Trend Micro Apex One™

Service Pack 1 Patch 4

Handbuch für Installation und Upgrade

Für Unternehmen und mittelständische Betriebe

Dokument-Nr.: APGM38866/191126

Release-Datum: März 2025

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

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

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

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

Bewerten Sie diese Dokumentation auf der folgenden Website:

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

Datenschutz und Offenlegung persönlicher Daten

Einige Funktionen, die in Trend Micro Produkten zur Verfügung stehen, erfassen und senden Feedback hinsichtlich Produktnutzungs- und Ermittlungsinformationen an Trend Micro. Einige dieser Informationen werden in bestimmten Rechtsordnungen und im Rahmen von bestimmten Vorschriften als persönliche Daten betrachtet. Wenn Sie nicht möchten, dass Trend Micro persönliche Daten erfasst, müssen Sie die entsprechenden Funktionen deaktivieren.

Über den folgenden Link erhalten Sie Informationen zu den Daten, die Trend Micro Apex One erfasst, sowie detaillierte Anweisungen zur Deaktivierung der speziellen Funktionen, die Auswirkungen auf die Informationen haben.

https://success.trendmicro.com/data-collection-disclosure

Die von Trend Micro gesammelten Daten unterliegen den im Trend Micro Datenschutzhinweis angegebenen Bedingungen:

https://www.trendmicro.com/privacy

Inhaltsverzeichnis

Vorwort

Kapitel 1: Planung der Trend Micro Apex One Installation und Aktualisierung

Kapitel 2: Installation von Trend Micro Apex One

Kapitel 3: Trend Micro Apex One upgraden

Kapitel 4: Aufgaben nach der Installation

Kapitel 5: Deinstallieren von Trend Micro Apex One

Kapitel 6: Ressourcen zur Fehlerbehebung

Kapitel 7: Technischer Support

Anhang A: Beispielbereitstellung

Stichwortverzeichnis

Vorwort

Vorwort

Willkommen im Trend Micro Apex One™*Installations- und Upgrade-Handbuch*. Dieses Dokument behandelt die Anforderungen und Verfahren zur Installation des Trend Micro Apex One-Servers und zur Aktualisierung des Servers und Security Agents.

Themen in diesem Kapitel:

Hinweis

Weitere Informationen zur Installation von Security Agents finden Sie im *Administratorhandbuch*.

Trend Micro Apex One Dokumentation

Die Trend Micro Apex One Dokumentation umfasst Folgendes:

TABELLE 1. Trend Micro Apex One Dokumentation

DOKUMENTATION	BESCHREIBUNG
Installations- und Upgrade-Handbuch	Ein PDF-Dokument mit einer Beschreibung der Anforderungen und Verfahren zum Installieren des Trend Micro Apex One Servers sowie zum Aktualisieren des Servers und der Agents **Hinweis** Das Installations- und Upgrade-Handbuch enthält möglicherweise keine Informationen zu Nebenversionen, Service Packs oder Patches.
Systemvoraussetzungen	Ein PDF-Dokument, in dem die Mindest- und die empfohlenen Systemanforderungen für die Installation des Trend Micro Apex One Servers und die Aktualisierung des Servers und der Agents beschrieben werden
Administratorhandbuch	Ein PDF-Dokument mit Informationen über die ersten Schritte, die Verfahren zur Security Agent-Installation sowie über die Trend Micro Apex One Server- und Agent-Verwaltung
Hilfe	Im WebHelp- oder CHM-Format erstellte HTML-Dateien, die Anleitungen, allgemeine Benutzerhinweise und feldspezifische Informationen enthalten. Auf die Hilfe kann über die Trend Micro Apex One Server- und Agent-Konsolen sowie über das Trend Micro Apex One 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
Wissensdatenbank	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://success.trendmicro.com

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

https://docs.trendmicro.com/de-de/enterprise/apex-one.aspx

Zielgruppe

Die Trend Micro Apex One Dokumentation ist für die folgenden Benutzergruppen gedacht:

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

Dokumentationskonventionen

Die Dokumentation verwendet die folgenden Konventionen:

TABELLE 2. Dokumentationskonventionen

KONVENTION	BESCHREIBUNG
GROSSSCHRIFT	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Schaltflächen, Registerkarten und Optionen
Kursivdruck	Verweise auf andere Dokumente
`Schreibmaschinenschrift`	Muster für Befehlszeilen, Programmcode, Internet-Adressen, Dateinamen und Programmanzeigen
Navigation > **Pfad**	Der Navigationspfad zu einem bestimmten Fenster **Datei** > **Speichern** bedeutet beispielsweise, dass Sie in der Benutzeroberfläche im Menü **Datei** auf **Speichern** klicken

Konvention	Beschreibung
 **Hinweis**	Konfigurationshinweise
 **Tipp**	Empfehlungen oder Vorschläge
 **Wichtig**	Informationen zu den erforderlichen oder standardmäßigen Konfigurationseinstellungen und Produktbeschränkungen
 **Warnung!**	Wichtige Aktionen und Konfigurationsoptionen

Begriffe

Die folgende Tabelle enthält die offizielle Terminologie, die innerhalb der Trend Micro Apex One Dokumentation verwendet wird:

Tabelle 3. Trend Micro Apex One Terminologie

Begriffe	Beschreibung
Security Agent	Das Trend Micro Apex One Agent Programm
Agent-Endpunkt	Der Endpunkt, auf dem der Security Agent installiert ist
Agent-Benutzer (oder Benutzer)	Die Person, die den Security Agent auf dem Agent-Endpunkt verwaltet
Server	Das Trend Micro Apex One Server-Programm.
Server-Computer	Der Endpunkt, auf dem der Trend Micro Apex One Server installiert ist
Administrator (oder Trend Micro Apex One Administrator)	Die Person, die den Trend Micro Apex One Server verwaltet.

