie die OfficeScan Listening-Ports in die ICF-Ausnahmeliste ein. Weitere Informationen zur Konfiguration von Ausnahmelisten finden Sie in der Firewall-Dokumentation.

Kapitel 2

OfficeScan installieren oder upgraden

In diesem Kapitel werden die Schritte beschrieben, die für die Installation oder ein Upgrade von Trend Micro™ OfficeScan™ notwendig sind.

Themen in diesem Kapitel:

Erstinstallation des OfficeScan Servers durchführen

Für eine Erstinstallation führen Sie Setup auf einem Computer aus, der die systemvoraussetzungen für erstinstallation und upgrade für den OfficeScan Server erfüllt. Setup installiert den OfficeScan Server und Plug-in Manager 2.0. Diese Version von Plug-in Manager stellt die Widget-Funktionalität in OfficeScan bereit. Informationen zu den Installationsfenstern und Konfigurierungsoptionen finden Sie unter die setup-installationsfenster (auf Seite 2-21).

Methoden und Anweisungen zur Client-Erstinstallation finden Sie im *Administratorhandbuch*.

Upgrade des OfficeScan Servers und der Clients durchführen

Wenn Sie das Setup auf einem Computer mit einem OfficeScan Server der Version 10.x oder 8.0 SP1 ausführen, wird der Server aktualisiert. Wenn auf einem Computer Plug-in Manager installiert ist, aktualisiert Setup auch Plug-in Manager auf Version 2.0. Wenn Plug-in Manager nicht installiert ist, wird automatisch Version 2.0 installiert. Diese Version von Plug-in Manager stellt die Widget-Funktionalität in OfficeScan bereit.

Abhängig von der Netzwerkbandbreite und der Anzahl der Clients, die der OfficeScan Server verwaltet, staffeln Sie die Client-Upgrades oder führen das Upgrade für alle Clients direkt im Anschluss an das Upgrade des Servers durch.

Tipp: Trend Micro empfiehlt sehr, die OfficeScan Clients nach dem Upgrade neu zu starten, um sicherzustellen, dass alle OfficeScan Komponenten aktualisiert wurden.

Vor dem Upgrade des OfficeScan Servers und der Clients

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

1. Das Installationspaket enthält Updates für OfficeScan Firewall-Treiber. Ist die OfficeScan Firewall in Ihrer aktuellen OfficeScan Version aktiviert, kann dies beim Verteilen des Pakets zu folgenden Störungen des Client-Computers führen:

   - Beim Start des Updates für den allgemeinen Firewall-Treiber werden die Client-Computer vorübergehend vom Netzwerk getrennt. Die Benutzer werden vor der Verbindungstrennung nicht benachrichtigt.

     Durch eine Option auf der Webkonsole von OfficeScan 10 SP1 oder höher, die standardmäßig aktiviert ist, wird das Update des allgemeinen Firewall-Treibers so lange verzögert, bis der Client-Computer neu gestartet wird. Stellen Sie sicher, dass diese Option aktiviert ist, um Probleme wegen der unterbrochenen Verbindung zu vermeiden. Um den Status dieser Option zu überprüfen, öffnen Sie die Webkonsole, navigieren Sie zu **Netzwerkcomputer > Allgemeine Client-Einstellungen**, und wechseln Sie dann in den Abschnitt **Firewall-Einstellungen**. Die Option lautet **OfficeScan Firewall-Treiber erst nach einem Neustart des Systems aktualisieren**.

   - Nach der Verteilung des Pakets ist auf dem Client-Computer noch die vorherige Version des OfficeScan TDI-Treibers vorhanden. Die neue Version wird erst beim Neustart des Computers geladen. Wird der Neustart des OfficeScan Clients nicht sofort ausgeführt, treten wahrscheinlich Probleme auf.

     Ist in der Webkonsole die Option zur Anzeige der Neustartbenachrichtigung aktiviert, wird der 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. Um den Status dieser Option zu überprüfen navigieren Sie auf der Webkonsole zu **Netzwerkcomputer > Allgemeine Client-Einstellungen**, und wechseln Sie dann in den Abschnitt **Warneinstellungen**. Die Option lautet **Eine Benachrichtigung anzeigen, wenn der Client-Computer zum Laden eines Kerneltreibers neu gestartet werden muss**.

2. Der OfficeScan Server kann nicht auf diese Version upgraden, wenn:
   - Ein Client während des Server-Upgrades das Anmeldeskript-Setup (AutoPcc.exe) ausführt. Stellen Sie sicher, dass während der Installation dieses Patches kein Client 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.

Upgrade-Methoden

Verwenden Sie eine der folgenden Upgrade-Methoden:

- *Upgrade-Methode 1: Das automatische Client-Upgrade deaktivieren* auf Seite 2-4
- *Upgrade-Methode 2: Update-Agents aktualisieren* auf Seite 2-8
- *Upgrade-Methode 3: Clients auf einen OfficeScan 10.6 Server verschieben* auf Seite 2-14
- *Upgrade-Methode 4: Das automatische Client-Upgrade aktivieren* auf Seite 2-16

Upgrade-Methode 1: Das automatische Client-Upgrade deaktivieren

Wenn Sie das automatische Client-Upgrade deaktivieren, haben Sie die Möglichkeit, zuerst das Upgrade des Servers durchzuführen und im Anschluss daran die Clients gruppenweise upzugraden. Verwenden Sie diese Upgrade-Methode, wenn Sie eine große Zahl von Clients upgraden müssen.

Teil 1: Konfigurieren der Update-Einstellungen auf dem OfficeScan Server der Version 10.x oder 8.0 SP1

1. Navigieren Sie zu **Netzwerkcomputer > Client-Verwaltung**.

2. Klicken Sie in der Client-Struktur auf das Symbol der Root-Domäne  , um alle Clients auszuwählen.

3. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.
4. Aktivieren Sie **Clients können Komponenten aktualisieren, aber kein Upgrade des Clients durchführen oder Hotfixes verteilen**.
5. 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. Clients, die die Einstellungen nicht übernehmen, führen automatisch ein Upgrade durch.

Teil 2: Upgrade des OfficeScan Servers durchführen

Weitere Informationen zum Upgrade des OfficeScan Servers finden Sie unter *Die Setup-Installationsfenster* auf Seite 2-21.

Hinweis: Um den Update-Prozess zu beschleunigen, beenden Sie den OfficeScan Client, bevor Sie ein Upgrade eines OfficeScan Servers durchführen, auf dem Windows Server 2008 Standard 64 Bit ausgeführt wird.

Konfigurieren Sie nach Abschluss der Installation die Einstellungen des OfficeScan Servers über die Webkonsole, bevor Sie mit dem Upgrade der Clients beginnen.

Ausführliche Hinweise zur Konfiguration von OfficeScan Einstellungen finden Sie im *Administratorhandbuch* und in der *OfficeScan Server Hilfe*.

Teil 3: Upgrade der OfficeScan Clients durchführen

1. 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)

2. Wechseln Sie zu **Netzwerkcomputer > Client-Verwaltung**.
3. Wählen Sie in der Client-Hierarchie die Clients aus, bei denen Sie ein Upgrade durchführen möchten. Sie können eine oder mehrere Domänen bzw. einzelne oder alle Clients 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 **Clients können Komponenten aktualisieren, aber kein Upgrade des Clients durchführen oder Hotfixes verteilen**.
6. Klicken Sie auf **Speichern**.
7. Überprüfen Sie die Upgrade-Ergebnisse.
   - *Upgrade-Ergebnisse (Online-Clients)* auf Seite 2-6
   - *Upgrade-Ergebnisse (Offline-Clients)* auf Seite 2-7
   - *Upgrade-Ergebnisse (Roaming-Clients)* auf Seite 2-8
8. Starten Sie die Client-Computer neu, um das Upgrade der Clients fertig zu stellen.
9. Wiederholen Sie Schritt 2 bis Schritt 8, bis das Upgrade für alle Clients durchgeführt wurde.

Upgrade-Ergebnisse (Online-Clients)

Hinweis: Starten Sie die Client-Computer nach dem Upgrade neu.

Automatisches Upgrade

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

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

Manuelles Upgrade

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

- Erstellen Sie ein EXE- oder MSI-Client-Paket, und verteilen Sie es.

  Hinweis: Weitere Anweisungen zum Erstellen eines Client-Pakets finden Sie im *Administratorhandbuch*.

- Fordern Sie die Client-Benutzer auf, auf dem Client-Computer **Jetzt aktualisieren** auszuführen.
- Weisen Sie die Benutzer von Client-Computern, auf denen Windows Server 2003, XP Professional, Server 2008, Vista™ (alle Editionen außer Vista Home) oder 7™ (alle Editionen außer 7 Home) ausgeführt wird, an, folgende Schritte durchzuführen:
  - Stellen Sie eine Verbindung zum Servercomputer her.
  - Navigieren Sie zu \\<Name des Server-Computers>\ofcscan.
  - Starten Sie **AutoPcc.exe**.
- Weisen Sie Benutzer von Computern unter Windows XP Home, Vista Home oder 7 Home an, mit der rechten Maustaste auf die Datei **AutoPcc.exe** zu klicken und die Option **Als Administrator ausführen** auszuwählen.
- Starten Sie ein manuelles Client-Update.

Manuelle Client-Updates initiieren:

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

Upgrade-Ergebnisse (Offline-Clients)

Offline-Clients werden upgegradet, wenn sie wieder online sind.

Upgrade-Ergebnisse (Roaming-Clients)

Roaming-Clients werden upgegradet, wenn sie wieder online gehen, oder, falls der Client über Berechtigungen für zeitgesteuerte Updates verfügt, wenn das zeitgesteuerte Update ausgeführt wird.

Upgrade-Methode 2: Update-Agents aktualisieren

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

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

Teil 1: Konfigurieren der Update-Einstellungen auf dem OfficeScan Server der Version 10.x oder 8.0 SP1

1. Navigieren Sie zu **Netzwerkcomputer > Client-Verwaltung**.
2. Klicken Sie in der Client-Struktur auf das Symbol der Root-Domäne  , um alle Clients auszuwählen.
3. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.
4. Aktivieren Sie **Clients können Komponenten aktualisieren, aber kein Upgrade des Clients durchführen oder Hotfixes verteilen**.
5. 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. Clients, die die Einstellungen nicht übernehmen, führen automatisch ein Upgrade durch.

Teil 2: Upgrade des OfficeScan Servers durchführen

Weitere Informationen zum Upgrade des OfficeScan Servers finden Sie unter *Die Setup-Installationsfenster* auf Seite 2-21.

Konfigurieren Sie nach Abschluss der Installation die Einstellungen des OfficeScan Servers über die Webkonsole, bevor Sie mit dem Upgrade der Update-Agents beginnen.

Ausführliche Hinweise zur Konfiguration von OfficeScan Einstellungen finden Sie im *Administratorhandbuch* und in der *OfficeScan Server Hilfe*.

Teil 3: Update-Agents aktualisieren

1. Wechseln Sie zu **Netzwerkcomputer > Client-Verwaltung**.
2. Wählen Sie in der Client-Hierarchie die Update-Agents aus, bei denen Sie ein Upgrade durchführen möchten.

   Tipp: Um Update-Agents leichter zu lokalisieren, wählen Sie eine Domäne, navigieren Sie zur **Client-Hierarchie-Ansicht** oberhalb der Client-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 **Clients können Komponenten aktualisieren, aber kein Upgrade des Clients durchführen oder Hotfixes verteilen**.
5. Klicken Sie auf **Speichern**.
6. Navigieren Sie zu **Updates > Netzwerkcomputer > Manuelles Update**.
7. Wählen Sie die Option **Clients manuell auswählen**, und klicken Sie auf **Auswählen**.
8. Wählen Sie in der Client-Hierarchie, 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 **Client-Hierarchie-Ansicht** oberhalb der Client-Hierarchie, und wählen Sie anschließend **Update-Agent-Ansicht**.

9. Klicken Sie oben in der Client-Hierarchie auf **Komponenten-Update starten**.
10. Überprüfen 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.
    - Roaming-Update-Agents werden upgegradet, wenn sie wieder online gehen, oder, falls der Update-Agent über Berechtigungen für zeitgesteuerte Updates verfügt, wenn das zeitgesteuerte Update ausgeführt wird.
11. Starten Sie die Computer 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

1. Wechseln Sie zu **Netzwerkcomputer > Client-Verwaltung**.
2. Wählen Sie die Update-Agents in der Client-Hierarchie aus.

Tipp: Um Update-Agents leichter zu lokalisieren, wählen Sie eine Domäne, navigieren Sie zur **Client-Hierarchie-Ansicht** oberhalb der Client-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**
    - **Client-Programme und Hotfixes**
6. Klicken Sie auf **Speichern**. Warten Sie, bis der Update-Agent das Herunterladen des Client-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: Upgrade der OfficeScan Clients durchführen

1. 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)
2. Wechseln Sie zu **Netzwerkcomputer > Client-Verwaltung**.
3. Wählen Sie in der Client-Hierarchie die Clients aus, bei denen Sie ein Upgrade durchführen möchten. Sie können eine oder mehrere Domänen bzw. einzelne oder alle Clients 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 **Clients können Komponenten aktualisieren, aber kein Upgrade des Clients durchführen oder Hotfixes verteilen**.
6. Klicken Sie auf **Speichern**.
7. Überprüfen Sie die Upgrade-Ergebnisse.
   - *Upgrade-Ergebnisse (Online-Clients)* auf Seite 2-12
   - *Upgrade-Ergebnisse (Offline-Clients)* auf Seite 2-13
   - *Upgrade-Ergebnisse (Roaming-Clients)* auf Seite 2-13
8. Starten Sie die Client-Computer neu, um das Upgrade der Clients fertig zu stellen.
9. Wiederholen Sie Schritt 2 bis Schritt 8, bis das Upgrade für alle Clients durchgeführt wurde.

Upgrade-Ergebnisse (Online-Clients)

Hinweis: Starten Sie die Client-Computer nach dem Upgrade neu.

Automatisches Upgrade

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

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

Manuelles Upgrade

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

- Erstellen Sie ein EXE- oder MSI-Client-Paket, und verteilen Sie es.

  Hinweis: Weitere Anweisungen zum Erstellen eines Client-Pakets finden Sie im *Administratorhandbuch*.

- Fordern Sie die Client-Benutzer auf, auf dem Client-Computer **Jetzt aktualisieren** auszuführen.
- Weisen Sie die Benutzer von Client-Computern, auf denen Windows Server 2003, XP Professional, Server 2008, Vista (alle Editionen außer Vista Home) oder 7 (alle Editionen außer 7 Home) ausgeführt wird, zur Durchführung folgender Schritte an:
  - Stellen Sie eine Verbindung zum Servercomputer her.
  - Navigieren Sie zu \\<Name des Server-Computers>\ofcscan.
  - Starten Sie **AutoPcc.exe**.

- Weisen Sie Benutzer von Computern unter Windows XP Home, Vista Home oder 7 Home an, mit der rechten Maustaste auf die Datei **AutoPcc.exe** zu klicken und die Option **Als Administrator ausführen** auszuwählen.
- Starten Sie ein manuelles Client-Update.

Manuelle Client-Updates initiieren:

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

Upgrade-Ergebnisse (Offline-Clients)

Offline-Clients werden upgegradet, wenn sie wieder online sind.

Upgrade-Ergebnisse (Roaming-Clients)

Roaming-Clients werden upgegradet, wenn sie wieder online gehen, oder, falls der Client über Berechtigungen für zeitgesteuerte Updates verfügt, wenn das zeitgesteuerte Update ausgeführt wird.

Upgrade-Methode 3: Clients auf einen OfficeScan 10.6 Server verschieben

Führen Sie eine Erstinstallation des OfficeScan 10,6 Servers durch, und verschieben Sie anschließend die Clients auf diesen Server. Die Clients werden beim Verschieben automatisch auf OfficeScan 10.6 aktualisiert.

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

1. Führen Sie die Erstinstallation des OfficeScan 10.6 Servers auf einem Computer durch. Weitere Informationen finden Sie unter *Die Setup-Installationsfenster* auf Seite 2-21.
2. Öffnen Sie die OfficeScan 10.6 Webkonsole.
3. 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)
4. Navigieren Sie zu **Netzwerkcomputer > Client-Verwaltung**.
5. Klicken Sie in der Client-Struktur auf das Symbol der Root-Domäne  , um alle Clients auszuwählen.
6. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.
7. Deaktivieren Sie **Clients können Komponenten aktualisieren, aber kein Upgrade des Clients durchführen oder Hotfixes verteilen**.
8. Klicken Sie auf **Für alle Clients übernehmen**.
9. Notieren Sie sich folgende Informationen über den OfficeScan 10.6 Server. Geben Sie diese Angaben auf dem OfficeScan Server der Version 10.x/8.0 SP1 an, wenn Sie Clients verschieben.
   - Computername oder IP-Adresse
   - Server-Listening-Port

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

Teil 2: Upgrade der OfficeScan Clients durchführen

1. Navigieren Sie auf der Webkonsole von OfficeScan 10.x/8.0 SP1 zu **Updates > Zusammenfassung**.
2. Klicken Sie auf **Benachrichtigung abbrechen**. Diese Funktionen löscht die Benachrichtigungswarteschlange des Servers, wodurch Probleme beim Verschieben der Clients auf den OfficeScan 10.6 Server vermieden werden.

   ACHTUNG! **Führen Sie die anschließenden Schritte sofort danach durch. Falls die Benachrichtigungswarteschlange des Servers aktualisiert wird, bevor die Clients verschoben werden, ist die Verschiebung möglicherweise nicht erfolgreich.**

3. Navigieren Sie zu **Netzwerkcomputer > Client-Verwaltung**.
4. Wählen Sie in der Client-Hierarchie die Clients aus, bei denen Sie ein Upgrade durchführen möchten. Wählen Sie nur Online-Clients, weil Offline- und Roaming-Clients nicht verschoben werden können.
5. Klicken Sie auf **Client-Hierarchie verwalten > Client verschieben**.
6. Geben Sie unterhalb von **Ausgewählte(n) Client(s) online auf einen anderen OfficeScan Server verschieben** den Computernamen oder die IP-Adresse des Servers sowie den Server-Listening-Port des OfficeScan 10.6 Servers an.
7. Klicken Sie auf **Verschieben**.

Upgrade-Ergebnisse

- Die Verschiebung und das Upgrade der Online-Clients beginnt.
- Tipps zur Verwaltung von Offline- und Roaming-Clients:
  - Deaktivieren Sie den Roaming-Modus auf Clients, damit Sie das Upgrade durchführen können.
  - Weisen Sie im Fall von Offline-Clients die Benutzer an, eine Verbindung zum Netzwerk aufzubauen, so dass die Clients online gehen. Weisen Sie im Fall von Clients, die seit längerer Zeit offline sind, die Benutzer an, den Client vom Computer zu deinstallieren und anschließend mit Hilfe einer geeigneten Client-Installationsmethode (wie dem Client Packager), die im *OfficeScan Administratorhandbuch* beschrieben wird, den OfficeScan 10,6 Client zu installieren.

Hinweis: Starten Sie die Client-Computer neu, um das Upgrade der Clients fertig zu stellen.