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

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

Begriffe	Beschreibung

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

Agent der intelligenten Suche	Ein Security Agent wurde so konfiguriert, dass die intelligente Suche verwendet wird.
Agent der herkömmlichen Suche	Ein Security Agent wurde so konfiguriert, dass die herkömmliche Suche verwendet wird.
Dual-stack	Elemente, die sowohl über IPv4- als auch IPv6-Adressen verfügen. Beispiel: • Endpunkte mit IPv4- und IPv6-Adressen • Security Agents auf Dual-Stack-Endpunkten installiert • Update-Agents, die Updates an Agents verteilen • Ein Dual-Stack-Proxy-Server, wie etwa DeleGate, kann zwischen IPv4- und IPv6-Adressen konvertieren
Reines IPv4	Ein Gerät, das nur über IPv4-Adressen verfügt
Reines IPv6	Ein Gerät, das nur über IPv6-Adressen verfügt
Plug-in-Lösungen	Native Apex One Funktionen und Plug-in-Programme, die über Plug-in Manager bereitgestellt werden

Kapitel 1

Planung der Trend Micro Apex One Installation und Aktualisierung

Dieses Kapitel beschreibt die Vorbereitung und Vorinstallationsinformationen für die Installation und das Upgrade von Trend Micro Apex One™.

Wichtig

- Sie können keine Neuinstallation des Trend Micro Apex One-Servers auf dem Server-Computer mit installiertem Apex Central durchführen.
- Wenn Sie auf Trend Micro Apex One upgraden und Control Manager auf demselben Server-Computer installiert ist, hängt die Unterstützung für einen einzelnen Server-Computer für Trend Micro Apex One und Apex Central von den aktivierten Funktionen ab.

  Für weitere Informationen navigieren Sie zu https://success.trendmicro.com/dcx/s/solution/000267022?language=en_US.

Themen in diesem Kapitel:

Apex One Server Anforderungen

Die folgenden Themen skizzieren einige Überlegungen, die Sie anstellen sollten, bevor Sie den Trend Micro Apex One-Server installieren oder aktualisieren.

Unterstützung des Betriebssystems

Die folgende Tabelle zeigt die Unterstützung des Betriebssystems und die Migrationsverfügbarkeit für den Trend Micro Apex One-Server.

Tipp

Trend Micro empfiehlt, dass Sie ein vollständiges Windows Update auf dem Zielserver-Computer durchführen, bevor Sie den Trend Micro Apex One-Server installieren oder aktualisieren

Betriebssystem	Apex One	Apex One Service Pack 1
Windows Server 2012	Ja	Ja
Windows Server 2012 R2	Ja	Ja
Windows Server 2016	Ja	Ja
Windows Server 2019	Ja	Ja
Windows Server 2022	Ja	Ja

Wichtig

Trend Micro Apex One bietet keine weitere Unterstützung für den Apache Server.

SQL Server-Anforderungen

Trend Micro Apex One stellt den Support für das ältere Codebase-Datenbankmodell ein, das von früheren OfficeScan-Versionen verwendet wurde. Sie können Ihren eigenen SQL Server vor der Installation vorbereiten oder das Trend Micro Apex One Setup-Programm SQL Server 2016 SP2 Express während des Serverinstallationsprozesses installieren lassen.

Wichtig

Nach dem Upgrade auf Trend Micro Apex One erscheint der ältere **Datenbanksicherung**-Bildschirm, der zur Sicherung der älteren Codebase-Datenbank verwendet wurde, nicht mehr in der Trend Micro Apex One-Webkonsole.

Die folgende Tabelle zeigt die Datenbankunterstützung und Migrationsverfügbarkeit für den Trend Micro Apex One-Server auf.

Datenbank	Apex One	Apex One mit Endpoint Sensor
Codebase	-	-
SQL Server 2014	Ja	-
SQL Server 2016	Ja	-
SQL Server 2016 SP2	Ja	Ja
SQL Server 2016 Express oder höher	Ja	-
SQL Server 2017	Ja	Ja
SQL Server 2019	Ja	Ja
SQL Server 2022	Ja	Ja

Hinweis

Beim Installieren oder Aktualisieren auf Trend Micro Apex One mit der Endpoint Sensor-Funktion müssen Sie **Full-Text and Semantic Extractions for Search** auf einer unterstützten SQL Server-Version aktivieren, bevor Sie mit dem Installationsprozess beginnen.

Weitere Informationen zu den Anforderungen des Endpoint Sensors finden Sie unter *Apex One Endpoint Sensor auf Seite 1-12*.

Security Agent Support

In der folgenden Tabelle sind die Anforderungen und empfohlenen Einstellungen für Security Agent aufgeführt.

Wichtig

Ressourcenspitzen können auftreten, wenn eine große Anzahl von Anwendungen gleichzeitig auf einem Endpunkt ausgeführt wird. Wenn der Zielendpunkt bereits wenig Speicher oder Festplattenspeicher hat, empfiehlt Trend Micro, die erforderlichen Hardwarekomponenten vor der Security Agent-Installation oder dem Upgrade von Apex One aufzurüsten.

Trend Micro empfiehlt, die minimalen Systemvoraussetzungen als dedizierte Ressourcen für das Security Agent-Programm zuzuweisen, um eine angemessene Leistung während umfangreicher Scanvorgänge sicherzustellen.

Vorgang	Beschreibung
HTTPS-Unterstützung	HTTPS-Kommunikation zwischen dem Trend Micro Apex One Server und dem Security Agent ist erforderlich. **Wichtig** Sie können nicht auf den Trend Micro Apex OneService Pack 1 Patch 4-Server upgraden, wenn Sie während des Upgrade-Vorgangs nicht die Option zur Erlaubnis der HTTPS-Kommunikation auswählen.
Kommunikation zwischen Server und Agents	Trend Micro empfiehlt, die AES-256-Verschlüsselung für Kommunikation zwischen dem Trend Micro Apex One-Server und Security Agents auf dem **Globale Agent-Einstellungen**-Bildschirm nach Abschluss der Installation zu aktivieren.
Unterstützung des Betriebssystems	Trend Micro Apex One unterstützt nur Endpunkte, die bestimmte Windows-Betriebssysteme ausführen. Für eine vollständige Liste der Trend Micro Apex One-Server und Security Agent-Anforderungen, siehe die *Systemvoraussetzungen*-Dokumente. Während einer Upgrade-Installation überprüft das Setup-Programm, ob alle Endpunkte, die an den Server berichten, ein unterstütztes Betriebssystem ausführen. Wenn das Setup-Programm ein nicht unterstütztes Betriebssystem erkennt, kann das Upgrade nicht fortgesetzt werden. Bevor Sie auf den Trend Micro Apex One-Server upgraden, verschieben Sie alle Agenten, die auf nicht unterstützten Betriebssystemen installiert sind, auf einen älteren OfficeScan-Server oder deinstallieren Sie das Agentenprogramm.

Installationsüberprüfung

Die folgende Tabelle zeigt, wie die erfolgreiche Durchführung des Trend Micro Apex One-Servers und Security Agent überprüft werden kann.

Vorgang	Beschreibung
Trend Micro Apex One Server	Überprüfen Sie, ob die folgenden Dienste ausgeführt werden: • Apex One Master-Dienst (`OfcService.exe`) • Apex One Plug-in Manager (`OfcAoSMgr.exe`) • Apex One Active Directory-Dienst (`OSCEIntegrationService.exe`) • Apex One-Protokollempfangsdienst (`OfcLogReceiverSvc.exe`) • Apex One Deep Discovery Service (`ofcDdaSvr.exe`) • Apex One-Datenbankprozess (`DbServer.exe`)

Security Agent	Überprüfen Sie, ob die folgenden Dienste ausgeführt werden:
	• Für Desktop-Plattformen:
	  • Apex One Gemeinsames Client Solution Framework-Dienst (`TmCCSF.exe`)
	  • Apex One NT Listener (`Tmlisten.exe`)
	  • Apex One NT-Echtzeitscan (`Ntrtscan.exe`)
	  • Apex One NT Firewall (`Tmpfw.exe`)
	  • Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)
	• Für Serverplattformen:
	  • Apex One Gemeinsames Client Solution Framework-Dienst (`TmCCSF.exe`)
	  • Apex One NT Listener (`Tmlisten.exe`)
	  • Apex One NT-Echtzeitscan (`Ntrtscan.exe`)

Erweiterte Funktionsanforderungen für Apex Central

Wenn Sie planen, die zusätzlichen Sicherheitsfunktionen zu implementieren, die durch die Integration mit der Trend Micro Apex Central Webkonsole verfügbar sind, stellen Sie sicher, dass Sie die

Auswirkungen der zusätzlichen Funktionen auf die Trend Micro Apex One Systemvoraussetzungen verstehen. Die folgenden Themen skizzieren die Systemvoraussetzungen, Installations- und Upgrade-Informationen sowie alle zusätzlichen Informationen zu den erweiterten Produktfunktionen.

Apex One Application Control

TABELLE 1-1. Voraussetzungen

VORGANG	VORAUSSETZUNGEN
Systemvoraussetzungen	Gleich wie Trend Micro Apex One-Server und Security Agent
Lizenz	• In der Apex One Vollversion für Windows- und Mac-Lizenzen enthalten • Eine bestehende Trend Micro Endpoint Application Control-Lizenz (aktiviert in Trend Micro Apex Central)
Apex Central-Registrierung	Erforderlich für die Lizenzierung und Security Agent Richtlinienbereitstellung

Vorgang	Voraussetzungen
Kompatibilität mit Trend Micro Endpoint Application Control	• Server: Der Trend Micro Apex One-Server mit Application Control kann auf demselben Server wie Trend Micro Endpoint Application Control existieren (nicht empfohlen). **Wichtig** Die Servereinstellungen von Trend Micro Endpoint Application Control sind nicht mit der Apex One Application Control-Funktion kompatibel. Sie müssen alle Richtlinien manuell über die Trend Micro Apex Central Webkonsole konfigurieren. • Agent: Sobald Sie eine Application Control-Richtlinie auf dem Apex One Security Agent bereitstellen, deinstalliert der Security Agent automatisch jeden vorhandenen Trend Micro Endpoint Application Control-Agent, bevor die Apex One Application Control-Einstellungen angewendet werden.

Tabelle 1-2. Informationen zur Neuinstallation

Typ	Beschreibung
Server	Das Apex One-Setup-Programm installiert die Application Control-Funktion automatisch während der normalen Trend Micro Apex One Serverinstallation. Nachdem überprüft wurde, dass der Aktivierungscode Application Control enthält, startet Trend Micro Apex One das **Trend Micro Application Control Dienst** auf dem Trend Micro Apex One-Server-Computer.
Agent	Das Security Agent-Programm enthält den Application Control-Dienst, installiert ihn jedoch nicht sofort während der normalen Security Agent-Installation. Um die Apex One Application Control-Funktion auf dem Security Agent zu installieren, müssen Sie eine Application Control-Richtlinie von der Trend Micro Apex Central-Webkonsole aktivieren und bereitstellen. Sobald Security Agent die Application Control-Einstellungen erhält, installiert Security Agent die Application Control-Funktion.

TABELLE 1-3. Upgrade-Hinweise

TYP	BESCHREIBUNG
OfficeScan Server	Die Trend Micro Apex One-Lizenz umfasst nur die Aktivierung von Application Control für Neuinstallationen. Wenn Sie von einer vorherigen Version des OfficeScan-Servers upgraden, müssen Sie Ihren Vertriebsmitarbeiter kontaktieren, um eine neue Lizenz zu erhalten, die die Application Control-Funktion aktiviert. Das Apex One-Setup-Programm installiert die Apex One Application Control-Funktion automatisch während der normalen Trend Micro Apex One Serverinstallation.
Trend Micro Endpoint Application Control Server	Trend Micro Apex One unterstützt kein Upgrade oder die Migration von Einstellungen vom eigenständigen Trend Micro Endpoint Application Control-Server zur Apex One Application Control-Funktion. **Wichtig** Die Servereinstellungen von Trend Micro Endpoint Application Control sind nicht mit der Apex One Application Control-Funktion kompatibel. Sie müssen alle Richtlinien manuell über die Trend Micro Apex Central Webkonsole konfigurieren.
Trend Micro Endpoint Application Control-Agent	Trend Micro Apex One unterstützt kein Upgrade des Trend Micro Endpoint Application Control-Agentenprogramms auf Apex One Security Agent. Wenn Sie Apex One Security Agent auf einem Endpunkt mit installiertem Trend Micro Endpoint Application Control-Agent installieren und eine Application Control-Richtlinie von der Trend Micro Apex Central-Konsole bereitstellen, deinstalliert Security Agent automatisch den Trend Micro Endpoint Application Control-Agent und installiert die Apex One Application Control-Funktion.