Upgrade-Methode 4: Das automatische Client-Upgrade aktivieren

Nachdem das Upgrade des OfficeScan Servers auf diese Version durchgeführt wurde, fordert der Server unverzüglich alle von ihm verwalteten Clients auf, ebenfalls ein Upgrade durchzuführen.

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

Teil 1: Konfigurieren der Update-Einstellungen auf dem OfficeScan Server der Version 10.x oder 8.0 SP1

1. 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)
2. Navigieren Sie zu **Netzwerkcomputer > Client-Verwaltung**.
3. Klicken Sie in der Client-Struktur auf das Symbol der Root-Domäne  , um alle Clients auszuwählen.
4. Klicken Sie auf **Einstellungen > Berechtigungen und andere Einstellungen**, und wechseln Sie zur Registerkarte **Andere Einstellungen**.
5. Deaktivieren Sie **Clients können Komponenten aktualisieren, aber kein Upgrade des Clients durchführen oder Hotfixes verteilen**.
6. Klicken Sie auf **Für alle Clients übernehmen**.

Tipp: Planen Sie eine ausreichende Zeitspanne für die Verteilung der Einstellungen an alle Clients vor dem Upgrade des OfficeScan Servers ein.

Teil 2: Upgrade des OfficeScan Servers durchführen

Weitere Informationen zum Upgrade des OfficeScan Servers finden Sie unter *Die Setup-Installationsfenster* auf Seite 2-21.

Upgrade-Ergebnisse

- Das Upgrade der Online-Clients wird sofort nach Abschluss des Server-Upgrades durchgeführt.
- Offline-Clients werden upgegradet, wenn sie wieder online sind.
- Roaming-Clients werden upgegradet, wenn sie wieder online gehen, oder, falls der Client über Berechtigungen für zeitgesteuerte Updates verfügt, wenn das zeitgesteuerte Update ausgeführt wird.

Hinweis: Starten Sie die Client-Computer neu, um das Upgrade der Clients fertig zu stellen.

Unbeaufsichtigte Installation bzw. unbeaufsichtigtes Upgrade durchführen

Sie können die Installation bzw. das Upgrade mehrerer OfficeScan Server unbeaufsichtigt ablaufen lassen, falls die Installationseinstellungen dieser Server übereinstimmen.

Wenn auf dem Zielcomputer eine unbeaufsichtigte Installation ausgeführt wird, werden OfficeScan 10.6 und Plug-in Manager 2.0 vom Setup installiert. Wenn eine frühere Version von OfficeScan oder Plug-in Manager vorhanden ist, führt Setup ein Upgrade aus. Plug-in Manager 2.0 stellt die Widget-Funktionalität in OfficeScan bereit.

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

1. Das Installationspaket enthält Updates für OfficeScan Firewall-Treiber. Ist die OfficeScan Firewall in Ihrer aktuellen OfficeScan Version aktiviert, kann dies beim Verteilen des Pakets zu folgenden Störungen des Client-Computers führen:
   - Beim Start des Updates für den allgemeinen Firewall-Treiber werden die Client-Computer vorübergehend vom Netzwerk getrennt. Die Benutzer werden vor der Verbindungstrennung nicht benachrichtigt.

Durch eine Option auf der Webkonsole von OfficeScan 10 SP1 oder höher, die standardmäßig aktiviert ist, wird das Update des allgemeinen Firewall-Treibers so lange verzögert, bis der Client-Computer neu gestartet wird. Stellen Sie sicher, dass diese Option aktiviert ist, um Probleme wegen der unterbrochenen Verbindung zu vermeiden. Um den Status dieser Option zu überprüfen, öffnen Sie die Webkonsole, navigieren Sie zu **Netzwerkcomputer > Allgemeine Client-Einstellungen**, und wechseln Sie dann in den Abschnitt **Firewall-Einstellungen**. Die Option lautet **OfficeScan Firewall-Treiber erst nach einem Neustart des Systems aktualisieren**.

- Nach der Verteilung des Pakets ist auf dem Client-Computer noch die vorherige Version des OfficeScan TDI-Treibers vorhanden. Die neue Version wird erst beim Neustart des Computers geladen. Wird der Neustart des OfficeScan Clients nicht sofort ausgeführt, treten wahrscheinlich Probleme auf.

  Ist in der Webkonsole die Option zur Anzeige der Neustartbenachrichtigung aktiviert, wird der 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. Um den Status dieser Option zu überprüfen navigieren Sie auf der Webkonsole zu **Netzwerkcomputer > Allgemeine Client-Einstellungen**, und wechseln Sie dann in den Abschnitt **Warneinstellungen**. Die Option lautet **Eine Benachrichtigung anzeigen, wenn der Client-Computer zum Laden eines Kerneltreibers neu gestartet werden muss**.

2. Während ein Client das Anmeldeskript-Setup (AutoPcc.exe) ausführt, kann der OfficeScan Server nicht auf diese Version upgraden. Stellen Sie sicher, dass während der Installation dieses Patches kein Client das Anmeldeskript ausführt.

Die unbeaufsichtigte Installation besteht aus zwei Abläufen:

1. Erstellen Sie eine Antwortdatei, indem Sie das Setup ausführen und die Installationeinstellungen 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 (Erstinstallation oder Upgrade). Informationen über wichtige Fenster finden Sie unter *Die Setup-Installationsfenster* auf Seite 2-21.
- Wenn Sie ein Upgrade der OfficeScan Server auf diese Version planen, erstellen Sie die Antwortdatei auf einem Computer, auf dem ein OfficeScan Server installiert ist.
- Bei einer Erstinstallation hingegen erstellen Sie die Antwortdatei auf einem Computer 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.

Die Setup-Konfiguration in einer Antwortdatei aufzeichnen:

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

1. Öffnen Sie eine Befehlszeile, und geben Sie das Verzeichnis der Datei **setup.exe** für OfficeScan ein. Beispiel: CD C:fficeScan Installeretup.exe.
2. Geben Sie folgenden Befehl ein:

   ```
   setup.exe -r
   ```

   Der Parameter -r weist das Programm an, zu starten und die Installationsdetails in einer Antwortdatei aufzuzeichnen.
3. Führen Sie die Installationsschritte in Setup durch.
4. Prüfen Sie anschließend die Antwortdatei **setup.iss** im Verzeichnis %windir%.

Eine unbeaufsichtigte Installation durchführen:

1. Kopieren Sie das Installationspaket und die Datei **setup.iss** auf den Zielcomputer.
2. Öffnen Sie auf dem Zielcomputer die Eingabeaufforderung, 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.
   - **<-f1Pfad>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".
   - **<-f2Pfad>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 die **Eingabetaste**. Setup führt nun eine unbeaufsichtigte Installation des Servers auf dem Computer durch.
5. Überprüfen Sie die OfficeScan Programmverknüpfungen auf dem Zielcomputer, um festzustellen, ob die Installation ordnungsgemäß durchgeführt wurde. Falls keine Verknüpfungen erstellt wurden, führen Sie die Installation erneut durch.

Von einer Testversion upgraden

Bevor Ihre Testversion abläuft, zeigt OfficeScan eine Meldung im Fenster "Zusammenfassung" an. Über die Webkonsole können Sie ein Upgrade von einer Testversion auf die Vollversion von OfficeScan durchführen, ohne dass Ihre Konfigurationseinstellungen verloren gehen. Beim Erwerb einer Lizenz für eine Vollversion erhalten Sie entweder einen Registrierungsschlüssel oder einen Aktivierungscode.

Upgrade von einer Testversion durchführen:

1. Öffnen Sie die OfficeScan Webkonsole.
2. Klicken Sie auf **Administration > Produktlizenz**. Das Fenster "Produktlizenz" wird angezeigt.
3. Wenn Sie über einen Aktivierungscode verfügen, geben Sie ihn in das Feld **Neuer Aktivierungscode** ein, und klicken Sie auf **Speichern**.
4. Wenn Ihnen der Aktivierungscode nicht bekannt ist, klicken Sie auf **Online-Registrierung**, und fordern Sie den Aktivierungscode mit dem Registrierungsschlüssel an.

Die Setup-Installationsfenster

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

TABELLE 2-1. Installationsfenster und -aufgaben

FENSTER	LOKAL/ UNBEAUFSICHTIGTE ERSTINSTALLATION	REMOTE-ERSTINSTALLATION	LOKAL/ UNBEAUFSICHTIGTES UPGRADE	REMOTE-UPGRADE
Begrüßungsfenster	✓	✓	✓	✓
Lizenzvereinbarung	✓	✓	✓	✓
Client-Verteilung	✓	✓	✓	✓
OfficScan Servereinstellungen	✓	✓	✓	✓
Installationsziel	✓	✓	✓	✓
Virensuche vor der Installation	✓	✓	✓	✓
Setup-Status (Computeranalyse) **Hinweis:** Die Analyse kann einige Zeit in Anspruch nehmen, insbesondere während der Initialisierung der HTTP-Server.	✓		✓	

TABELLE 2-1. Installationsfenster und -aufgaben (Fortsetzung)

FENSTER	LOKAL/ UNBEAUFSICHTIGTE ERSTINSTALLATION	REMOTE-ERSTINSTALLATION	LOKAL/ UNBEAUFSICHTIGTES UPGRADE	REMOTE-UPGRADE
Installationspfad	✓	✓		✓
Proxy-Einstellungen	✓	✓		✓
Webserver-Einstellungen	✓	✓		✓
Identifizierung des Server-Computers	✓	✓		✓
Registrierung und Aktivierung	✓	✓	✓	✓
Installation des integrierten Smart Protection Servers	✓	✓	✓	✓
Web-Reputation-Dienste aktivieren	✓	✓	✓	✓
Ziel der Remote-Installation		✓		✓
Analyse des Zielcomputers		✓		✓
OfficeScan Programme	✓	✓		✓
Installation/Upgrade des Cisco Trust Agent	✓			
Cisco Trust Agent Lizenzvereinbarung	✓			

TABELLE 2-1. Installationsfenster und -aufgaben (Fortsetzung)

FENSTER	LOKAL/ UNBEAUFSICHTIGTE ERSTINSTALLATION	REMOTE-ERSTINSTALLATION	LOKAL/ UNBEAUFSICHTIGTES UPGRADE	REMOTE-UPGRADE
Trend Micro Smart Protection Network	✓	✓		
Kennwort für das Administratorkonto	✓	✓		
Client-Installationspfad	✓	✓		
Antiviren-Funktionen	✓	✓		
Anti-Spyware-Funktion Wird ein lokales Upgrade durchgeführt, wird dieses Fenster nicht angezeigt, falls zuvor die Lizenz für Web Reputation und Anti-Spyware aktiviert wurde.	✓	✓	✓	✓
Web-Reputation-Richtlinie	✓	✓	✓	✓
Verknüpfung mit Programmordner	✓			
Installationsdaten	✓	✓	✓	✓
Installation des OfficeScan Servers	✓	✓	✓	✓
Installation des Policy Servers	✓			
Abschluss der Installation von OfficeScan Server	✓	✓	✓	✓

Lizenzvereinbarung

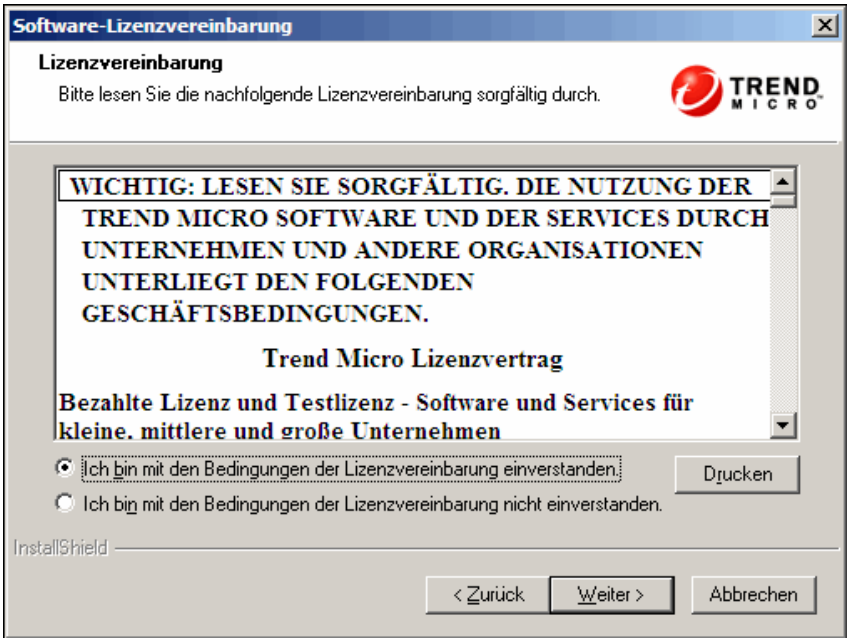


ABBILDUNG 2-1. Fenster "Lizenzvereinbarung"

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.

Client-Verteilung

ABBILDUNG 2-2. Fenster "Client-Verteilung"

Es gibt mehrere Methoden, um OfficeScan Clients zu installieren oder zu aktualisieren. In diesem Fenster wird eine Liste der verschiedenen Verteilungsmethoden und der ungefähr erforderlichen Netzwerkbandbreite angezeigt. Diese Angaben ändern sich, wenn der OfficeScan Server aktualisiert wird, weil die momentan auf dem Server verfügbaren OfficeScan Komponenten im Client-Installationspaket enthalten sind.

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

Hinweis: Für alle Installationsmethoden sind lokale Administratorrechte auf den Zielcomputern erforderlich.

OfficScan Servereinstellungen

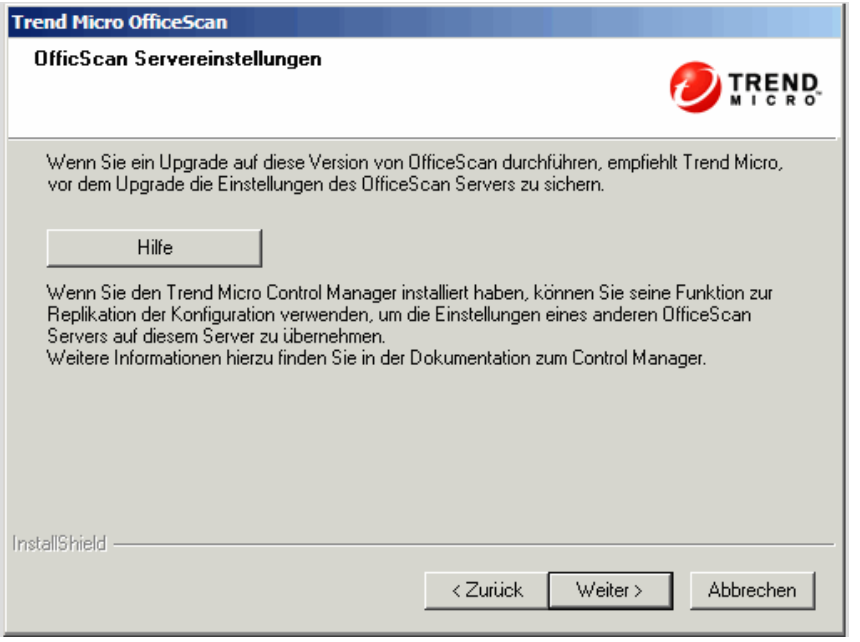


ABBILDUNG 2-3. Das Fenster "OfficeScan Servereinstellungen"

Wenn Sie ein Upgrade auf diese Version von OfficeScan durchführen, empfiehlt Trend Micro, vor dem Upgrade die OfficeScan Datenbank von der OfficeScan Webkonsole aus zu sichern. In der OfficeScan Serverdatenbank sind alle OfficeScan Einstellungen, einschließlich Sucheinstellungen und Berechtigungen, gespeichert. Beim Sichern der Datenbank wird diese von OfficeScan automatisch defragmentiert und eventuelle Schäden an der Index-Datei werden repariert.

Verwenden Sie kein anderes Tool oder keine andere Anwendung zur Datenbanksicherung. Weitere Informationen zur Sicherung der Datenbank finden Sie unter Einstellungen und Konfigurationen von OfficeScan (auf Seite 1-13).

Trend Micro Control Manager eignet sich außerdem zum Sichern und Replizieren der Servereinstellungen. Mit Hilfe dieser Servereinstellungen können Sie entweder den OfficeScan Server wiederherstellen, wenn es während der Aktualisierungen zu Problemen kommt, oder die Servereinstellungen auf einen anderen OfficeScan Server kopieren. Weitere Informationen finden Sie im *Administratorhandbuch für Trend Micro Control Manager*.

Installationsziel

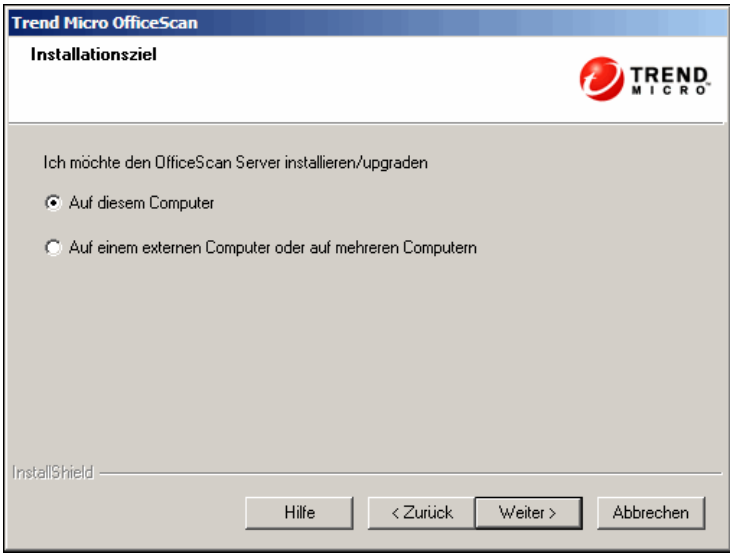


ABBILDUNG 2-4. Das Fenster "Installationsziel"

Führen Sie Setup aus, und installieren Sie den OfficeScan Server entweder auf dem Computer, auf dem Setup ausgeführt wird, oder auf anderen Computern im Netzwerk. Wenn Setup auf dem Zielcomputer eine Vorgängerversion von OfficeScan entdeckt, werden Sie zum Upgrade aufgefordert. Nur die folgenden Versionen von OfficeScan können auf diese Version upgraden:

- 10.5 Patch 1
- 10.5
- 10.0 Service Pack 1
- 10.0
- 8.0 Service Pack 1

Remote-Installations-/Upgrade-Hinweise

Bei diesem Vorgang prüft Setup, ob der Zielcomputer die Voraussetzungen für die Installation oder das Upgrade des Servers erfüllt. Bevor Sie den Vorgang fortsetzen:

- Stellen Sie sicher, dass Sie auf dem Zielcomputer über Administratorrechte verfügen.
- Notieren Sie den Host-Namen des Computers und die Anmeldedaten (Benutzername und Kennwort).
- Prüfen Sie, ob die Zielcomputer die Systemvoraussetzungen für die Installation des OfficeScan Servers erfüllen.
- Stellen Sie sicher, dass auf dem Computer Microsoft IIS Server 5.0 oder höher installiert ist, wenn er als Webserver eingesetzt wird. Wenn Sie sich für den Apache Webserver entscheiden, installiert Setup diesen automatisch, falls er noch nicht auf dem Zielcomputer vorhanden ist.