Tabelle 1-4. Installationsüberprüfung

Typ	Beschreibung

Trend Micro Apex One Server	Nach der Installation des Trend Micro Apex One-Servers mit einer gültigen Lizenz für die Funktion können Sie Folgendes überprüfen:
	• Der **Trend Micro Application Control Dienst** läuft auf dem Trend Micro Apex One Server Computer.
	• Der Application Control-Dienstordner befindet sich auf dem Trend Micro Apex One-Server-Computer an folgendem Ort:
	`<Server installation folder>/iServiceSvr/iAC`
	• Die Installationsprotokolldatei des Application Control-Dienstes befindet sich auf dem Trend Micro Apex One-Server-Computer an folgendem Ort:
	`%windir%/OFCMAS.LOG`

Security Agent Endpunkt	Nach der Installation von Security Agent und der Bereitstellung einer Application Control-Richtlinie von Trend Micro Apex Central können Sie Folgendes überprüfen: • Der **Trend Micro Application Control Service (Agent)** läuft auf dem Security Agent Endpunkt. • Der Ordner des Application Control-Dienstes befindet sich auf dem Endpunkt an folgendem Ort: `<Security Agent installation folder>/iService/iAC`

Tabelle 1-5. Konfiguration nach der Installation

Einstellungen	Beschreibung
Server	Gehen Sie in der Trend Micro Apex Central Webkonsole zu **Administration** > **Updates** > **Manuelles Update** und stellen Sie sicher, dass Sie die **Pattern für Certified Safe Software** herunterladen.
Security Agent Endpunkt	Gehen Sie in der Trend Micro Apex Central-Webkonsole zu **Richtlinien** > **Policy Management** und fügen Sie die **Application Control-Einstellungen** für die Apex One Security Agent-Richtlinien hinzu oder ändern Sie sie nach Bedarf.

Apex One Endpoint Sensor

Endpoint Sensor ist für Kunden verfügbar, die die Apex One™: Endpoint Sensor-Lizenz erworben haben und mit Trend Micro Apex Central integrieren. Sie können die Endpoint Sensor-Richtlinieneinstellungen nur über die Trend Micro Apex Central Webkonsole konfigurieren.

Bevor Sie den Trend Micro Apex One-Server installieren, stellen Sie sicher, dass Sie Zugriff auf die richtige Version von SQL Server haben. Wenn Sie die Endpoint Sensor-Funktion nutzen möchten, müssen Sie bestimmte SQL Server-Versionen installieren und vorbereiten.

Hinweis

Wenn Sie den Endpoint Sensor-Dienst nicht installieren und einen unterstützten SQL Server mit **Full-Text and Semantic Extractions for Search** aktiviert auswählen, ist die einzige Möglichkeit, Endpoint Sensor später zu verwenden, zum Bildschirm **Uninstall or change a program** von Windows **Systemsteuerung** zu gehen.

Wählen Sie den Trend Micro Apex One Server aus und klicken Sie auf **Ändern**.

- *Voraussetzungen auf Seite 1-13*
- *Informationen zur Neuinstallation auf Seite 1-15*
- *Upgrade-Hinweise auf Seite 1-16*

TABELLE 1-6. Voraussetzungen

VORGANG	VORAUSSETZUNGEN
Systemvoraussetzungen	Server: Gleiche Betriebssystemanforderungen wie der Trend Micro Apex One-Server (SQL Server-Anforderungen unterscheiden sich) Endpunkte: Gleiche Systemvoraussetzungen wie der Apex One Security Agent **Wichtig** Diese Funktion wird offiziell nur auf den folgenden Plattformen unterstützt: • Windows 10 • Windows 11
Lizenz	• Apex One Endpoint Sensor-Lizenz (aktiviert in Trend Micro Apex Central) • Eine bestehende Trend Micro Endpoint Sensor-Lizenz (aktiviert in Trend Micro Apex Central)
Apex Central-Registrierung	Erforderlich für die Lizenzierung und Security Agent Richtlinienbereitstellung

VORGANG	VORAUSSETZUNGEN

Kompatibilität mit Trend Micro Endpoint Sensor	• Server: Wenn Sie den Trend Micro Apex One-Server mit der Apex One Endpoint Sensor-Funktion auf demselben Server wie den eigenständigen Trend Micro Endpoint Sensor-Server installieren (nicht empfohlen):
	  • Der eigenständige Trend Micro Endpoint Sensor-Server ist deaktiviert.
	  • Die eigenständigen Trend Micro Endpoint Sensor-Dateien und die Datenbank verbleiben auf dem Server-Computer und können die Leistung beeinträchtigen.
	
	Wichtig
	Standalone Trend Micro Endpoint Sensor-Servereinstellungen sind nicht kompatibel mit der Apex One Endpoint Sensor-Funktion. Sie müssen alle Richtlinien manuell über die Trend Micro Apex Central Webkonsole konfigurieren.
	
	• Agent: Sobald Sie eine Endpoint Sensor-Richtlinie auf dem Apex One Security Agent bereitstellen, deinstalliert der Security Agent automatisch jeden vorhandenen eigenständigen Trend Micro Endpoint Sensor-Agent, bevor die Apex One Endpoint Sensor-Einstellungen angewendet werden.

Redis-Dienst	Der Trend Micro Apex One-Server-Computer darf keinen vorhandenen Redis-Dienst installiert haben. Sie müssen jeden vorhandenen Redis-Dienst deinstallieren und dem Installationsprogramm erlauben, einen neuen Dienst zu installieren. Überprüfung Nachdem Sie auf **Weiter** auf dem **Installation von Endpoint Sensor**-Bildschirm geklickt haben

VORGANG	VORAUSSETZUNGEN
SQL Server-Version	• SQL Server 2022 • SQL Server 2019 • SQL Server 2017 • SQL Server 2016 SP2 **Hinweis** Diese Funktion unterstützt keine SQL Server Express-Versionen. Überprüfung Nach dem Klicken auf **Weiter** auf dem Bildschirm **Setup der Apex One Datenbank**
Datenbankkonfiguration	**Full-Text and Semantic Extractions for Search** aktiviert Weitere Informationen zum Aktivieren von **Full-Text and Semantic Extractions for Search** finden Sie in Ihrer SQL Server-Dokumentation. Überprüfung Nach dem Klicken auf **Weiter** auf dem Bildschirm **Setup der Apex One Datenbank**
	Zugriffsrechte auf die **tempdb**-Datenbank für Datenbankwartungsfunktionen Überprüfung Keine

TABELLE 1-7. Informationen zur Neuinstallation

TYP	BESCHREIBUNG
Server	Das Apex One-Setup-Programm bietet die Möglichkeit, die Apex One Endpoint Sensor-Funktion während der normalen Trend Micro Apex One Serverinstallation zu installieren.

Typ	Beschreibung
Agent	Das Security Agent-Programm umfasst den Endpoint Sensor-Dienst, installiert ihn jedoch nicht sofort während der normalen Security Agent-Installation. Um den Endpoint Sensor-Dienst auf dem Security Agent zu installieren, müssen Sie eine Endpoint Sensor-Richtlinie von der Trend Micro Apex Central-Webkonsole aktivieren und bereitstellen. Sobald der Security Agent die Endpoint Sensor-Einstellungen erhält, installiert der Security Agent den Endpoint Sensor-Dienst.

Tabelle 1-8. Upgrade-Hinweise

Typ	Beschreibung
OfficeScan Server	Das Apex One-Setup-Programm bietet die Möglichkeit, die Apex One Endpoint Sensor-Funktion während normaler Trend Micro Apex One-Server-Upgrades zu installieren.
Trend Micro Endpoint Sensor Server	Trend Micro Apex One unterstützt kein Upgrade oder keine Einstellungen-Migration vom eigenständigen Trend Micro Endpoint Sensor-Server zur Apex One Endpoint Sensor-Funktion. **Wichtig** Standalone Trend Micro Endpoint Sensor-Servereinstellungen sind nicht kompatibel mit der Apex One Endpoint Sensor-Funktion. Sie müssen alle Richtlinien manuell über die Trend Micro Apex Central Webkonsole konfigurieren.
Trend Micro Endpoint Sensor-Agent	Trend Micro Apex One unterstützt kein Upgrade des Trend Micro Endpoint Sensor-Agentenprogramms auf Apex One Security Agent. Wenn Sie das Apex One Security Agent auf einem Endpunkt mit dem eigenständigen Trend Micro Endpoint Sensor-Agenten installieren und eine Endpoint Sensor-Richtlinie von der Trend Micro Apex Central-Konsole bereitstellen, deinstalliert das Security Agent automatisch den Trend Micro Endpoint Sensor-Agenten und installiert die Apex One Endpoint Sensor-Funktion.

Managed Detection and Response Service

Der Managed Detection and Response (MDR) Service ist nur verfügbar, wenn Sie den Endpoint Sensor Service erworben und den MDR Service über einen Vertriebsmitarbeiter abonniert haben. Die Systemvoraussetzungen, Bereitstellung und Aktualisierung des MDR Services folgen dem Endpoint Sensor Service, mit Ausnahme der folgenden zusätzlichen Aufgabenanforderungen.

Task	Zusätzlicher erforderlicher Festplattenspeicher
Bewertungsaufgabe	Wenn der MDR-Dienst eine Bewertungsaufgabe beginnt, werden zusätzliche 20 GB Festplattenspeicher (pro 100 Endpunkte) auf dem Trend Micro Apex One-Server benötigt, um die zusätzlichen Protokollinformationen zu verarbeiten.
Trend Micro Investigation Kit (TMIK)	Wenn der MDR-Dienst das TMIK bereitstellt, werden zusätzliche 40 GB Festplattenspeicher (pro 100 Endpunkte) auf dem Trend Micro Apex One-Server benötigt, um die zusätzlichen Protokollinformationen zu verarbeiten.

Apex One Vulnerability Protection

- *Voraussetzungen auf Seite 1-17*
- *Informationen zur Neuinstallation auf Seite 1-18*
- *Upgrade-Hinweise auf Seite 1-19*
- *Installationsüberprüfung auf Seite 1-20*
- *Konfiguration nach der Installation auf Seite 1-20*

Tabelle 1-9. Voraussetzungen

Vorgang	Voraussetzungen
Systemvoraussetzungen	Gleich wie Trend Micro Apex One-Server und Security Agent

Vorgang	Voraussetzungen
Lizenz	• In der Apex One Vollversion für Windows- und Mac-Lizenzen enthalten • Eine bestehende Trend Micro Vulnerability Protection-Lizenz (aktiviert in Trend Micro Apex Central)
Apex Central-Registrierung	Erforderlich für die Lizenzierung und Security Agent Richtlinienbereitstellung
Kompatibilität mit Trend Micro Vulnerability Protection	• Server: Der Trend Micro Apex One-Server mit Vulnerability Protection kann auf demselben Server wie Trend Micro Vulnerability Protection existieren (nicht empfohlen). • Agent: Sobald Sie eine Vulnerability Protection-Richtlinie auf dem Apex One Security Agent bereitstellen, deinstalliert der Security Agent automatisch jeden vorhandenen Trend Micro Vulnerability Protection-Agent, bevor die Apex One Vulnerability Protection-Einstellungen angewendet werden.
Kompatibilität mit anderen Trend Micro-Produkten	Die folgenden Trend Micro-Produkte sind nicht mit der Apex One Vulnerability Protection-Funktion kompatibel: • Deep Security Agent • Intrusion Defense Firewall-Agent Sie können die Apex One Vulnerability Protection-Funktion auf Security Agents nicht aktivieren, wenn auf Endpunkten ein inkompatibles Agentenprogramm installiert ist. Sie müssen das konfliktverursachende Programm deinstallieren, bevor Sie die Apex One Vulnerability Protection-Funktion aktivieren.