Bei einem lokalen Upgrade behält OfficeScan die Einstellungen der früheren Installation (inkl. Servername, Proxy-Server-Daten und Portnummern) bei. Diese Einstellungen können während des Upgrades nicht verändert werden. Ändern Sie die Einstellungen nach dem Upgrade über die OfficeScan Webkonsole.

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.

Virensuche vor der Installation

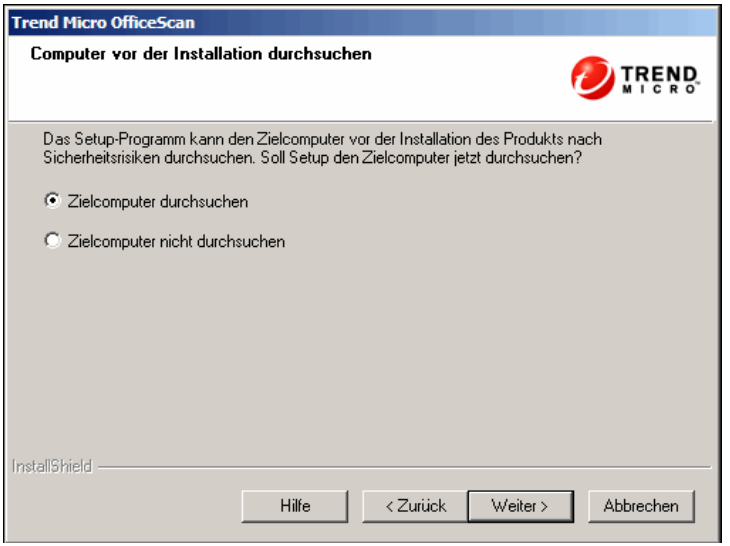


ABBILDUNG 2-5. Das Fenster "Computer vor der Installation durchsuchen"

Vor der Installation von OfficeScan Server kann Setup den Zielcomputer nach Sicherheitsrisiken durchsuchen. Setup durchsucht die anfälligsten Bereiche des Computers, wie beispielsweise folgende:

- 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.

Installationspfad

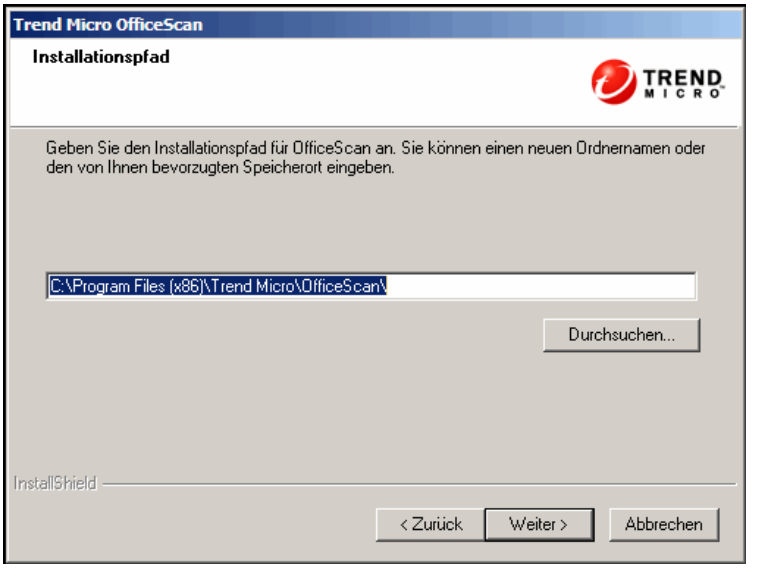


ABBILDUNG 2-6. Das Fenster "Installationspfad"

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

Der Installationspfad, den Sie angeben, wird nur bei einer remote durchgeführten Erstinstallation angewendet. Bei einem remote durchgeführten Upgrade verwendet OfficeScan die Einstellungen aus der früheren Version.

Proxy-Einstellungen

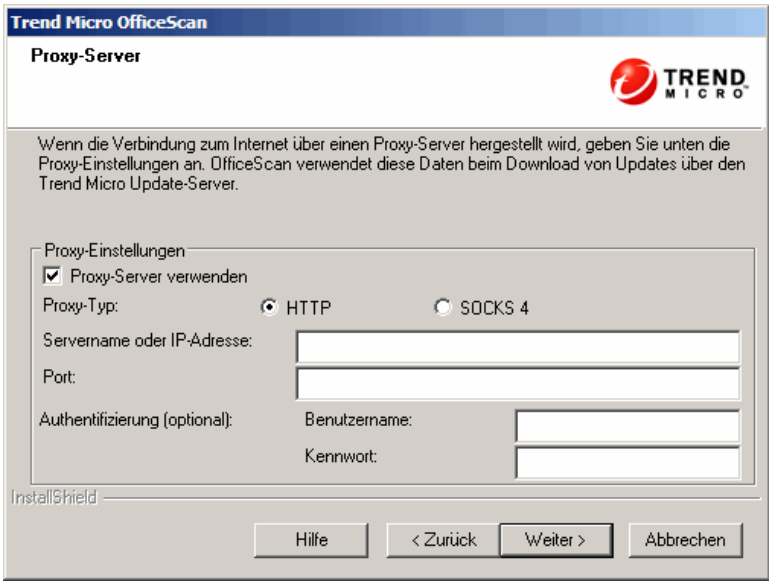


ABBILDUNG 2-7. Das Fenster "Proxy-Server"

Der OfficeScan Server verwendet für die Kommunikation zwischen Client 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 Download von Updates vom ActiveUpdate Server.

Die Proxy-Einstellungen können Sie 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.

IPv6-Unterstützung

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

Webserver-Einstellungen

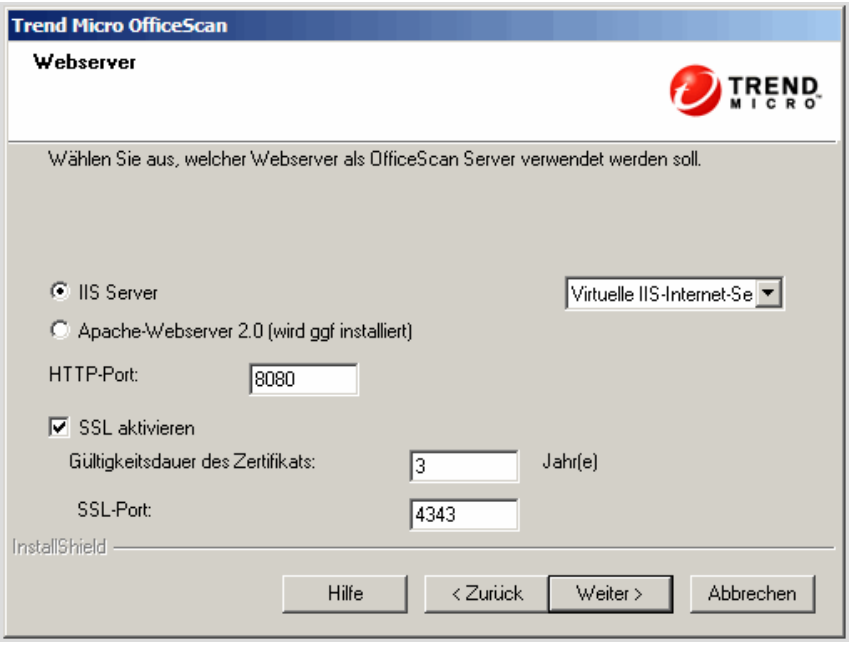


ABBILDUNG 2-8. Das Fenster "Webserver"

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

Die Webserver-Einstellungen betreffen nur eine Remote-Erstinstallation. Wenn Sie ein Remote-Upgrade durchführen, verwendet OfficeScan die Einstellungen aus der Vorgängerversion.

IPv6-Unterstützung

Wählen Sie für Neuinstallationen den IIS-Server zum Aktivieren der IPv6-Unterstützung. Der Apache Webserver unterstützt keine IPv6-Adressierung. Wenn der Zielcomputer nur eine IPv6-Adresse hat und Sie Apache wählen, wird die Installation nicht fortgesetzt. Wenn der Zielcomputer sowohl eine IPv6- als auch IPv4-Adresse hat, können Sie Apache wählen. In diesem Fall wird jedoch die IPv6-Unterstützung nach der Installation des Servers nicht aktiviert.

Wenn Sie ein Upgrade dieser OfficeScan Version durchführen, muss der zu aktualisierende OfficeScan Server bereits IIS verwenden. Wenn der Server Apache verwendet, konfigurieren Sie diesen vor dem Upgrade für die Verwendung von IIS.

Webserver

Erkennt Setup auf dem Zielcomputer sowohl IIS als auch Apache Webserver, können Sie einen der beiden Webserver auswählen. Ist keiner der beiden Webserver auf dem Zielcomputer vorhanden, können Sie IIS nicht auswählen. OfficeScan installiert automatisch den Apache Webserver 2.0.63.

Bei Verwendung des Apache Webservers:

- Apache Webserver 2.0.x ist erforderlich. Falls Apache Webserver auf Ihrem Computer installiert ist, aber nicht die Version 2.0.x hat, installiert OfficeScan Version 2.0.63 und verwendet diese. Die vorhandene Version von Apache Webserver wird nicht entfernt.
- Bei aktiviertem SSL und vorhandenem Apache Webserver 2.0.x müssen beim Apache Webserver die SSL-Einstellungen vorkonfiguriert sein.
- Standardmäßig wird auf dem Apache-Webserver als einziges Konto das Administratorkonto erstellt.

  Tipp: Erstellen Sie ein anderes Konto, über das der Webserver ausgeführt wird. Ansonsten wäre die Sicherheit des OfficeScan Servers gefährdet, wenn ein Hacker die Kontrolle über den Apache Server übernimmt.

- Weitere Informationen über Upgrades, Patches und Sicherheitsfragen vor der Installation des Apache Webservers finden Sie auf der Apache Website.

Bei Verwendung des IIS Webservers:

- Die folgenden Versionen von Microsoft Internet Information Server (IIS) sind erforderlich:
  - Version 6.0 unter Windows Server 2003
  - Version 7.0 unter Windows Server 2008
  - Version 7.5 unter Windows Server 2008 R2
- Der Webserver sollte auf keinem Computer 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 horcht auf dem HTTP-Port nach Client-Anfragen und leitet diese an den OfficeScan Master Service weiter. Dieser Dienst sendet über den festgelegten Kommunikationsport Informationen an die Clients. Setup erzeugt bei der Installation eine zufällige Portnummer für die Client-Kommunikation.

SSL-Unterstützung

Aktivieren Sie SSL (Secure Sockets Layer) für eine sichere Kommunikation zwischen dem Server und der Webkonsole. SSL bietet eine zusätzliche Schutzebene vor Hacker-Angriffen. Obwohl OfficeScan die auf der Webkonsole festgelegten Kennwörter vor dem Versenden an den OfficeScan Server verschlüsselt, können Hacker das Paket auskundschaften und 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 verschüsselt.

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)
Apache Webserver mit aktiviertem SSL	8080 (configurable)	4343 (configurable)
Apache Webserver mit deaktiviertem SSL	8080 (configurable)	n. v.
IIS Standard-Website mit aktiviertem SSL	80 (not configurable)	443 (not configurable)
IIS Standard-Website mit deaktiviertem SSL	80 (not configurable)	n. v.
IIS virtuelle Website mit aktiviertem SSL	8080 (configurable)	4343 (configurable)
IIS virtuelle Website mit deaktiviertem SSL	8080 (configurable)	n. v.

Identifizierung des Server-Computers

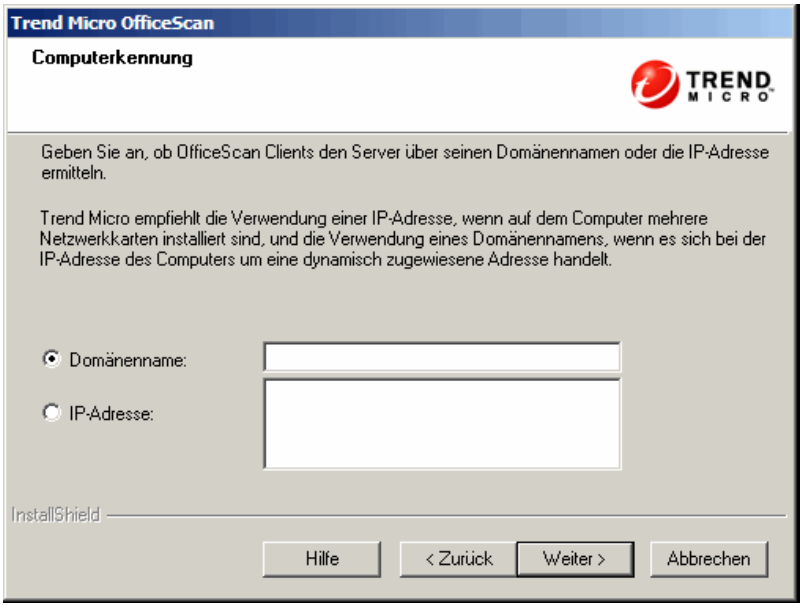


ABBILDUNG 2-9. Das Fenster "Computerkennung"

Die in diesem Fenster gewählte Option betrifft nur eine remote durchgeführte Erstinstallation. Bei remote durchgeführten Upgrades verwendet OfficeScan die Einstellungen aus der früheren Version.

Legen Sie fest, ob OfficeScan Clients den Server über ihren Hostnamen (Domäne) oder die IP-Adresse identifizieren.

Wird der Server-Computer über die IP-Adresse identifiziert, wird bei einer Änderung dieser IP-Adresse die Kommunikation zwischen dem OfficeScan Server und den Clients unterbrochen. Die Verbindung kann dann nur durch eine erneute Verteilung aller Clients wiederhergestellt werden. Dasselbe gilt für den Fall, dass der Server-Computer über einen Hostnamen ermittelt und dieser Hostname 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. Die IP-Adresse sollte ebenfalls nicht geändert werden, wenn OfficeScan diese von einem DHCP-Server empfängt.

Wenn Sie statische IP-Adressen verwenden, identifizieren Sie den Server über seine IP-Adresse. Sind außerdem mehrere Netzwerk-Schnittstellenkarten (NICs) auf dem Server-Computer vorhanden, sollte anstelle des Hostnamens eine entsprechende IP-Adresse verwendet werden, um sicherzustellen, dass die Client/Server-Verbindung hergestellt werden kann.

IPv6-Unterstützung

Wenn der Server IPv4- und IPv6-Clients verwaltet, muss er eine IPv4- wie auch eine IPv6-Adresse haben und über seinen Hostnamen identifiziert werden. Wenn der Server über seine IPv4-Adresse identifiziert wird, können IPv6-Clients keine Verbindung zum Server herstellen. Dasselbe Problem tritt auf, wenn reine IPv4-Clients eine Verbindung mit einem Server herstellen, der über seine IPv6-Adresse identifiziert wird.

Wenn der Server nur IPv6-Clients 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.

Registrierung und Aktivierung

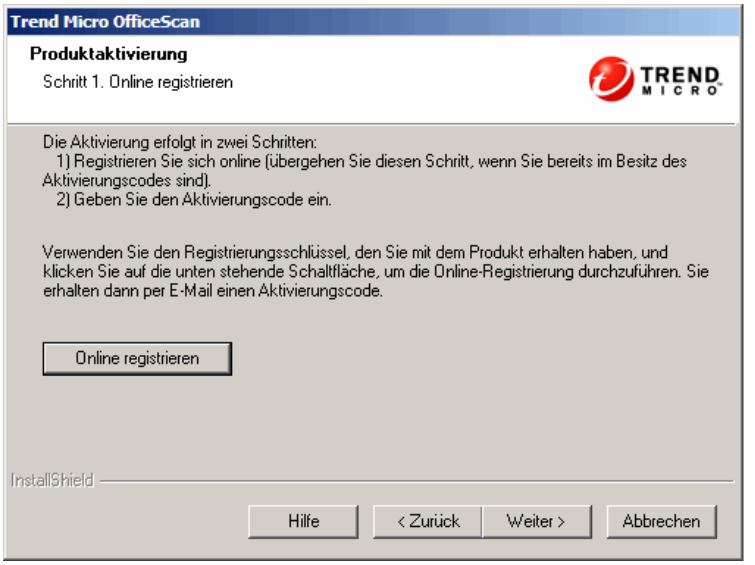


ABBILDUNG 2-10. Fenster "Produktregistrierung"

Registrieren Sie OfficeScan über den Registrierungsschlüssel, den Sie mit dem Produkt erhalten haben. Der Aktivierungscode wird Ihnen anschließend zugesendet. Falls Sie die Registrierung bereits durchgeführt und den Aktivierungscode erhalten haben, können Sie diesen Schritt überspringen.

Wenn Sie nicht über die Aktivierungscodes verfügen, klicken Sie auf **Online registrieren**. Setup leitet Sie dann an die Registrierungsseite von Trend Micro weiter. Nach Abschluss der Registrierung erhalten Sie von Trend Micro eine E-Mail mit den Aktivierungscodes. Sie können den Installationsvorgang dann fortsetzen.

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

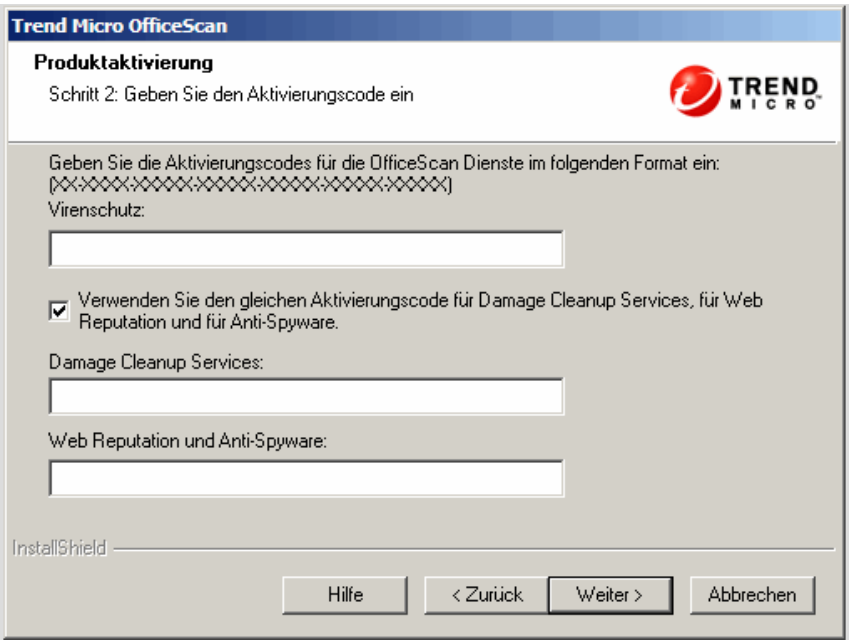


ABBILDUNG 2-11. Das Fenster "Produktaktivierung"

Wenn Sie bereits über Aktivierungscodes verfügen, können Sie diese eingeben und die Installation fortsetzen. Achten Sie bei der Eingabe auf Groß- und Kleinschreibung.

Wenn Sie einen Aktivierungscode erhalten haben, der für alle Dienste gültig ist:

1. Wählen Sie **Verwenden Sie den gleichen Aktivierungscode für Damage Cleanup Services, für Web Reputation und für Anti-Spyware** aus.
2. Geben Sie im Textfeld **Antivirus** den Aktivierungscode ein.

Installation des integrierten Smart Protection Servers

ABBILDUNG 2-12. Fenster für die Installation des integrierten Smart Protection Servers

Das Setup kann den integrierten Smart Protection Server auf dem Zielcomputer installieren. Der integrierte Server bietet File-Reputation-Dienste für Clients mit intelligenter Suche sowie Web-Reputation-Dienste für Clients, die den Web-Reputation-Richtlinien unterliegen. Der integrierte Server wird von der OfficeScan Webkonsole aus verwaltet.

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

Tipp: Weil der integrierte Smart Protection Server und der OfficeScan Server auf demselben Computer ausgeführt werden können, kann die Computerleistung bei sehr hohem Datenaufkommen für die beiden Server signifikant beeinträchtigt werden. Um den Datenverkehr zum OfficeScan Server-Computer zu reduzieren, ordnen Sie einen eigenständigen Smart Protection Server als primäre Smart Protection Quelle und den integrierten Server als eine Backup-Quelle zu. Weitere Informationen zum Konfigurieren von Smart Protection Quellen für Clients finden Sie im *Administratorhandbuch*.

Lizenzen

Aktivieren Sie die Lizenzen für die folgenden Dienste, um die intelligente Suche zu verwenden:

- Virenschutz
- Web Reputation und Anti-Spyware

Weitere Informationen zu OfficeScan Lizenzen finden Sie unter *Registrierung und Aktivierung* auf Seite 2-39.

Wenn Sie die Lizenzen nicht aktivieren, können Sie dennoch den integrierten Smart Protection Server installieren, doch die Clients können dann weder die intelligente Suche nutzen noch eine Verbindung mit einem Smart Protection Server aufbauen. Zu Lizenz- und Aktivierungsfragen wenden Sie sich an Ihren Trend Micro Vertriebspartner.

Client-Verbindungsprotokolle für File-Reputation-Dienste

Clients können sich mit den File-Reputation-Diensten des integrierten Smart Protection Servers über die Protokolle HTTP bzw. HTTPS verbinden. HTTPS ermöglicht eine sicherere Verbindung, während HTTP weniger Bandbreite benötigt.

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

Die Portnummern für File-Reputation-Dienste richten sich nach dem Webserver, den Sie für den OfficeScan Server verwenden möchten (Apache oder IIS). Weitere Informationen finden Sie unter *Webserver-Einstellungen* auf Seite 2-33.

The HTTP-Port wird im Installationsfenster nicht angezeigt. Der HTTPS-Port wird angezeigt und kann möglicherweise konfiguriert werden.

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)
Apache Webserver mit aktiviertem SSL	8080	4343
Apache Webserver mit deaktiviertem SSL	8080	4345 (configurable)
IIS Standard-Website mit aktiviertem SSL	8082	443 (not configurable)
IIS Standard-Website mit deaktiviertem SSL	8082	443 (not configurable)
IIS virtuelle Website mit aktiviertem SSL	8082	4345 (configurable)
IIS virtuelle Website mit deaktiviertem SSL	8082	4345 (configurable)

Integrierter Server nicht installiert

Wenn Sie eine Erstinstallation oder ein Upgrade von OfficeScan 8.0 SP1 durchführen und ausgewählt haben, den integrierten Server nicht zu installieren:

- Die herkömmliche Suche wird die standardmäßige Suchmethode.
- Wenn Sie sich dafür entscheiden, die Web-Reputation-Richtlinien in einem separaten Installationsfenster zu aktivieren (ausführliche Hinweise finden Sie unter *Web-Reputation-Richtlinie* auf Seite 2-62), können Clients keine Web-Reputation-Abfragen senden, da angenommen wird, dass kein Smart Protection Server installiert ist.

Falls ein eigenständiger Server nach der Installation oder dem Upgrade 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 in der Liste der Smart Protection Quelle hinzu, sodass Clients Datei- und Web-Reputation-Abfragen an den Server senden können.

Wenn Sie ein Upgrade von einem OfficeScan Server der Version 10.x durchführen, wobei der integrierte Server deaktiviert wurde, wird der integrierte Server nicht installiert. Clients behalten ihre Suchmethoden und die Smart Protection Quellen, an die sie Abfragen senden, bei.

Web-Reputation-Dienste aktivieren

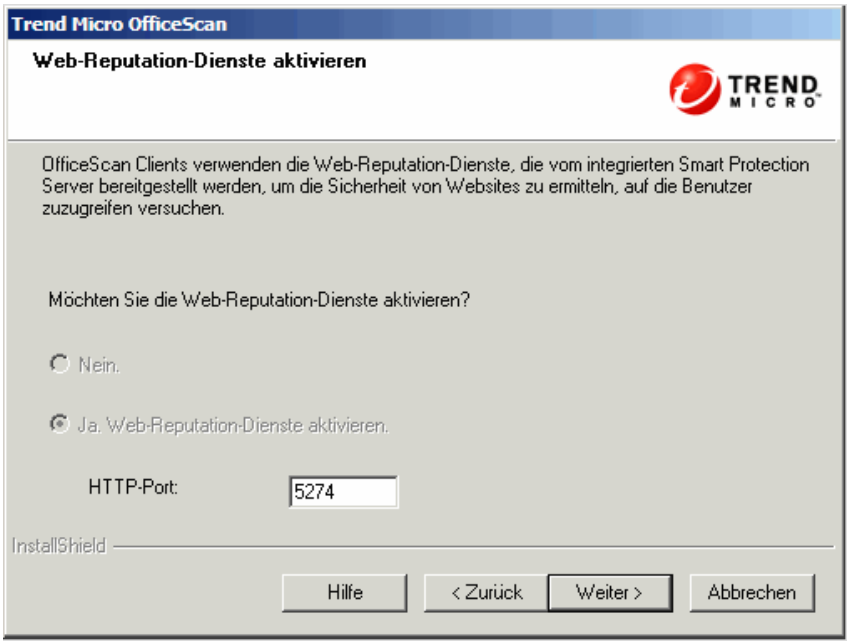


ABBILDUNG 2-13. Das Fenster "Web-Reputation-Dienst aktivieren"

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. Diese 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 Clients Web-Reputation-Daten von einem lokalen Server beziehen, anstatt eine Verbindung zum Smart Protection Network herzustellen.

Client-Verbindungsprotokolle für Web-Reputation-Dienste

Clients können sich mit den Web-Reputation-Diensten des integrierten Smart Protection Servers über die Protokolle HTTP bzw. HTTPS verbinden.

Die HTTP-Portnummer für Web-Reputation-Dienste richtet sich nach dem Webserver, den Sie für den OfficeScan Server verwenden möchten (Apache oder IIS). Weitere Informationen finden Sie unter *Webserver-Einstellungen* auf Seite 2-33.

TABELLE 2-4. Ports für die Web-Reputation-Dienste des integrierten Smart Protection Servers

WEBSERVER UND EINSTELLUNGEN	HTTP-PORT FÜR WEB-REPUTATION-DIENSTE
Apache Webserver mit aktiviertem SSL	8080 (not configurable)
Apache Webserver mit deaktiviertem SSL	8080 (not configurable)
IIS Standard-Website mit aktiviertem SSL	80 (not configurable)
IIS Standard-Website mit deaktiviertem SSL	80 (not configurable)
IIS virtuelle Website mit aktiviertem SSL	5274 (configurable)
IIS virtuelle Website mit deaktiviertem SSL	5274 (configurable)

Ziel der Remote-Installation

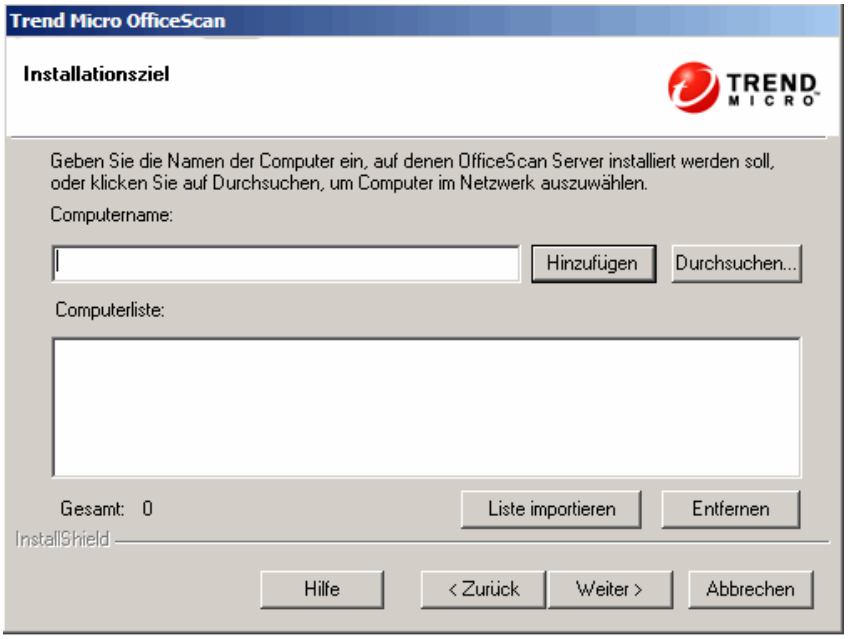


ABBILDUNG 2-14. Das Fenster für das Ziel der Remote-Installation

Geben Sie den Zielcomputer an, auf dem OfficeScan installiert wird. Geben Sie den Host-Namen oder die IP-Adresse des Computers ein. Klicken Sie auf **Durchsuchen**, um nach Computern im Netzwerk zu suchen.

Sie können die Computernamen auch aus einer Textdatei importieren. Klicken Sie hierzu auf **Liste importieren**. Bei der gleichzeitigen Installation von OfficeScan Server auf mehreren gültigen Computer, erfolgt die Installation nach deren Reihenfolge in der Textdatei.

In der Textdatei:

- Tragen Sie pro Zeile einen Computernamen ein.
- Verwenden Sie das UNC- (Unified Naming Convention) Format (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

\\domain3\test.xyz

Hinweise zur Durchführung der Remote-Installation:

- Stellen Sie sicher, dass Sie auf dem Zielcomputer über Administratorrechte verfügen.
- Notieren Sie den Host-Namen des Computers und die Anmeldedaten (Benutzername und Kennwort).
- Prüfen Sie, ob die Zielcomputer die Systemvoraussetzungen für die Installation des OfficeScan Servers erfüllen.
- Stellen Sie sicher, dass auf dem Computer Microsoft IIS Server 5.0 oder höher installiert ist, wenn er als Webserver eingesetzt wird. Wenn Sie sich für den Apache Webserver entscheiden, installiert Setup diesen automatisch, falls er noch nicht auf dem Zielcomputer vorhanden ist.
- Der Computer, auf dem Setup ausgeführt wird, darf nicht als Zielcomputer angegeben werden. Starten Sie stattdessen die lokale Installation auf dem Computer.

Klicken Sie nach der Angabe der Zielcomputer auf **Weiter**. Setup überprüft, ob die Computer die OfficeScan Installationsvoraussetzungen erfüllen.

Analyse des Zielcomputers

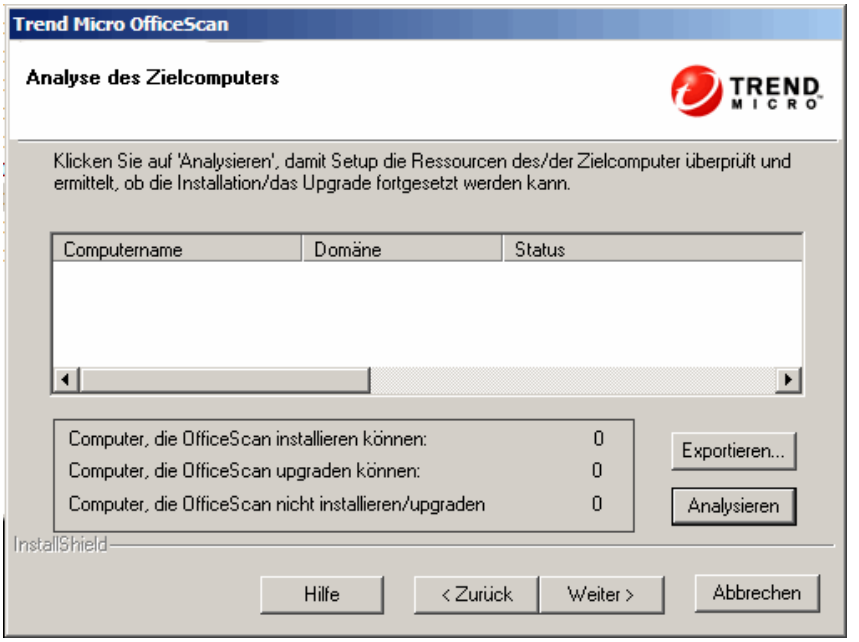


ABBILDUNG 2-15. Das Fenster "Analyse des Zielcomputers"

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

Bei der Installation auf mehreren Computern wird die Installation fortgesetzt, wenn mindestens einer der Computer die Voraussetzungen erfüllt. Setup installiert den OfficeScan Server auf diesem Computer und ignoriert Computer mit negativem Ergebnis.

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

OfficeScan Programme

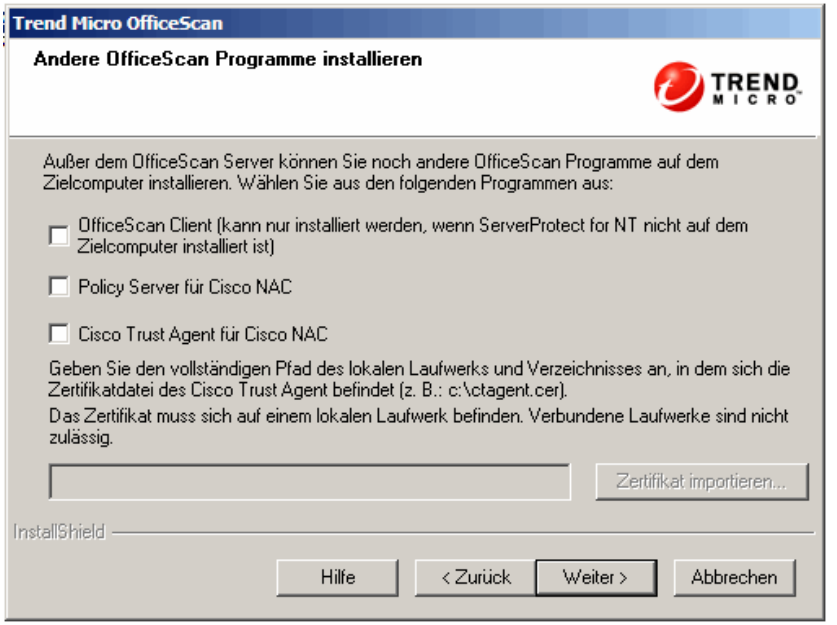


ABBILDUNG 2-16. Das Fenster für die Installation der OfficeScan Programme

Die folgenden OfficeScan Programme stehen bei der Installation zur Auswahl:

- OfficeScan Client
- Policy Server für Cisco NAC
- Cisco Trust Agent

Hinweis: Wenn Sie den OfficeScan Server auf einem reinen IPv6-Computer installieren, dürfen Sie nicht den Policy Server für Cisco NAC und Cisco Trust Agent installieren. Diese Programme unterstützen keine IPv6-Adressierung.

OfficeScan Client

Das Client-Programm dient dem Schutz vor Sicherheitsrisiken Der Computer, auf dem der OfficeScan Server installiert ist, benötigt deshalb zu seinem Schutz auch das Client-Programm. Der Schutz des Servers ist automatisch gewährleistet, wenn Sie den Client zusammen mit dem Server installieren. Dadurch sparen Sie sich die zusätzliche Aufgabe, den Client nach dem Server zu installieren.

Hinweis: Installieren Sie den Client nach der Installation des Servers auf anderen Computern im Netzwerk. Weitere Informationen zu den Client-Installationsmethoden finden Sie im *Administratorhandbuch*.

Wenn Sie ein Upgrade von OfficeScan durchführen, wird dieses Fenster nicht angezeigt.

Ist eine Endpunkt-Sicherheitssoftware von Trend Micro oder Drittanbietern auf dem Server-Computer installiert, kann OfficeScan diese Software möglicherweise nicht automatisch deinstallieren und durch den OfficeScan Client ersetzen. Eine Liste der Programme, die OfficeScan automatisch deinstalliert, erhalten Sie von Ihrem Support-Anbieter. Software, die nicht automatisch deinstalliert werden kann, müssen Sie manuell deinstallieren, bevor die Installation von OfficeScan fortgesetzt werden kann.

Cisco Network Admission Control (NAC) Programme

Der Schwerpunkt von Cisco NAC liegt in der Durchsetzung von Zugriffsrechten und Antiviren- und Sicherheitsrichtlinien zur Kontrolle von Sicherheitsrisiken innerhalb des Netzwerks. Dadurch können Client-Computer über das Netzwerk Informationen über Sicherheitsprobleme austauschen.

Ebenso wie OfficeScan besteht auch Cisco NAC aus einer Server- (Policy Server for Cisco NAC) und einer Client-Komponente (Cisco Trust Agent, CTA). Cisco NAC wird zusammen mit den entsprechenden Cisco-Routern verwendet und benötigt eine Verbindung zum Cisco Admission Control Server (ACS).

Hinweis: Cisco NAC-Programme sind nicht verfügbar, wenn Sie den Antivirus-Service nicht aktivieren.

Den Policy Server oder CTA können Sie nicht installieren und kein Upgrade durchführen, wenn Sie eine Server-Installation remote vornehmen. Nach der Remote-Installation können Sie den CTA über die OfficeScan Webkonsole auf den Clients installieren. Der Policy Server wird über den Policy Server Installer im OfficeScan Setup-Paket installiert. Weitere Informationen zu Cisco NAC finden Sie im *Administratorhandbuch*.

Policy Server für Cisco NAC

Ebenso wie die OfficeScan Webkonsole ist der Policy Server für Cisco NAC eine webbasierte Konsole, auf der die Richtlinien für den Zugriff auf das Netzwerk konfiguriert werden. Der Policy Server überprüft ständig, ob der Client über aktuelle Scan Engines und Pattern verfügt.

OfficeScan Server und Policy Server können entweder auf demselben Computer und über dieselbe Standard-Website oder auf zwei verschiedenen Computern installiert werden. Bei der Installation auf demselben Computer kann Setup beide Komponenten gleichzeitig während der Server-Installation installieren. Der Policy Server kann auch zu einem späteren Zeitpunkt installiert werden. Bei der Installation des Policy Servers auf einem anderen Computer führen Sie den Policy Server Installer auf diesem Computer aus.

Sie können über das OfficeScan Setup-Paket auf den Policy Server Installer zugreifen.