Tabelle 1-10. Informationen zur Neuinstallation

Typ	Beschreibung
Server	Das Apex One-Setup-Programm installiert die Apex One Vulnerability Protection-Funktion automatisch während der normalen Trend Micro Apex One-Serverinstallation. Nachdem überprüft wurde, dass der Aktivierungscode Vulnerability Protection enthält, startet Trend Micro Apex One das **Trend Micro Vulnerability Protection Dienst** auf dem Trend Micro Apex One-Server-Computer.

Typ	Beschreibung
Agent	Das Security Agent-Programm enthält die Apex One Vulnerability Protection-Funktion, installiert sie jedoch nicht sofort während der normalen Security Agent-Installation. Um die Vulnerability Protection-Funktion auf dem Security Agent zu installieren, müssen Sie eine Vulnerability Protection-Richtlinie von der Trend Micro Apex Central-Webkonsole aktivieren und bereitstellen. Sobald das Security Agent die Einstellungen für Vulnerability Protection erhält, installiert das Security Agent die Funktion Vulnerability Protection.

Tabelle 1-11. Upgrade-Hinweise

Typ	Beschreibung
OfficeScan Server	Die Trend Micro Apex One-Lizenz umfasst nur die Aktivierung von Vulnerability Protection für Neuinstallationen. Wenn Sie von einer vorherigen Version des OfficeScan-Servers upgraden, müssen Sie sich an Ihren Vertriebsmitarbeiter wenden, um eine neue Lizenz zu erhalten, die die Vulnerability Protection-Funktion aktiviert. Das Apex One-Setup-Programm installiert die Apex One Vulnerability Protection-Funktion automatisch während der normalen Trend Micro Apex One-Serverinstallation.
Trend Micro Vulnerability Protection Server	Trend Micro Apex One unterstützt keine Aktualisierung oder Einstellungenmigration vom eigenständigen Trend Micro Vulnerability Protection-Server zur Apex One Vulnerability Protection-Funktion.
Trend Micro Vulnerability Protection-Agent	Trend Micro Apex One unterstützt kein Upgrade des Trend Micro Vulnerability Protection-Agentenprogramms auf Apex One Security Agent. Wenn Sie Apex One Security Agent auf einem Endpunkt mit installiertem Trend Micro Vulnerability Protection-Agent installieren und eine Vulnerability Protection-Richtlinie von der Trend Micro Apex Central-Konsole bereitstellen, deinstalliert Security Agent automatisch den Trend Micro Vulnerability Protection-Agent und installiert die Apex One Vulnerability Protection-Funktion.

TABELLE 1-12. Installationsüberprüfung

TYP	BESCHREIBUNG

Trend Micro Apex One Server	Nach der Installation des Trend Micro Apex One-Servers mit einer gültigen Lizenz für die Funktion können Sie Folgendes überprüfen:
	• Der **Trend Micro Vulnerability Protection Dienst** läuft auf dem Trend Micro Apex One Server Computer.
	• Der Vulnerability Protection-Dienstordner befindet sich auf dem Trend Micro Apex One-Server-Computer an folgendem Speicherort:
	`<Server installation folder>/iServiceSvr/iVP`
	• Die Installationsprotokolldatei des Vulnerability Protection-Dienstes befindet sich auf dem Trend Micro Apex One-Server-Computer an folgendem Speicherort:
	`<Server installation folder>/iServiceSvr/iVP/install.log`

Security Agent Endpunkt	Nach der Installation von Security Agent und der Bereitstellung einer Vulnerability Protection-Richtlinie von Trend Micro Apex Central können Sie Folgendes überprüfen: • Der **Trend Micro Vulnerability Protection Service (Agent)** läuft auf dem Security Agent Endpunkt. • Der Ordner des Vulnerability Protection-Dienstes befindet sich auf dem Endpunkt an folgendem Ort: `<Security Agent installation folder>/iService/iVP`

TABELLE 1-13. Konfiguration nach der Installation

EINSTELLUNGEN	BESCHREIBUNG
Server	Gehen Sie in der Trend Micro Apex Central Webkonsole zu **Administration** > **Updates** > **Zeitgesteuertes Update** und stellen Sie sicher, dass Sie automatische Updates des **Vulnerability Protection-Pattern** planen.
Security Agent Endpunkt	Gehen Sie in der Trend Micro Apex Central-Webkonsole zu **Richtlinien** > **Policy Management** und fügen Sie die **Vulnerability Protection Settings** für die Apex One Security Agent-Richtlinien hinzu oder ändern Sie sie nach Bedarf.

Installations- und Upgrade-Checkliste

Das Setup fordert die folgenden Informationen an, wenn der Trend Micro Apex One-Server installiert oder aktualisiert wird.