Cisco Trust Agent (CTA) für Cisco NAC

CTA ist ein Programm, das über den OfficeScan Server ausgeführt und auf Clients installiert wird. Dadurch kann der OfficeScan Client Antiviren-Informationen an den Cisco ACS berichten.

Bei Auswahl dieser Option während der Server-Installation installiert der OfficeScan Server CTA automatisch auf allen Clients, die der Server verwaltet. In nächsten Fenster fordert Setup Sie zur Auswahl von Cisco Trust Agent oder Cisco Trust Agent Supplicant auf. Der einzige Unterschied zwischen den beiden Versionen besteht darin, dass das Supplicant-Paket in der Sicherungsschicht (Ebene 2) die Authentifizierung für den Computer und den Endbenutzer erfordert.

Wenn Sie diese Option nicht wählen, können Sie den CTA dennoch über die Webkonsole auf den Clients installieren (**Cisco NAC > Agent Deployment**). Bei jedem neuen Client, der zum Server hinzugefügt wird, muss dieser Vorgang jedoch wiederholt werden. Weitere Informationen zur Installation von CTA über die Webkonsole finden Sie in der *OfficeScan Server-Hilfe*.

Die CTA-Installation erfordert eine Zertifikatsdatei (.cer), über die CTA eine verschlüsselte Kommunikationssitzung mit dem Cisco ACS aufbauen kann. Diese Zertifikatsdatei wird von einem CA- (Certificate Authority) Server erzeugt. Die Zertifikatsdatei erhalten Sie von Ihrem Trend Micro Vertriebspartner. Sie geben das Zertifikat während der Server-Installation oder über die Webkonsole ein (**Cisco NAC > Client-Zertifikat**).

Installation/Upgrade des Cisco Trust Agent

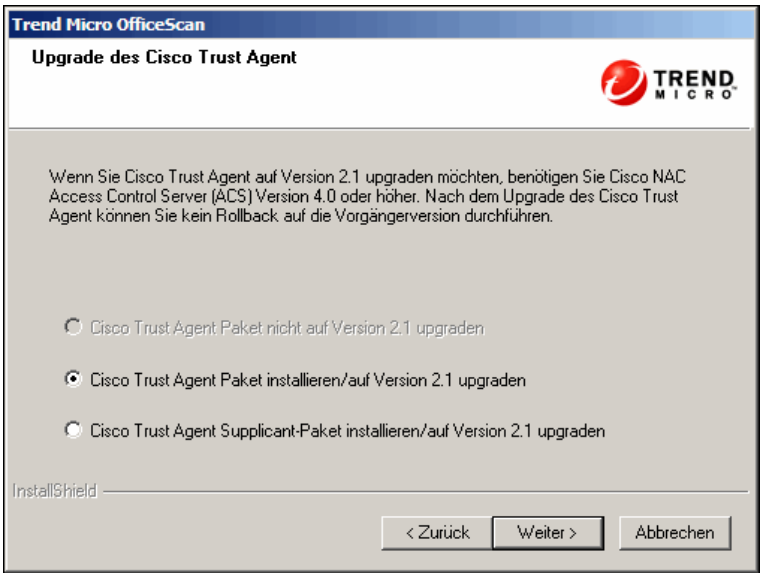


ABBILDUNG 2-17. Das Fenster "Upgrade des Cisco Trust Agent"

Bei der Erstinstallation wird dieses Fenster nur dann angezeigt, wenn Sie im vorherigen Fenster die Installation des Cisco Trust Agent ausgewählt haben. Wählen Sie das CTA-Paket aus, das auf den Clients installiert werden soll.

Bei einem Upgrade wird dieses Fenster nur dann angezeigt, wenn CTA zuvor installiert wurde. Geben Sie an, ob der CTA auf die aktuelle Version (2.1) upgegradet werden soll. Wählen Sie bei einem Upgrade das CTA-Upgrade-Paket aus.

Wenn Sie bei der Installation des Servers nicht angegeben haben, dass der CTA installiert werden soll, können Sie ihn auch über die Webkonsole installieren.

Cisco Trust Agent Lizenzvereinbarung

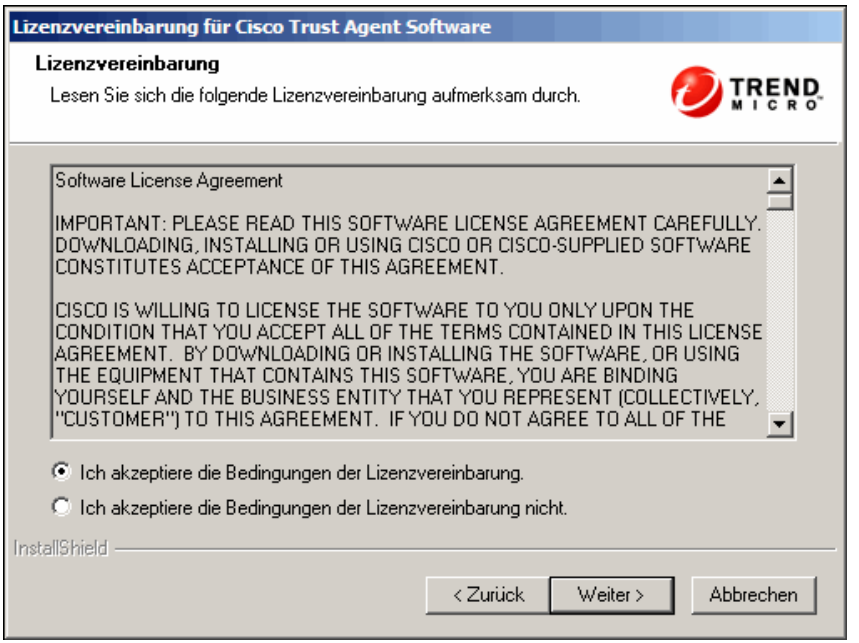


ABBILDUNG 2-18. Das Fenster "Lizenzvereinbarung für Cisco Trust Agent Software"

Lesen Sie die Lizenzvereinbarung aufmerksam durch, und stimmen Sie den Bedingungen der Lizenzvereinbarung zu, um die Installation fortzusetzen.

Trend Micro Smart Protection Network

Das Trend Micro™ Smart Protection Network ist eine Content-Sicherheitsinfrastruktur mit webbasiertem Client der nächsten Generation, die zum Schutz der Kunden vor Sicherheitsrisiken und Internet-Bedrohungen entwickelt wurde. Es unterstützt sowohl lokale als auch gehostete Lösungen, um Benutzer kontinuierlich zu schützen, unabhängig davon, ob sie sich im Netzwerk, zu Hause oder unterwegs befinden. Dazu werden schlanke Clients eingesetzt, um auf eine einzigartige, webbasierte Kombination von E-Mail-, File- und Web-Reputation-Technologien und Bedrohungsdatenbanken zuzugreifen. 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.

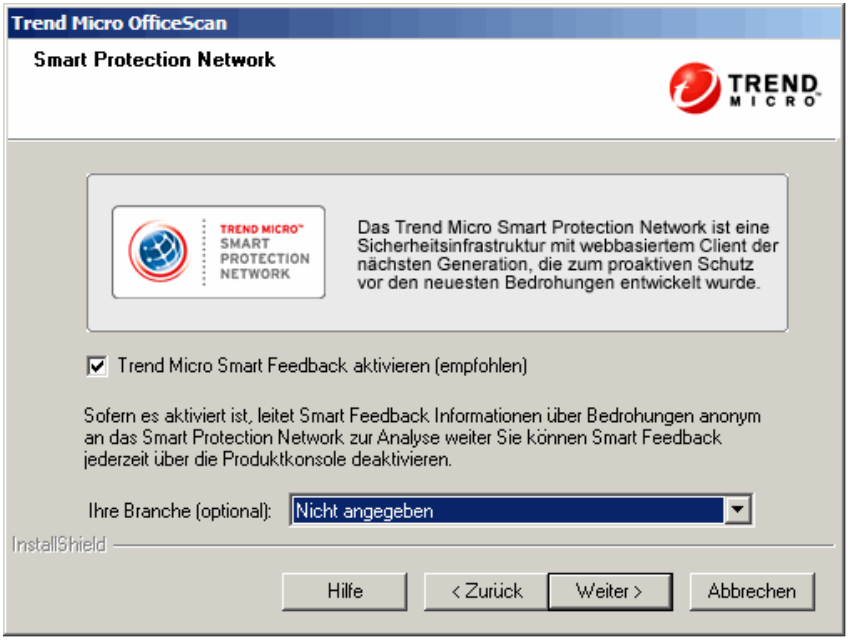


ABBILDUNG 2-19. Das Fenster "Smart Protection Network"

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 einzelnen 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. Beispiel: Routinemäßiges Senden von Reputationsprüfungen an das Trend Micro Smart Protection Network. 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. Der Datenschutz der Personal- oder Geschäftsdaten eines Kunden ist jederzeit gewährleistet, weil die gesammelten Bedrohungsdaten auf der Reputation der Kommunikationsquelle basieren.

Trend Micro Smart Feedback sammelt relevante Daten von den Trend Micro Smart Protection Servern der Clients und überträgt sie an die Trend Micro Back-End-Server. Diese Daten werden zur weiteren Analyse verwendet, was zu verbesserten und weiterentwickelteren Lösungen führen kann, die zum Schutz von Trend Micro Kunden verteilt werden können.

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

Weitere Informationen zum Smart Protection Network finden Sie unter:

http://de.trendmicro.com/de/technology/smart-protection-network/

Kennwort für das Administratorkonto

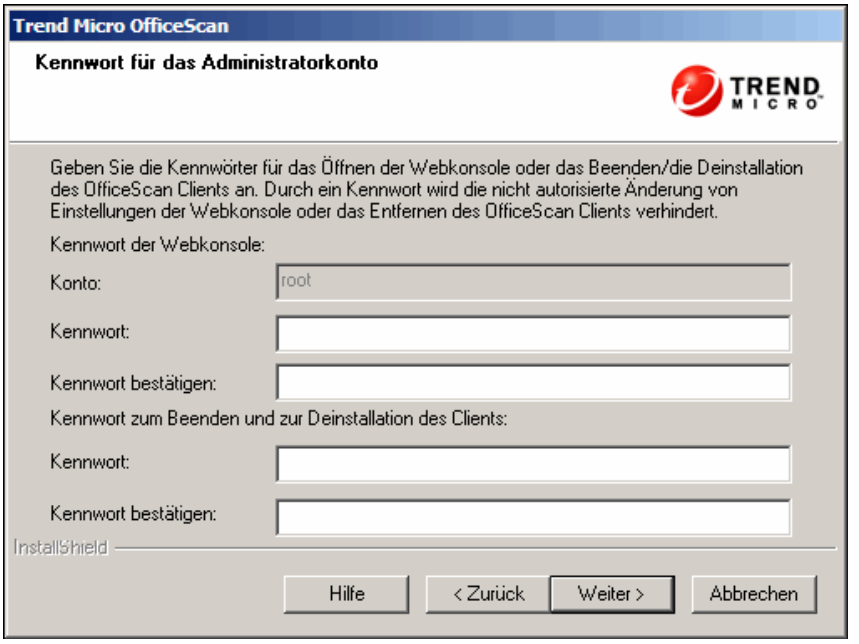


ABBILDUNG 2-20. Das Fenster "Kennwort für das Administratorkonto"

Erstellen Sie Kennwörter für folgende Aufgaben:

Auf die Webkonsole zugreifen

Setup erstellt während der Installation ein Root-Konto. Das Root-Konto hat vollen Zugriff 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 Ihnen und anderen OfficeScan Administratoren bekannt ist. Wenn Sie das Kennwort vergessen, wenden Sie sich zur Unterstützung beim Zurücksetzen des Kennworts an Ihren Support-Anbieter.

OfficeScan Client beenden und deinstallieren

Legen Sie ein Kennwort fest, um unberechtigtes Beenden oder Entfernen des OfficeScan Clients zu verhindern. Deinstallieren oder beenden Sie den Client nur, wenn Probleme mit Client-Funktionen auftreten, und installieren/starten Sie das Programm sofort wieder.

Client-Installationspfad

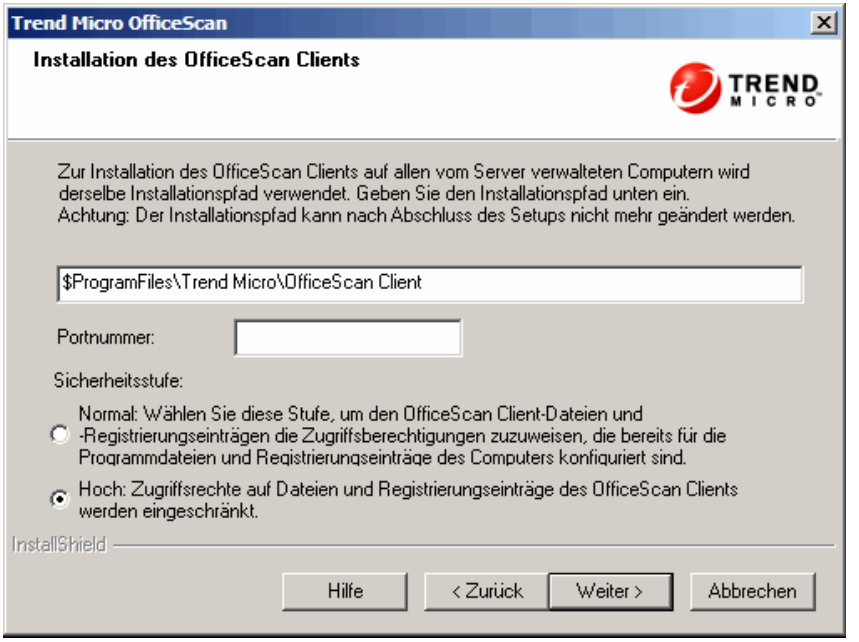


ABBILDUNG 2-21. Das Fenster "Installationspfad des OfficeScan Clients"

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

Tipp: Trend Micro empfiehlt, die Standardeinstellungen zu verwenden.

Falls Sie einen anderen Installationspfad festlegen, geben Sie einen statischen Pfad ein, oder verwenden Sie Variablen. Falls der eingegebene Pfad ein Verzeichnis enthält, das auf dem Client nicht vorhanden ist, erstellt Setup das Verzeichnis automatisch während der Installation des Clients.

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

Hinweis: Der Client-Installationspfad kann nach Fertigstellung der Installation des OfficeScan Servers nicht mehr geändert werden. Alle OfficeScan Clients, die installiert werden, verwenden den gleichen Installationspfad.

Sie können folgende Variablen für den Client-Installationspfad verwenden:

- **$BOOTDISK:** Der Laufwerksbuchstabe der Festplatte, von der der Computer 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 Clients. Sie können eine andere Portnummer angeben.
- **Client-Sicherheitsstufe:** Nach der Installation von OfficeScan können Sie die Sicherheitsstufe über die OfficeScan Konsole ändern (**Netzwerkcomputer > Client-Verwaltung > Einstellungen > Berechtigungen und andere Einstellungen > Andere Einstellungen**).
  - **Normal:** Diese Berechtigung gewährt allen Benutzern (der Benutzergruppe "Alle") Vollzugriff auf das Programmverzeichnis und die Registrierungseinträge des Clients.
  - **Hoch:** Das Installationsverzeichnis des Clients übernimmt die Rechte des Ordners **Programme**, und die Registrierungseinträge des Clients übernehmen die Berechtigungen vom **HKLM\Software** schlüssel. Dies schränkt die Berechtigungen von 'normalen' Benutzern (Benutzer ohne Administratorrechte) für die meisten Active Directory Konfigurationen auf einen Lesezugriff ein.

Antiviren-Funktionen

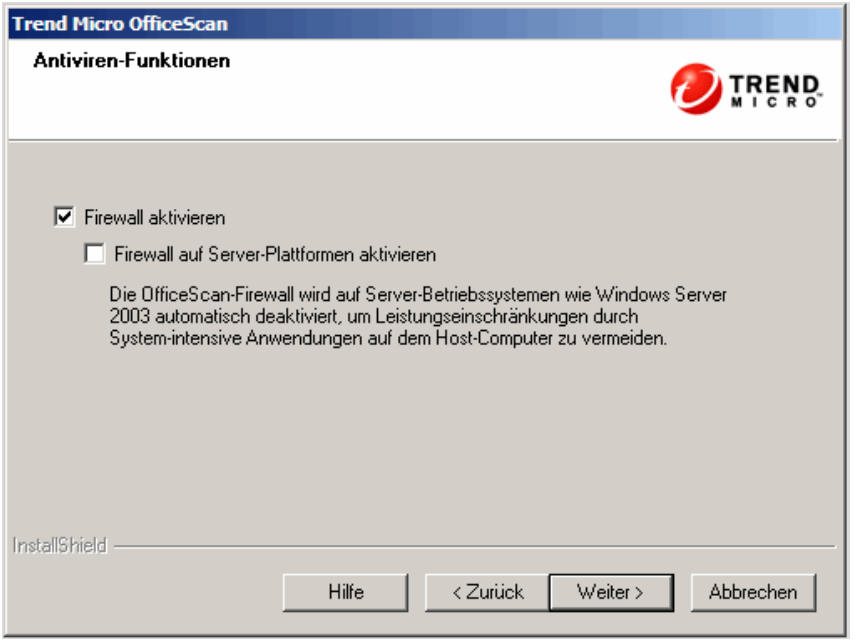


ABBILDUNG 2-22. Das Fenster "Antiviren-Funktionen"

Dieses Fenster wird nur bei aktiviertem Virenschutz angezeigt.

OfficeScan Firewall

Die OfficeScan Firewall mit Stateful-Inspection-Technologie schützt Clients und Server im Netzwerk durch leistungsstarkes Suchen und Entfernen von Netzwerkviren. Sie können Regeln erstellen, um Verbindungen nach IP-Adresse, Portnummer oder Protokoll zu filtern, und anschließend die Regeln auf unterschiedliche Benutzergruppen anwenden.

Sie können die Firewall deaktivieren und diese später wieder von der Webkonsole des OfficeScan Servers aus 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 von OfficeScan nicht deaktiviert wird.

Anti-Spyware-Funktion

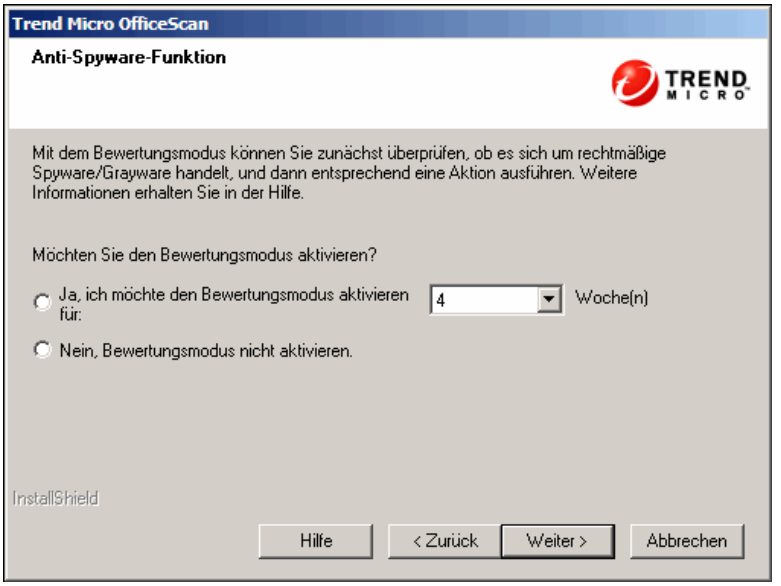


ABBILDUNG 2-23. Das Fenster "Anti-Spyware-Funktion"

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

Im Bewertungsmodus protokollieren alle vom Server verwalteten Clients Spyware/Grayware, die während der manuellen Suche, zeitgesteuerten Suche, Echtzeitsuche und der Funktion "Jetzt durchsuchen" gefunden wurde. Dabei werden jedoch die Spyware-/Grayware-Komponenten nicht gesäubert. Bei der Säuberung werden Prozesse beendet oder Registrierungseinträge, Dateien, Cookies und Shortcuts gelöscht.

Mit dem Bewertungsmodus von Trend Micro können Sie Elemente überprüfen, welche Trend Micro als Spyware/Grayware einstuft, und dann eine geeignete Aktion konfigurieren. Beispielsweise können Sie entdeckte Spyware/Grayware, die Sie als ungefährlich erachten, zur Liste der zulässigen 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 über die Webkonsole ändern (**Netzwerkcomputer > Allgemeine Client-Einstellungen > Spyware-/Grayware-Einstellungen**).

Web-Reputation-Richtlinie

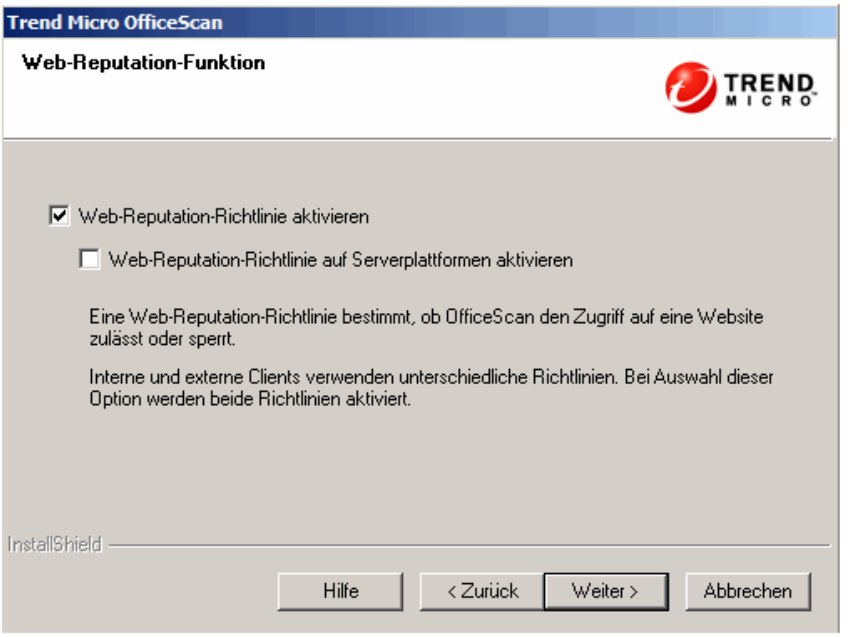


ABBILDUNG 2-24. Das Fenster "Web-Reputation-Funktion"

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

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

Clients ermitteln ihren Standort und die anzuwendende Richtlinie anhand der Standortkriterien, die Sie in der Webkonsole im Fenster 'Computerstandort' festgelegt haben. Clients wechseln die Richtlinien mit jedem Standortwechsel.

Sie können die Einstellungen für Web-Reputation-Richtlinien nach der Installation über die Webkonsole konfigurieren. In der Regel konfigurieren OfficeScan Administratoren eine strengere Richtlinie für externe Clients.

Web-Reputation-Richtlinien sind granulare Einstellungen in der OfficeScan Client-Hierarchie. Sie können bestimmte Richtlinien für Client-Gruppen oder einzelne Clients erzwingen. Sie können auch eine einzelne Richtlinie für alle Clients erzwingen.

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

Hinweis: Der integrierte Server wird mit dem OfficeScan Server installiert. Weitere Informationen finden Sie unter *Installation des integrierten Smart Protection Servers* auf Seite 2-41. Der eigenständige Server wird separat installiert.

Verknüpfung mit Programmordner

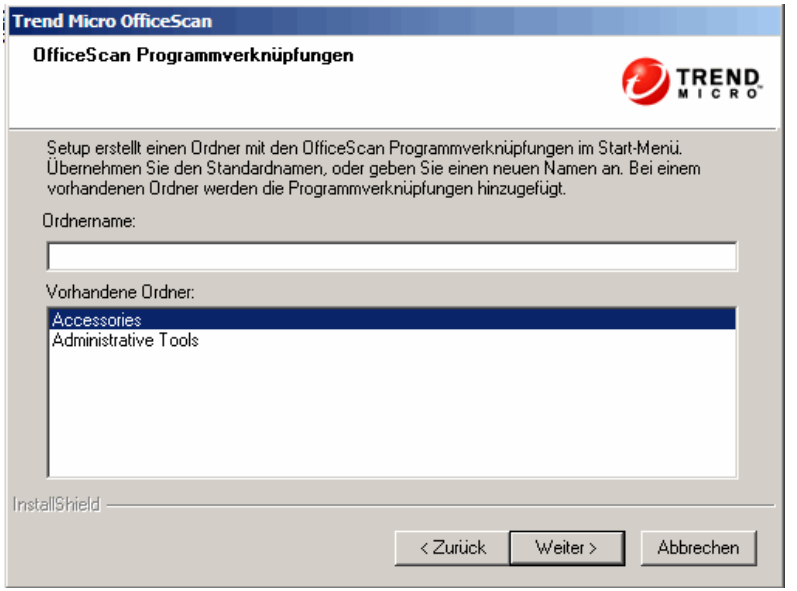


ABBILDUNG 2-25. Das Fenster für die Programmverknüpfungen

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

Installationsdaten

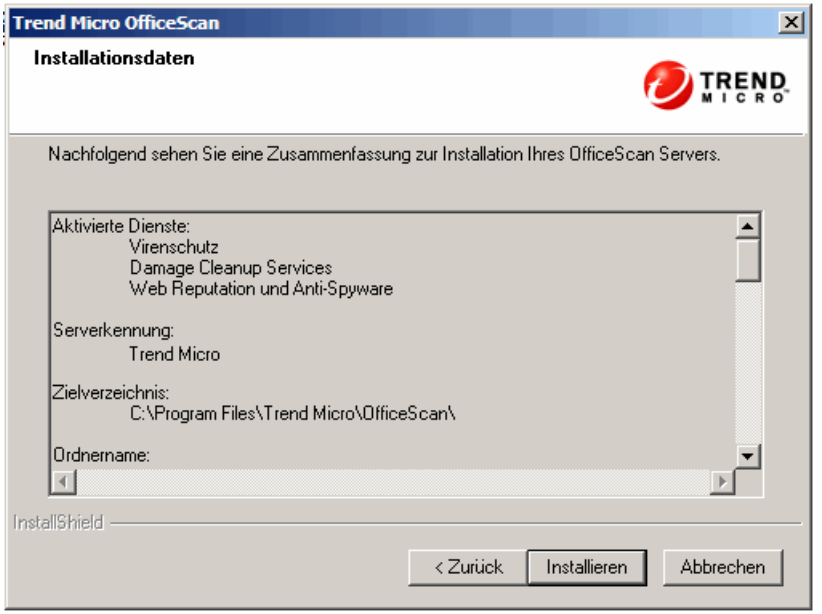


ABBILDUNG 2-26. Das Fenster mit den Installationsdaten

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.

Installation des Policy Servers

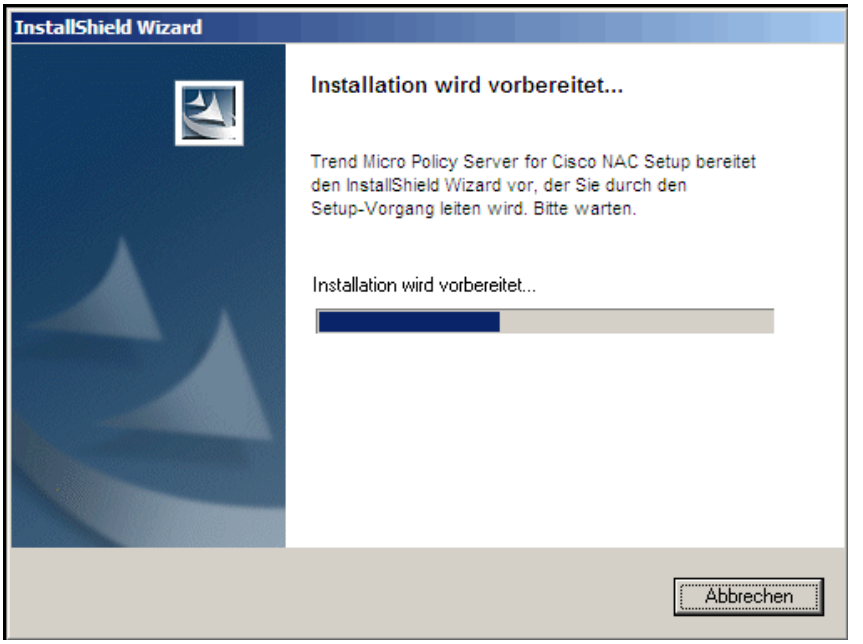


ABBILDUNG 2-27. Das Fenster für die Installation von Policy Server

Dieses Fenster wird angezeigt, wenn Sie den Policy Server für Cisco NAC installieren. Die Einstellungen und Optionen der Fenster im Verlauf der Installation des Policy Servers ähneln den meisten Einstellungen, die Sie während der Installation des OfficeScan Servers vorgenommenen haben.

- **Lizenzvereinbarung:** Akzeptieren Sie die Bedingungen der Lizenzvereinbarung, um fortzufahren.
- **Installationspfad:** Übernehmen Sie den Standard-Installationspfad, oder geben Sie einen Speicherort auf dem lokalen Computer an, auf dem der Policy Server installiert wird.
- **Webserver:** Legen Sie fest, ob ein IIS oder ein Apache Webserver verwendet wird.
- **Webserver-Konfiguration:** Legen Sie die Einstellungen für den ausgewählten Webserver fest.

- **Kennwort der Webkonsole:** Legen Sie ein Kennwort für den Zugriff auf die Policy Server Konsole fest. Die Konsole ist von der Konsole des OfficeScan Servers getrennt, auch wenn Sie die Konsole über OfficeScan aufrufen können.
- **Authentifizierung des ACS-Servers:** Der ACS Server empfängt über das Netzzugangsgerät Antiviren-Daten vom OfficeScan Client und leitet sie zur Überprüfung an eine externe Benutzerdatenbank weiter. Das Ergebnis der Überprüfung, das Anweisungen für den OfficeScan Client enthalten kann, wird dann an das Netzzugangsgerät weitergeleitet.
- **Installationsdaten:** Überprüfen Sie die Installationsdaten.

Abschluss der Installation von OfficeScan Server

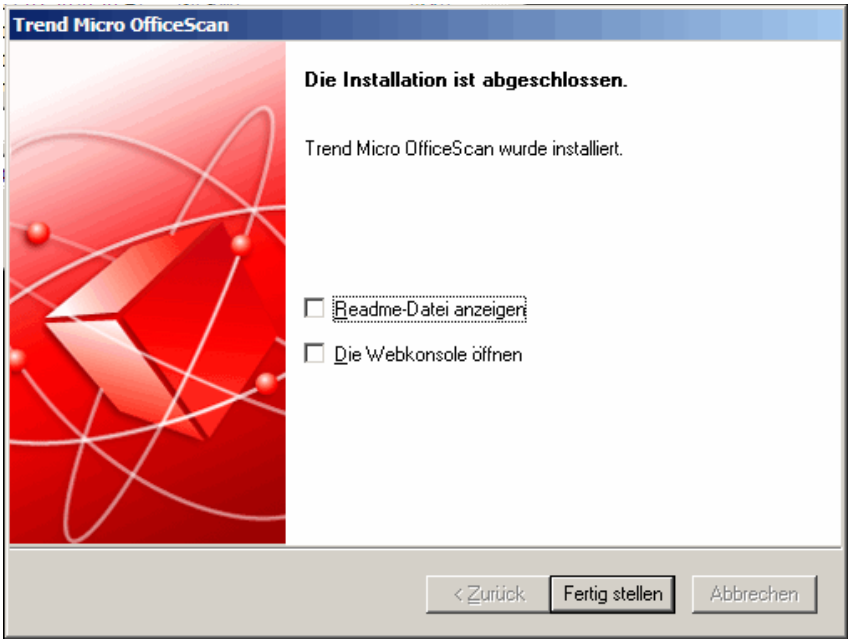


ABBILDUNG 2-28. Fenster "Installation abgeschlossen"

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

Sie können auch die Webkonsole öffnen, um die OfficeScan Einstellungen zu konfigurieren.

Aufgaben nach der Installation

Führen Sie im Anschlus an die Installation folgende Aufgaben aus:

- *Die Installation bzw. das Upgrade des Servers auf Vollständigkeit überprüfen* auf Seite 2-68
- *Aktualisieren der OfficeScan Komponenten* auf Seite 2-71
- *Überprüfen der Standardeinstellungen* auf Seite 2-72
- *Client Mover für veraltete Plattformen verwenden* auf Seite 2-73. Führen Sie diese Aufgaben nur dann durch, wenn im Netzwerk Clients mit Windows 95, 98, Me, NT, 2000 oder Itanium-Architektur vorhanden sind.
- *Registrieren von OfficeScan beim Control Manager* auf Seite 2-76. Nur neu installierte OfficeScan Server werden beim Control Manager registriert.

Die Installation bzw. das Upgrade des Servers auf Vollständigkeit überprüfen

Nach Abschluss der Installation oder des Upgrades sollten Sie Folgendes überprüfen:

TABELLE 2-5. Nach der Installation oder dem Upgrade von OfficeScan zu überprüfende Elemente

ZU ÜBERPRÜFENDES ELEMENT	DETAILS
Verknüpfungen für OfficeScan Server	Die Trend Micro OfficeScan Server-Verknüpfungen werden auf dem Server-Computer im Windows Menü **Start** angezeigt.
Programmliste	**Trend Micro OfficeScan Server** wird auf dem Server-Computer in der Liste **Software** der Systemsteuerung aufgeführt.

TABELLE 2-5. Nach der Installation oder dem Upgrade von OfficeScan zu überprüfende Elemente (Fortsetzung)

ZU ÜBERPRÜFENDES ELEMENT	DETAILS
OfficeScan Webkonsole	Geben Sie die folgenden URLs im Internet Explorer ein: • HTTP-Verbindung: http://<Name des OfficeScan Servers>:<Portnummer>/OfficeScan • HTTPS-Verbindung: https://<Name des OfficeScan Servers>:<Portnummer>/OfficeScan Wobei <Name des OfficeScan Servers> für den Namen oder die IP-Adresse des OfficeScan Servers steht. Das Anmeldefenster der OfficeScan Webkonsole wird angezeigt.

TABELLE 2-5. Nach der Installation oder dem Upgrade von OfficeScan zu überprüfende Elemente (Fortsetzung)

ZU ÜBERPRÜFENDES ELEMENT	DETAILS
OfficeScan Server-Dienste	Folgende OfficeScan Server-Dienste werden in der Microsoft Management-Konsole aufgeführt: • **OfficeScan Active Directory Integrationsdienst:** Dieser Dienst zeigt an, ob die Active-Directory-Integration und die rollenbasierte Administration ordnungsgemäß funktionieren. • **OfficeScan Control Manager Agent:** Der Status dieses Dienstes sollte "Gestartet" lauten, wenn der OfficeScan Server bei Control Manager registriert ist. • **OfficeScan Master Service:** Der Status dieses Dienstes sollte "Gestartet" lauten. • **OfficeScan Plug-in Manager:** Der Status dieses Dienstes sollte "Gestartet" lauten. • **Intelligenter Suchserver von Trend Micro:** Der Status dieses Dienstes sollte "Gestartet" lauten. • **Trend Micro Local Web Classification Server:** Der Status dieses Dienstes sollte "Gestartet" lauten, wenn die Web-Reputation-Dienste bei der Installation aktiviert wurden. • **Trend Micro Policy Server für Cisco NAC:** Der Status dieses Dienstes sollte "Gestartet" lauten, wenn Policy Server installiert 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%.

TABELLE 2-5. Nach der Installation oder dem Upgrade von OfficeScan zu überprüfende Elemente (Fortsetzung)

ZU ÜBERPRÜFENDES ELEMENT	DETAILS
Registrierungsschlüssel	Es sind folgende Registrierungsschlüssel vorhanden: HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan
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 des OfficeScan Servers.

Die Installation des integrierten Smart Protection Servers überprüfen:

1. Navigieren Sie auf der Webkonsole des OfficeScan Servers zu **Smart Protection > Smart Protection Server 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 der OfficeScan Komponenten

Nach der Installation oder dem Upgrade von OfficeScan müssen die Komponenten auf dem Server aktualisiert werden.

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:

1. Öffnen Sie die OfficeScan Webkonsole.
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.

Überprüfen der Standardeinstellungen

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 bietet verschiedene Suchtypen, mit denen Sie Computer vor Sicherheitsrisiken schützen können. Die Sucheinstellungen können Sie über die Webkonsole unter **Netzwerkcomputer > Client-Verwaltung > Einstellungen > {Suchtyp}** ändern.

Allgemeine Client-Einstellungen

In OfficeScan stehen verschiedene Einstellungsarten zur Verfügung, die für alle am Server registrierten Clients oder für alle Clients mit einer bestimmten Berechtigung gelten. Allgemeine Client-Einstellungen können Sie über die Webkonsole unter **Netzwerkcomputer > Allgemeine Client-Einstellungen** ändern.

Client-Berechtigungen

Zu den Client-Standardberechtigungen zählt das Anzeigen der Registerkarten **Mail Scan** und **Toolbox** in der Client-Konsole. Client-Standardberechtigungen können Sie über die Webkonsole unter **Netzwerkcomputer > Client-Verwaltung > Einstellungen > Berechtigungen und andere Einstellungen** ändern.

Client Mover für veraltete Plattformen verwenden

Der OfficeScan Client unterstützt die Betriebssysteme Windows 95, 98, Me, NT und 2000 sowie die Itanium-Plattform nicht mehr. Wenn OfficeScan Clients auf einer dieser Plattformen ausgeführt werden und Sie den Server, der sie verwaltet, auf Version 10.6 aktualisieren, hat das folgende Konsequenzen:

- Die OfficeScan Clients werden nicht aktualisiert.
- Nicht unterstützte Clients werden vom OfficeScan 10.6 Server nicht mehr verwaltet. Diese Clients erhalten den Status "Keine Verbindung zum Server".
- Die Informationen des Clients werden auf dem OfficeScan 10.6 Server in der Datei **unsupCln.txt** gespeichert. Mit Hilfe dieser Datei "verschieben" Sie die Clients auf einen Server mit derselben Version. Verschieben bedeutet, dass Sie einen neuen Server für die Verwaltung der Clients bestimmen.
- Sie müssen auf dem OfficeScan 10.6 Server-Computer das Client Mover Tool für veraltete Plattformen ausführen. Dieses Tool benachrichtigt die Clients, dass sie von einem neuen Server verwaltet werden, und überprüft, ob die Client-Verschiebung erfolgt ist. Wenn die Clients die Benachrichtigung erhalten, werden sie bei ihrem neuen übergeordneten Server registriert.