Tabelle 1-14. Installations- und Upgrade-Checkliste

Installationsinformationen	Erforderliche Informationen während	
	Neuinstallation	Upgrade
Trend Micro Apex One Installationspfad Der Standardinstallationspfad des Servers ist: • `C:\Programme\Trend Micro\Apex One` • `C:\Programme (x86)\Trend Micro\Apex One` (für x64 Plattformen) Identifizieren Sie den Installationspfad oder verwenden Sie den Standardpfad. Wenn der Pfad nicht existiert, wird er von der Installation automatisch erstellt.	Ja	Nein
Proxy-Server-Einstellungen Wenn der Trend Micro Apex One-Server über einen Proxy-Server mit dem Internet verbunden ist, geben Sie Folgendes an: • Proxy-Typ (HTTP oder SOCKS 4) • Servername oder IP-Adresse • Port • Proxy-Authentifizierungsdaten	Ja	Nein

Installationsinformationen	Erforderliche Informationen während	
	Neuinstallation	Upgrade
Webserver-Einstellungen Der Webserver führt Webkonsole-CGIs aus und akzeptiert Befehle von Agents. Geben Sie Folgendes an: • HTTP-Port: Der Standardport ist 8080. Wenn Sie die IIS-Standardwebsite verwenden, überprüfen Sie den TCP-Port des HTTP-Servers. **Warnung!** Viele Hacker- und Virus/Malware-Angriffe, die über HTTP erfolgen, nutzen die Ports 80 und/oder 8080. Die meisten Organisationen verwenden diese Portnummern als Standard-TCP-Port für HTTP-Kommunikation. Verwenden Sie andere Portnummern, wenn die Standard-Portnummern derzeit in Gebrauch sind. Wenn sichere Verbindungen aktiviert werden: • Gültigkeitsdauer des SSL-Zertifikats • SSL-Port (Standard: 4343)	Ja	Nein

Registrierung
 	
Registrieren Sie das Produkt, um die Aktivierungscodes zu erhalten. Die folgenden Informationen sind erforderlich, um das Produkt zu registrieren:
 	
• Für zurückkehrende Benutzer:
 	
  • Online-Registrierungskonto (Anmeldename und Passwort)
 	
• Für Benutzer ohne Konto:
 	
  • Registrierungsschlüssel
	Ja	Ja

Installationsinformationen	Erforderliche Informationen während	
	Neuinstallation	Upgrade
Aktivierung Erhalten Sie den Aktivierungscode	Ja	Ja
Installation des integrierten Smart Protection Servers Bei der Installation des Integrierten Servers geben Sie Folgendes an: • Gültigkeitsdauer des SSL-Zertifikats • SSL-Port	Ja	Ja
Installiert den Security Agent	Ja	Nein
Kennwort für das Administratorkonto Die Einrichtung erstellt ein Root-Konto für die Anmeldung an der Webkonsole. Geben Sie Folgendes an: • Root-Konto-Passwort Verhindern Sie die unbefugte Deinstallation oder das Entladen von Security Agent, indem Sie Folgendes angeben: • Security Agent Deinstallations-/Entladepasswort	Ja	Nein
Security Agent Installationspfad Geben Sie das Verzeichnis auf dem Agenten-Endpunkt an, in dem die Security Agent-Installation erfolgt. Geben Sie Folgendes an: • Installationspfad: Der Standardinstallationspfad des Agenten ist `C:\Programme\Trend Micro\Security Agent` oder `C:\Programme (x86)\Trend Micro\Security Agent`. Identifizieren Sie den Installationspfad oder verwenden Sie den Standardpfad. Wenn der Pfad nicht existiert, wird er während der Agenteninstallation von Setup erstellt. • Security Agent Kommunikationsportnummer	Ja	Nein

Installationsinformationen	Erforderliche Informationen während	
	Neuinstallation	Upgrade
Datenbank-Backup Geben Sie einen Speicherort auf dem Server-Computer an, um den Trend Micro Apex One-Server für Rollback-Zwecke zu sichern. **Hinweis** Das Sicherungspaket erfordert mindestens 300 MB freien Speicherplatz und kann einige Zeit in Anspruch nehmen, um abgeschlossen zu werden.	Nein	Ja
Serverauthentifizierungszertifikat Trend Micro Apex One versucht, während der Installation vorhandene Authentifizierungszertifikate zu erkennen. Wenn Trend Micro Apex One kein Zertifikat erkennt, geben Sie das Sicherungspasswort für das neue Zertifikat an.	Ja	Ja
Verknüpfung zum Programmordner Die Verknüpfung zum Trend Micro Apex One-Server-Installationsordner wird im Windows-Startmenü angezeigt. Der Standardname der Verknüpfung ist Trend Micro Trend Micro Apex One Server-<Server_name>. Wählen Sie einen anderen Namen oder verwenden Sie den Standardnamen.	Ja	Nein

Bekannte Kompatibilitätsprobleme

In diesem Abschnitt werden Kompatibilitätsprobleme bei der Installation des Trend Micro Apex One-Servers auf demselben endpunkt mit bestimmten Drittanbieteranwendungen erläutert. Weitere Informationen finden Sie in der Dokumentation der Drittanbieteranwendungen.

Microsoft Lockdown Tools und URLScan

Bei der Verwendung des Microsoft IIS Lockdown-Tools oder URLScan kann das Sperren der folgenden Trend Micro Apex One-Dateien Security Agent und die Serverkommunikation blockieren:

- Konfigurationsdateien (`.ini`)
- `.dat`DAT-Dateien
- Dynamische Linkbibliothek (`.dll`) Dateien
- Ausführbare Dateien (`.exe`)

Verhinderung von URLScan-Interferenzen in der Agent-Server-Kommunikation

Prozedur

1. Beenden Sie den World Wide Web Publishing-Dienst auf dem Trend Micro Apex One-Servercomputer.
2. Ändern Sie die URLScan-Konfigurationsdatei, um die oben angegebenen Dateitypen zuzulassen.
3. Starten Sie den World Wide Web Publishing Dienst neu.

Microsoft Exchange Server

Bei der Installation des Security Agent während der Serverinstallation benötigt Trend Micro Apex One Zugriff auf alle Dateien, die der Agent durchsucht. Da Microsoft Exchange Server Nachrichten in lokalen Verzeichnissen speichert, ist es notwendig, diese Verzeichnisse von der Durchsuchung auszuschließen, damit der Exchange Server E-Mail-Nachrichten verarbeiten kann.