Clients verschieben:

1. Bereiten Sie einen neuen übergeordneten Server vor. Dieser Server muss die gleiche Version haben wie die zu verschiebenden Clients.
2. Notieren Sie den Computernamen/die IP-Adresse und den Server-Listening-Port des Servers. Sie benötigen diese Angaben zum Verschieben der Clients.

   Den Server-Listening-Port können Sie der Webkonsole des Servers entnehmen, indem Sie zu **Administration > Webserver** navigieren.
3. Navigieren Sie auf dem OfficeScan 10.6 Server-Computer zum Ordner <Installationsordner des Servers>\PCCSRV\Admin\Utility\ClientMover, und führen Sie **clientmover.exe** aus.

4. Geben Sie im Befehlsfenster folgenden Befehl ein:

   ```
   ClientMover /P:<ExportDataPath> /S:<ServerIP:port> /N
   ```

   Wobei gilt:

   - **ExportDataPath:** Der Pfad und Name der Datei (unsupCln.txt) mit den Angaben zu den Clients.
   - **ServerIP:port:** Die IP-Adresse und Server-Listening-Port-Nummer des neuen übergeordneten Servers.
   - **/N:** Ein Befehl, der die Clients benachrichtigt und anschließend auf den neuen übergeordneten Server verschiebt. Dieser Befehl wird in Verbindung mit dem /V-Befehl verwendet.

   Beispiel:

   ClientMover /P:"C:\Program Files\TrendMicro\OfficeScan\PCCSRV\Private\unsupcln.txt" /S:123.12.12.123:23456 /N

5. Überprüfen Sie mit dem /V-Befehl, ob das Tool die Clients wirklich verschoben hat. Dieser Befehl vergleicht die IP-Adresse des OfficeScan 10.6 Servers mit der Adresse des neuen übergeordneten Servers. Stimmen die IP-Adressen überein, konnten die Clients nicht verschoben werden.

   Beispiel:

   ClientMover /P:"C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Private\unsupcln.txt" /S:123.12.12.123:23456 /V

6. Das Ergebnis überprüfen:

   a. Öffnen Sie das Ergebnisprotokoll unter \PCCSRV\Private\. Der Name der Protokolldatei lautet "unsupcln.txt.log.<Datum_Zeit>".

      Beispiel: unsupcln.txt.log.20080101_123202

   b. Überprüfen Sie im selben Ordner, ob OfficeScan die Datei unsupcln.txt aktualisiert und gesichert hat. Der Name der Sicherungsdatei ist unsupcln.txt.bak.

Der Eintrag in der aktualisierten Datei unsupcln.txt lautet beispielsweise:

```
------------------------------------------------------------

x12xx345-6xxx-78xx-xx91-234x567x8x91 1234567891 23456 0

------------------------------------------------------------
```

Wobei gilt:

- "x12xx345-6xxx-78xx-xx91-234x567x8x91" ist die GUID des Clients.
- "1234567891" ist die IP-Adresse des Clients in Dezimalschreibweise.
- "23456" ist der Client-Listening-Port.
- "0" ist das Ergebnis und bedeutet, dass die Benachrichtigung erfolgt ist.

  Weitere mögliche Ergebnisse:

  - 1 = Client-Benachrichtigung erfolgreich
  - 2 = Client-Benachrichtigung fehlgeschlagen
  - 3 = Überprüfung erfolgreich
  - 4 = Überprüfung fehlgeschlagen

Beispieleintrag in der Datei "unsupcln.txt.log.<Datum_Zeit>":

```
------------------------------------------------------------

x12xx345-6xxx-78xx-xx91-234x567x8x91 123.12.12.123:23456
Senden der Benachrichtigung nicht möglich. Überprüfen Sie
den Status von Netzwerk und Client.

------------------------------------------------------------
```

Wobei gilt:

- "x12xx345-6xxx-78xx-xx91-234x567x8x91" ist die GUID des Clients.
- "123.12.12.123:23456" ist die IP-Adresse und der Listening-Port des Clients.
- Das Ergebnis lautet "Die Benachrichtigung konnte nicht gesendet werden. Überprüfen Sie den Status von Netzwerk und Client."

7. Mit dem /F-Befehl können Sie die Benachrichtigung oder Überprüfung ohne Berücksichtigung des aktuellen Client-Status durchsetzen.

Registrieren von OfficeScan beim Control Manager

Falls ein Control Manager Server neu installierte OfficeScan Server verwalten soll, müssen Sie OfficeScan nach der Installation beim Control Manager registrieren. Dazu navigieren Sie auf der OfficeScan Webkonsole zu **Administration > Control Manager Einstellungen**. Weitere Informationen zu diesem Verfahren finden Sie in der *OfficeScan Server-Hilfe* oder im *OfficeScan Administratorhandbuch*.

Deinstallation und Rollback

Wenn Probleme mit OfficeScan auftreten, haben Sie folgende Möglichkeiten:

- Verwenden Sie das Deinstallationsprogramm, um OfficeScan Server sicher vom Computer zu entfernen. Verschieben Sie vor der Deinstallation des Servers die von ihm verwalteten Clients auf einen anderen OfficeScan Server.
- Führen Sie ein Rollback der Clients auf die Version früherer OfficeScan Versionen durch, anstatt den OfficeScan Server zu deinstallieren. Weitere Informationen finden Sie unter *Rollback zu früheren OfficeScan Versionen* auf Seite 2-83.

Deinstallation des OfficeScan Servers

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

Vor der Deinstallation des OfficeScan Servers

Verschieben Sie vor der Deinstallation des Servers die von ihm verwalteten Clients auf einen 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.

Clients auf einen anderen OfficeScan Server verschieben

Die OfficeScan Webkonsole bietet eine Option an, mit der vom Server verwaltete Clients auf einen anderen OfficeScan Server verschoben werden können.

Clients auf einen anderen OfficeScan Server verschieben:

1. Notieren Sie sich folgende Informationen für den anderen OfficeScan Server. Sie benötigen die Angaben, wenn Sie die OfficeScan Clients verschieben.
   - Computername oder IP-Adresse
   - Server-Listening-Port

     Um den Server-Listening-Port anzuzeigen, navigieren Sie zu **Administration > Verbindungseinstellungen**. Die Portnummer wird auf dem Bildschirm angezeigt.
2. Auf der Webkonsole des Servers, den Sie deinstallieren möchten, navigieren Sie zu **Netzwerkcomputer > Client-Verwaltung**.
3. Wählen Sie in der Client-Hierarchie die Clients aus, die Sie aktualisieren möchten, und klicken Sie anschließend auf **Client-Hierarchie verwalten > Client verschieben**.
4. Geben Sie unterhalb von **Ausgewählte(n) Client(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 Clients 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. Erstellen Sie eine Sicherungskopie der OfficeScan Server-Datenbank an einem Speicherort außerhalb des OfficeScan Programmordners.

Die OfficeScan Datenbank und die Konfigurationsdateien sichern und wiederherstellen:

1. Sichern Sie die Datenbank über die OfficeScan Webkonsole, indem Sie zu **Administration > Datenbank-Backup** navigieren. Anleitungen hierzu finden Sie im *Administratorhandbuch* und in der *OfficeScan Server Hilfe*.

ACHTUNG! **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. Sichern Sie manuell folgende Dateien und Ordner unter <Installationsordner des Servers>\PCCSRV:
   - **ofcscan.ini:** Diese Datei enthält allgemeine Client-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 *Deinstallation des OfficeScan Servers* auf Seite 2-76.
5. Führen Sie eine Erstinstallation durch. Weitere Informationen finden Sie unter *Erstinstallation des OfficeScan Servers durchführen* auf Seite 2-2.
6. Öffnen Sie nach beendetem Setup die Microsoft Management-Konsole (klicken Sie auf **Start > Ausführen**, und geben Sie **services.msc** ein).
7. Klicken Sie mit der rechten Maustaste auf **OfficeScan Master Service** und anschließend auf **Beenden**.
8. Kopieren Sie die Sicherungsdateien in den Ordner <Installationsordner des Servers>\PCCSRV auf dem Zielcomputer. Hierdurch werden die OfficeScan Server-Datenbank und die entsprechenden Dateien und Ordner überschrieben.
9. Starten Sie den OfficeScan Master-Dienst 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 für die Deinstallation von OfficeScan Clients finden Sie im *Administratorhandbuch*.

Den OfficeScan Server mit Hilfe des Deinstallationsprograms deinstallieren:

1. Wenn Sie eine Erstinstallation auf dem Server-Computer durchgeführt haben, können Sie diesen Schritt überspringen.

   Wenn Sie ein Upgrade des Servers von einer Vorgängerversion auf diese Version durchgeführt haben:

   a. Wenn der Plug-in Manager zurzeit installiert ist, deinstallieren Sie ihn.

   b. Wenn der Plug-in-Manager nicht installiert ist, löschen Sie den **AOS**-Registrierungsschlüssel unter HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\.

2. 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 Server manuell deinstallieren:

Teil 1: Deinstallation des integrierten Smart Protection Servers

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
   ```

   Dieser Befehl deinstalliert OfficeScan-Dienste, entfernt jedoch weder die Konfigurationsdateien noch die OfficeScan Datenbank.
4. Navigieren Sie zum Ordner <Installationsordner des Servers>\PCCSRV\private, und öffnen Sie die Datei **ofcserver.ini**.
5. Ändern Sie die folgenden Einstellungen:

TABELLE 2-6. ofcserver.ini-Einstellungen

EINSTELLUNG	ANWEISUNG
WSS_INSTALL=1	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:
   - Bei Verwendung eines IIS Webservers:

     ```
     [WSS_WEB_SERVER]
     ServerPort=8082
     IIS_VhostName=Smart Protection Server (integriert)
     IIS_VHostIdx=5
     ```

     Hinweis: Der Wert für IIS_VHostidx sollte derselbe wie der "isapi"-Wert sein, der durch die folgende Zeile dargestellt wird:

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

     ```
     [WSS_SSL]
     SSLPort=<SSL-Port>
     ```
   - Bei Verwendung des Apache Webservers:

     ```
     [WSS_WEB_SERVER]
     ServerPort=8082
     [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
   - Website des Smart Protection Server (integriert)

Teil 2: Deinstallation des OfficeScan Servers

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

   ACHTUNG! Die nächsten Schritte erfordern, dass Sie Registrierungsschlüssel löschen. Unsachgemäße Änderungen an der Registrierung können zu ernsthaften Systemproblemen führen. Erstellen Sie immer eine Sicherungskopie, bevor Sie Änderungen an der Registrierung vornehmen. Weitere Informationen finden Sie in der Hilfe zum Registrierungseditor.

   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-Computer lautet der Pfad HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfficeScan\.

   d. Navigieren Sie zu HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\, und löschen Sie den Ordner **OfficeScan Management Console-<Server-Name>**.

2. Navigieren Sie zum Ordner <Installationsordner des Servers>\PCCSRV, und heben Sie die Freigabe des Ordners **PCCSRV** auf.
3. Starten Sie den Server-Computer neu.
4. Navigieren Sie zum Ordner <Installationsordner des Servers>\PCCSRV, und löschen Sie den Ordner **PCCSRV**.
5. Löschen Sie die OfficeScan Website von der IIS Konsole aus.
   a. Öffnen Sie die IIS Konsole.
   b. Erweitern Sie **Servername**.

c. Falls Sie OfficeScan auf einer separaten Website installiert haben, navigieren Sie zum Ordner **Web Sites**, und löschen Sie **OfficeScan**.

d. Falls Sie unterhalb der Standard-Website virtuelle OfficeScan Verzeichnisse installiert haben, navigieren Sie zur **Standard-Website**, und löschen anschließend das virtuelle OfficeScan Verzeichnis.

Rollback zu früheren OfficeScan Versionen

Wenn Probleme beim Upgrade von OfficeScan Clients auftreten, können Sie ein Rollback der Clients zu ihrer früheren Version durchführen.

Um ein erfolgreiches Rollback durchzuführen, bereiten Sie Folgendes vor:

- Einen OfficeScan Server, der die Clients verwaltet, für die ein Rollback durchgeführt wird. Die Serverversion sollte eine der folgenden sein:
  - 10.5 Patch 1
  - 10.5
  - 10.0 Service Pack 1
  - 10.0
  - 8.0 Service Pack 1
- Einen Computer, der als Update-Quelle dient. Diese Update-Quelle enthält die Dateien und Komponenten des Rollbacks. Wird ein Client, für den ein Rollback ausgeführt werden soll, von dieser Quelle aus aktualisiert, wird der Client deinstalliert, und die vorherige Version des Clients wird installiert.
- Den OfficeScan 10.6 Server, der die Clients verwaltet, für die das Rollback ausgeführt werden soll.
- Die OfficeScan 10.6 Clients, für die das Rollback ausgeführt werden soll.

Teil 1: Vorbereiten der Vorgängerversion des OfficeScan Servers:

1. Bereiten Sie einen Computer 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 OfficeScan 10.6 Servereinstellungen auf die Vorgängerversion von OfficeScan Server.

Beachten Sie die folgenden Einstellungen:

a. Client-Einstellungen

- Durchsuchen
- Update-Agents
- Berechtigungen
- Liste der zulässigen Spyware/Grayware (für OfficeScan 8.0 SP1 oder höher)
- Ausnahmeliste der Verhaltensüberwachung (für OfficeScan 10.0 SP1 oder höher)

b. Allgemeine Client-Einstellungen

c. Web-Reputation-Einstellungen (für OfficeScan 8.0 SP1 oder höher)

- Computerstandort
- Richtlinien
- Proxy

d. OfficeScan Firewall-Einstellungen

- Richtlinie
- Profile

e. Zeitplan der Verbindungsüberprüfung

f. Update-Einstellungen

- Zeitgesteuertes Serverupdate
- Server-Update-Adresse
- Zeitgesteuertes Client-Update
- Update-Adresse des Clients

g. Einstellungen der Protokollwartung

h. Benachrichtigungen - alle Benachrichtigungseinstellungen

i. Administrationseinstellungen

- Quarantäne-Manager
- Control Manager
- Datenbanksicherung

4. Führen Sie auf der Vorgängerversion von OfficeScan Server Client Packager zweimal aus, um zwei Client-Installationspakete zu erstellen, ein Paket für x86-Computer und ein weiteres für x64-Computer.

   Einstellungen im Client-Installationspaket für x86-Computer:

   - Packettyp: Setup
   - Windows Betriebssystem: 32-Bit
   - Ausgabedatei: InstNTPkg.exe

   Einstellungen im Client-Installationspaket für x64-Computer:

   - 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: Update-Quelle für Clients, für die ein Rollback durchgeführt werden soll, vorbereiten

1. Bereiten Sie einen Computer vor, der als Update-Quelle dient.
2. Navigieren Sie auf dem OfficeScan 10.6 Servercomputer zu <Installationsordner des Servers>\PCCSRV, und kopieren Sie den Ordner **Download** (einschließlich seiner Unterordner) auf den Computer, der als Update-Quelle dient (der im voranstehenden Schritt vorbereitete Computer).

   Kopieren Sie den Ordner **Download** z. B. in das folgende Verzeichnis des Computers, der als Update-Quelle fungiert:

   C:\OfficeScanUpdateSource
3. Führen Sie auf dem OfficeScan 10.6 Servercomputer folgende Schritte durch:
   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 Client-Installationspaket für x86-Computer (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 Client-Installationspaket für x64-Computer (InstPkg.exe)

j. Komprimieren Sie den Unterordner "RollbackNTPkgx64" zu "RollbackNTPkgx64.zip".

k. Kopieren Sie die folgenden komprimierten Dateien aus dem temporären Ordner auf den Computer, der als Update-Quelle fungiert:

- RollbackAgent.zip
- RollbackAgent_64x.zip
- RollbackNTPkg.zip
- RollbackNTPkgx64.zip

Hinweis: Kopieren Sie die Dateien in den Ordner "\Download\Product" auf dem Computer, der als Update-Quelle fungiert. Kopieren Sie die Dateien z. B. nach "C:\OfficeScanUpdateSource\Download\Product".

---

4. Auf dem Computer, der als Update-Quelle fungiert:
   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.

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

      ACHTUNG! 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_1]

      Version=**<Vorherige OfficeScan Version>**

      Update_Path=product/RollbackAgent.zip, **<RollbackAgent-Dateigröße>**

      Path=product/RollBackNTPkg.zip, **<RollBackNTPkg-Dateigröße>**

[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. Zum 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 (10.6)
- **<Vorherige OfficeScan Version>:** Vorherige OfficeScan Version. Beispiel: 10.0.

Teil 3: Rollback der Clients durchführen

1. Führen Sie auf der OfficeScan 10.6 Webkonsole folgende Schritte durch:
   a. Navigieren Sie zu **Updates > Netzwerkcomputer > Update-Adresse**.
   b. Wählen Sie **Benutzerdefinierte Update-Adresse** aus.
   c. Klicken Sie in der **Liste der benutzerdefinierten Update-Quelle** auf **Hinzufügen**. Es öffnet sich ein neues Fenster.

d. Geben Sie die IP-Adressen der Clients ein, für die das Rollback ausgeführt werden soll.

e. Geben Sie die URL der Update-Quelle an. Geben Sie z. B. Folgendes ein:

http://<IP-Adresse der Update-Quelle>/OfficeScanUpdateSource/

f. Klicken Sie auf **Speichern**. Das Fenster wird geschlossen.

g. Klicken Sie auf **Alle Clients benachrichtigen**.

Wird ein Client, für den ein Rollback ausgeführt werden soll, von der Update-Quelle aus aktualisiert, wird der Client deinstalliert, und die vorherige Version des Clients wird installiert.

2. Fordern Sie den Benutzer nach der Installation der vorherigen Client-Version auf, den Computer neu zu starten. Nach dem Neustart berichtet der Client an den in Teil 1 vorbereiteten OfficeScan Server.

Kapitel 3

Hilfe anfordern

Dieses Kapitel beschreibt, wie Sie eventuell auftretende Probleme beheben und wie Sie Kontakt zum Support aufnemen können.

Themen in diesem Kapitel:

Ressourcen zur Fehlerbehebung

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:

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. Kopieren 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.

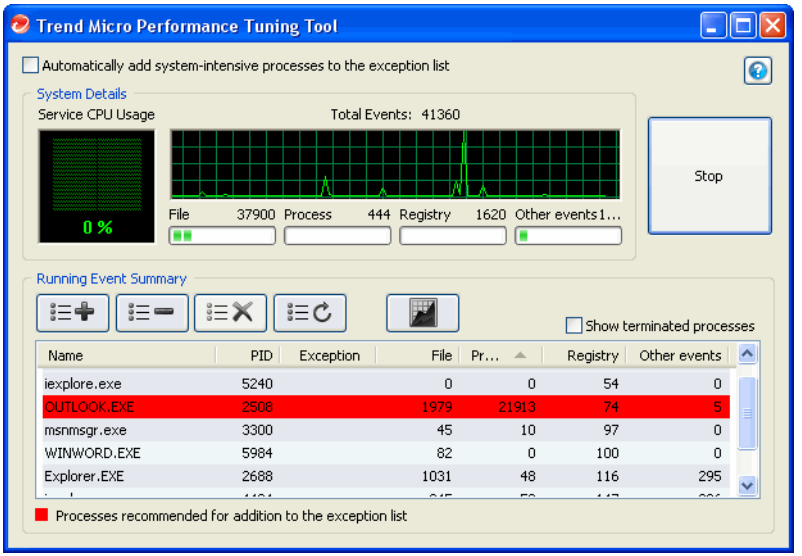


ABBILDUNG 3-1. Markierter systemintensiver Prozess

7. Wählen Sie einen systemintensiven Prozess, und klicken Sie auf die Schaltfläche **Zur Ausnahmeliste 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 Ausnahmeliste 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 Ausnahmeliste der Verhaltensüberwachung hinzu. Weitere Informationen finden Sie im Administratorhandbuch.

Installationsprotokolle

Verwenden Sie zur Behebung von Installationsproblemen die von OfficeScan automatisch erstellten Installationsprotokolle.

TABELLE 3-1. Installationsprotokolldateien

PROTOKOLLDATEI	DATEINAME	SPEICHERORT
Lokales Installations-/Upgrade-Protokoll des Servers	OFCMAS.LOG	%windir%
Remote-Installations-/Upgrade-Protokoll des Servers	OFCMAS.LOG (auf dem Computer, auf dem Setup gestartet wurde) OFCMAS.LOG (auf dem Zielcomputer)	%windir%

TABELLE 3-1. Installationsprotokolldateien (Fortsetzung)

PROTOKOLLDATEI	DATEINAME	SPEICHERORT
Client-Installationsprotokoll	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 Computer aktiviert, auf dem das Setup ausgeführt wird, und nicht auf dem Remote-Computer.).

ACHTUNG! 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.

Debug-Protokollierung auf dem OfficeScan Server aktivieren:

Möglichkeit 1:

1. Melden Sie sich an der Webkonsole an.
2. Klicken Sie auf dem Banner der Webkonsole auf das erste "c" 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:

1. Kopieren Sie den Ordner "LogServer", der sich im Ordner <Installationsordner des Servers>\\PCCSRV\\Private befindet, 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 die Datei ofcdebug.ini unter C:\LogServer.
4. Führen Sie die entsprechende Aufgabe durch (d. h. den Server deinstallieren und installieren, auf eine neue Version upgraden oder eine Remote-Installation/ein Remote-Upgrade durchführen).
5. Überprüfen Sie die Datei ofcdebug.log unter C:\LogServer.

Hinweis: Wenn auf dem OfficeScan Server ein OfficeScan Client vorhanden ist, werden die Debug-Meldungen des Clients auch in die Debug-Protokolle des Servers eingetragen.

Debug-Protokolle für den Client

Sie können die Debug-Protokollierung vor der Installation des OfficeScan Clients aktivieren.

ACHTUNG! **Debug-Protokolle können die Client-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.**

Debug-Protokollierung auf dem OfficeScan Server aktivieren:

1. Erstellen Sie eine Datei mit dem Namen ofcdebug.ini und dem folgenden Inhalt:

   [Debug]

   Debuglog=C:\ofcdebug.log

   debuglevel=9

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1

2. Senden Sie die Datei ofcdebug.ini an die Client-Benutzer, und weisen Sie sie an, die Datei im Laufwerk C:\ zu speichern. LogServer.exe wird automatisch beim Systemstart des Client-Computers ausgeführt. Weisen Sie die Benutzer an, das Befehlsfenster von LogServer.exe, das beim Systemstart des Computers geöffnet wird, NICHT zu schließen, da OfficeScan in diesem Fall die Debug-Protokollierung beenden würde. Schließt der Benutzer das Befehlsfenster, kann die Debug-Protokollierung erneut gestartet werden, indem der Prozess LogServer.exe im Ordner \OfficeScan Client ausgeführt wird.
3. Prüfen Sie auf jedem Client-Computer die Datei ofcdebug.log im Laufwerk C:\.
4. Löschen Sie die Datei ofcdebug.ini, um die Debug-Protokollierung für den OfficeScan Client zu deaktivieren.

Kontaktaufnahme mit Trend Micro

Technischer Support

Trend Micro bietet allen registrierten Benutzern technischen Support, Pattern-Downloads und Programm-Updates für die Dauer eines (1) Jahres. Nach Ablauf dieser Frist muss der Wartungsvertrag verlängert werden. Setzen Sie sich mit uns in Verbindung, wenn Sie Hilfe benötigen oder eine Frage haben. Wir freuen uns ebenso über Ihre Anregungen.

Trend Micro Incorporated bietet allen registrierten Benutzern weltweit technischen Support.

- Auf der folgenden Website finden Sie eine Liste unserer weltweiten Support-Büros:

  http://esupport.trendmicro.com

- Auf dieser Website finden Sie die Dokumentation der neuesten Trend Micro Produkte:

  http://docs.trendmicro.com/de-de/home.aspx

Anschriften/Telefonnummern weltweit

Weltweite Kontaktadressen für den asiatisch-pazifischen Raum, Australien und Neuseeland, Europa, Lateinamerika und Kanada finden Sie unter folgender Adresse:

http://de.trendmicro.com/de/about/contact_us/index.html

Internet-Adresse:

http://www.trendmicro.com

E-Mail: support@trendmicro.com

Schnelle Lösung des Problems

Bei der Kontaktaufnahme mit Trend Micro sollten Sie folgende Informationen bereithalten:

- Version von Microsoft Windows und des Service Packs
- Art des Netzwerks
- Marke und Modell des Computers sowie zusätzliche Hardware, die an den Computer angeschlossen ist
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Ausführliche Beschreibung der Installationsumgebung
- Genauer Wortlaut eventueller Fehlermeldungen
- Schritte, um das Problem nachvollziehen zu können

Die Knowledge Base von Trend Micro

Die Knowledge Base befindet sich auf der Website von Trend Micro. Sie enthält aktuelle Antworten auf Fragen zu den Produkten. Wenn Sie in der Produktdokumentation keine Antwort auf Ihre Frage finden, können Sie die Frage auch über die Knowledge Base an das Supportteam richten. Zugriff auf die Knowledge Base erhalten Sie unter:

http://esupport.trendmicro.com

Trend Micro aktualisiert die Einträge in der Knowledge Base regelmäßig und erweitert sie täglich um neue Lösungen. Wenn Sie keine Lösung für Ihr Problem finden, können Sie dieses auch in einer E-Mail schildern und direkt an einen Support-Mitarbeiter von Trend Micro senden, der das Problem untersucht und Ihnen schnellstmöglich weiterhilft.

TrendLabs

TrendLabs[SM] ist das globale Netzwerk für Antiviren-Forschung und Support von Trend Micro. Auf drei Kontinenten und mit über 250 Virenforschern und -experten, die rund um die Uhr im Einsatz sind, stellt TrendLabs Service und Support für Sie und alle Trend Micro Kunden bereit.

Nach dem Kauf eines Trend Micro Produkts stehen Ihnen folgende Service-Leistungen zur Verfügung:

- Regelmäßige Viren-Pattern-Updates für alle bekannten "In-the-zoo"- und "In-the-wild"-Computerviren und bösartigen Codes
- Notfall-Support bei Virenausbruch
- E-Mail-Kontakt mit Antiviren-Technikern
- Knowledge Base, die Online-Datenbank von Trend Micro mit Informationen über bekannte Probleme

TrendLabs besitzt die ISO-9002-Qualitätssicherungszertifizierung.

Security Information Center

Umfassende Sicherheitsinformationen finden Sie auf der Trend Micro Website unter:

http://www.trendmicro.com/vinfo/de/virusencyclo/default.asp

Verfügbare Informationen:

- Liste mit Viren und bösartigen mobilen Codes, die zum jeweiligen Zeitpunkt im Umlauf und aktiv sind
- Falschmeldungen (Hoaxes)
- Beratung zu Internet-Bedrohungen
- Wöchentlicher Virenbericht
- Virenenzyklopädie, die eine ausführliche Liste von Namen und Symptomen bekannter Viren und bösartigen mobilen Codes enthält
- Glossar

Verdächtige Dateien an Trend Micro senden

Wenn Sie bei einer Datei eine Vireninfektion o. ä. vermuten, die Scan Engine diese Datei jedoch nicht entdeckt oder gesäubert hat, können Sie die Datei an Trend Micro senden. Weitere Informationen finden Sie auf der folgenden Website:

http://subwiz.trendmicro.com/SubWiz

Außerdem können Sie an Trend Micro URLs von Websites schicken, hinter denen Sie eine Phishing-Website oder einen Infektionsüberträger vermuten, d. h. eine Quelle von Internet-Bedrohungen, wie z. B. Spyware und Viren.

- Senden Sie eine E-Mail an die folgende Adresse, und geben Sie als Betreff "Phish or Disease Vector" an.

  virusresponse@trendmicro.com

- Sie können auch das webbasierte Formular verwenden unter:

  http://subwiz.trendmicro.com/SubWiz

Anregungen und Kritik

Das Trend Micro Team ist stets bemüht, die Dokumentation zu verbessern. Falls Sie Fragen, Kommentare oder Vorschläge zu diesem oder einem anderen Dokument von Trend Micro haben, navigieren Sie zur folgenden Site:

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

Anhang A

Verteilungsbeispiel

Dieser Abschnitt veranschaulicht, wie OfficeScan ausgehend von der Netzwerktopologie und den verfügbaren Netzwerkressourcen verteilt wird. Dieses Beispiel können Sie als Grundlage für die Verteilungsplanung von OfficeScan in Ihrem Unternehmen verwenden.

Basisnetzwerk

In Abbildung A-1 ist ein Basisnetzwerk dargestellt, in dem der OfficeScan Server und die Clients 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 ein Computer, der die OfficeScan Systemvoraussetzungen erfüllt und über die entsprechenden Ressourcen verfügt, optimal für die Installation des OfficeScan Servers.

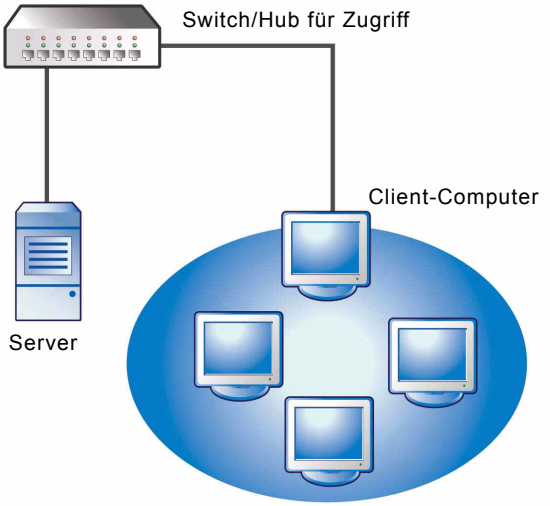


ABBILDUNG A-1. Topologie eines Basisnetzwerks

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 einen größeren Aufschluss über die ideale Verteilung von OfficeScan. Abbildung A-2 stellt eine Netzwerktopologie mit mehreren Standorten dar.

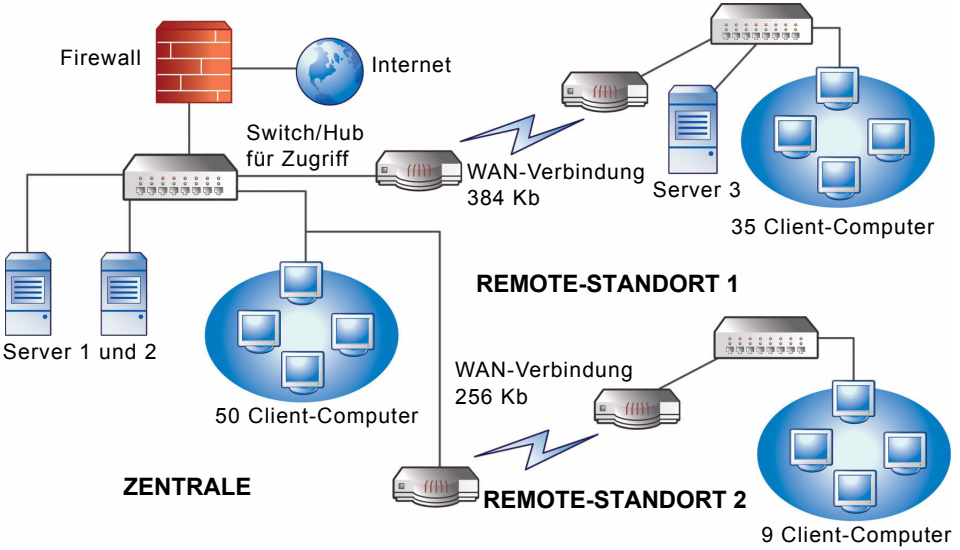


ABBILDUNG A-2. Netzwerktopologie mit mehreren Standorten

Angaben zum Netzwerk:

- Die durchschnittliche Auslastung der WAN-Verbindung von Remote-Standort 1 beträgt während der Geschäftszeiten 70 Prozent. An diesem Standort gibt es 35 Clients.
- Die durchschnittliche Auslastung der WAN-Verbindung von Remote-Standort 2 beträgt während der Geschäftszeiten 40 Prozent. An diesem Standort gibt es 9 Clients.

- Server 3 fungiert nur als Datei- und Druckerserver für die Gruppe am Remote-Standort 1. Dieser Computer eignet sich möglicherweise für die Installation eines OfficeScan Servers. Der zusätzliche Verwaltungsaufwand lohnt sich jedoch wahrscheinlich nicht. Auf allen Servern wird Windows Server 2003 ausgeführt. Im Netzwerk wird Active Directory eingesetzt, dient jedoch hauptsächlich zur Authentifizierung im Netzwerk.
- Auf allen Clients in der Zentrale sowie am Remote-Standort 1 und 2 wird Windows Server 2003 oder Windows XP ausgeführt.

Aufgaben:

1. Geben Sie den Computer an, auf dem der OfficeScan Server installiert wird. Informationen über das Installationsverfahren finden Sie unter *Erstinstallation des OfficeScan Servers durchführen* auf Seite 2-2.
2. Ermitteln Sie die verfügbaren Installationsmethoden für den Client, und schließen Sie Methoden aus, die die Voraussetzungen nicht erfüllen. Weitere Informationen zu den Client-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 Computer übertragen werden, kann diese Option nicht verwendet werden.
   - Remote-Installation über die Webkonsole

     Diese Methode eignet sich für alle über das LAN verbundenen Computer im Hauptbüro. Da auf all diesen Computern Windows Server 2003 ausgeführt wird, lässt sich das Paket ganz einfach auf die Computer verteilen.

     Aufgrund der geringen Verbindungsgeschwindigkeit zwischen zwei Remote-Standorten kann sich diese Verteilungsmethode negativ auf die verfügbare Bandbreite auswirken, falls OfficeScan während der Geschäftszeit installiert wird. 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 Computern kann OfficeScan jedoch nicht erfolgreich installiert werden.

- Verteilung des Client-Pakets

  Die Installation mit dem Client Packager scheint die sinnvollste Option für die Verteilung auf einen Remote-Standort zu sein. 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 Computer am besten.

Verteilung im Hauptbüro

Im Hauptbüro lässt sich der Client 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 ist die Erstellung eines Client-Pakets im Microsoft Installer Package Format (MSI), das dann im DFS bereitgestellt wird. Weitere Informationen zu dem Verfahren finden Sie im *Administratorhandbuch*. Da das Paket beim nächsten zeitgesteuerten Update auf den Server 3 repliziert wird, wirkt sich die Verteilung des Client-Pakets nur in sehr geringem Maß auf die Bandbreite aus.

Sie können ein Client-Paket auch über Active Directory verteilen. Weitere Informationen finden Sie im *Administratorhandbuch*.

Die Auswirkung von Komponenten-Updates im WAN möglichst gering halten:

1. Bestimmen Sie einen Client, der am Remote-Standort 1 die Funktion des Update-Agents übernimmt.
   a. Öffnen Sie hierfür die Webkonsole, und navigieren Sie zu **Netzwerkcomputer > Client-Verwaltung**.
   b. Wählen Sie in der Client-Hierarchie den Client aus, der die Funktion des Update-Agents übernimmt, und klicken Sie auf **Einstellungen > Update-Agent Einstellungen**.
2. Wählen Sie am Remote-Standort 1 die Clients aus, deren Komponenten über den Update-Agent aktualisiert werden.
   a. Navigieren Sie zu **Updates > Netzwerkcomputer > Update-Adresse**.
   b. Wählen Sie **Benutzerdefinierte Update-Adresse**, und klicken Sie auf **Hinzufügen**.
   c. Geben Sie in dem daraufhin angezeigten Fenster den IP-Adressbereich der Computer am 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. Während der Geschäftszeiten stehen jedoch 60 Prozent der Bandbreite zur Verfügung. Wenn die Bandbreite während der Geschäftszeiten zu 40 Prozent ausgelastet ist, steht eine Bandbreite von ca. 154 Kb/s zur Verfügung.

Am besten lässt sich der OfficeScan Client an diesem Standort mit demselben Client-Paket im MSI Format wie an Remote-Standort 1 installieren. Da jedoch an diesem Standort kein Server vorhanden ist, kann das verteilte Dateisystem (DFS) nicht verwendet werden.

Eine Möglichkeit besteht in der Verwendung von Management-Tools anderer Hersteller, mit denen der Administrator Freigabeverzeichnisse auf Remote-Computern erstellen oder konfigurieren kann, ohne physisch auf diese Computer zuzugreifen. Nachdem das Freigabeverzeichnis auf einem einzelnen Computer erstellt wurde, ist für das Kopieren des Client-Pakets auf das Verzeichnis weniger Aufwand erforderlich, als für die Installation des Clients auf neun Computern.

Sie können eine weitere Active Directory Richtlinie verwenden, die DFS Freigabe jedoch wieder nicht als Adresse angeben.

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 gering zu halten, können Sie auch einen Client als Update-Agent bestimmen. Weitere Informationen finden Sie unter *Verteilung am Remote-Standort 1* auf Seite A-5.

Anhang B

Nicht mehr verfügbare OfficeScan Funktionen

Dieser Abschnitt enthält eine Liste mit Funktionen aus Vorgängerversionen von OfficeScan, die in dieser Version nicht mehr verfügbar sind.

TABELLE B-1. Nicht mehr verfügbare OfficeScan Funktionen

FUNKTION	STATUS IN OFFICESCAN 10.6
OfficeScan Watchdog	Die Funktion "OfficeScan Watchdog" (Neustart von OfficeScan Client-Diensten, die unerwartet nicht mehr reagieren) wird vom OfficeScan Client durchgeführt. Die Einstellungen für den Neustart des Dienstes werden auf der Webkonsole konfiguriert.

Index

V

W