Trend Micro Apex One schließt automatisch alle Microsoft Exchange 2000/2003-Verzeichnisse vom Durchsuchen aus. Konfigurieren Sie diese Einstellung in der Webkonsole (**Agents** > **Globale Agent-Einstellungen> Sucheinstellungen** auf der **Sicherheitseinstellungen**-Registerkarte). Für Details zum Suchausschluss von Microsoft Exchange 2007, siehe:

https://technet.microsoft.com/en-us/library/bb332342(EXCHG.80).aspx

Datenbankserver

Administratoren können Datenbankserver durchsuchen, jedoch kann dies bei Anwendungen, die auf die Datenbanken zugreifen, zu Leistungseinbußen führen. Erwägen Sie, Datenbanken und deren Sicherungsordner von der Echtzeitsuche auszuschließen. Führen Sie eine manuelle Suche bei geringem Netzaufkommen durch, um die Auswirkungen der Datenbanksuchen zu minimieren.

Kapitel 2

Installation von Trend Micro Apex One

In diesem Kapitel werden die Schritte zur Installation von Trend Micro Apex One™ beschrieben.

Themen in diesem Kapitel:

Überlegungen zur Neuinstallation

Wichtig

Sie können keine Neuinstallation des Trend Micro Apex One-Servers auf dem Server-Computer mit installiertem Apex Central durchführen.

Berücksichtigen Sie Folgendes bei der Neuinstallation des Trend Micro Apex One-Servers:

- *Standort des Trend Micro Apex One Servers auf Seite 2-2*
- *Serverleistung auf Seite 2-3*
- *Bereitstellung der Suchmethode während der Installation auf Seite 2-4*
- *Netzwerkdatenverkehr auf Seite 2-5*
- *Drittanbieter-Sicherheitssoftware auf Seite 2-7*
- *Active Directory auf Seite 2-7*

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

http://docs.trendmicro.com/en-us/home.aspx

Standort des Trend Micro Apex One Servers

Trend Micro Apex One kann eine Vielzahl von Netzwerkumgebungen unterstützen. Zum Beispiel können Sie eine Firewall zwischen dem Trend Micro Apex One-Server und seinen Agenten positionieren oder sowohl den Server als auch alle Agenten hinter einer einzigen Netzwerk-Firewall platzieren. Wenn sich eine Firewall zwischen dem Server und seinen Agenten befindet, konfigurieren Sie die Firewall so, dass sie den Datenverkehr zwischen den Agenten- und Server-Listening-Ports zulässt.

Weitere Informationen zur Behebung potenzieller Probleme bei der Verwaltung von Security Agents in einem Netzwerk, das Network Address Translation verwendet, finden Sie im *Administratorhandbuch*.

Wichtig

Aus Sicherheitsgründen empfiehlt Trend Micro, den Trend Micro Apex One-Server innerhalb des Unternehmensintranets zu installieren. Wenn Sie Endpunkte verwalten müssen, die das lokale Intranet verlassen, empfiehlt Trend Micro, den Trend Micro Apex One-Edge-Relais-Server in der DMZ zu installieren.

Serverleistung

Unternehmensnetzwerke benötigen Server mit höheren Spezifikationen als die, die für kleine und mittelgroße Unternehmen erforderlich sind.

Tipp

Trend Micro empfiehlt mindestens 2 GHz Dual-Prozessoren und über 3 GB RAM für den Trend Micro Apex One-Server.

Die Anzahl der vernetzten endpunktAgents, die ein einzelner Trend Micro Apex One-Server verwalten kann, hängt von mehreren Faktoren ab, wie z.B. den verfügbaren Serverressourcen und der Netzwerktopologie. Wenden Sie sich an Ihren Trend Micro-Vertreter, um Hilfe bei der Bestimmung der Anzahl der Agents zu erhalten, die der Server verwalten kann.

Dedizierter Server

Beim Auswählen des endpunkts, auf dem Sie den Trend Micro Apex One Server hosten, beachten Sie Folgendes:

- Die CPU-Auslastung des endpunkts
- Andere Aufgaben des endpunkts

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

Bereitstellung der Suchmethode während der Installation

In dieser Trend Micro Apex One Version können Sie Agents so konfigurieren, dass entweder die intelligente Suche oder die herkömmliche Suche verwendet wird.

Herkömmliche Suche

Herkömmliche Suche ist die Suchmethode, die in allen früheren Trend Micro Apex One-Versionen verwendet wurde. Eine Herkömmliche Suche Agent speichert alle Trend Micro Apex One-Komponenten auf dem Agentendpunkt und durchsucht alle Dateien lokal.

intelligente Suche

Die intelligente Suche nutzt Bedrohungssignaturen, die in der Cloud gespeichert sind. Im Modus der intelligenten Suche durchsucht das Trend Micro Apex OneAgent zunächst lokal nach Sicherheitsrisiken. Wenn das Agent das Risiko der Datei während der Suche nicht bestimmen kann, verbindet sich das Agent mit einem Smart Protection Server.

Die intelligente Suche bietet die folgenden Funktionen und Vorteile:

- Bietet schnelle, Echtzeit-Sicherheitsstatus-Abfragefunktionen in der Cloud
- Reduziert die Gesamtzeit, die benötigt wird, um Schutz gegen neue Bedrohungen bereitzustellen
- Reduziert die bei Pattern-Updates verbrauchte Netzwerkbandbreite. Der Großteil der Pattern-Definitions-Updates muss nur an die Cloud und nicht an viele Agents geliefert werden.
- Reduziert die Kosten und den Aufwand, die mit unternehmensweiten Musterbereitstellungen verbunden sind
- Senkt den Arbeitsspeicherbedarf auf den Endpunkten. Der Bedarf erhöht sich mit der Zeit auch kaum.

Bereitstellung der Suchmethode

Während neuer Installationen ist die standardmäßige Suchmethode für Agents die Smart-Suchmethode. Trend Micro Apex One ermöglicht es Ihnen auch, die Suchmethode für jede Domain nach der Installation des Servers anzupassen. Beachten Sie Folgendes:

- Wenn Sie die Suchmethode nach der Installation des Servers nicht geändert haben, verwenden alle Agents, die Sie installieren, die intelligente Suche.
- Wenn Sie die Herkömmliche Suche auf allen Agents verwenden möchten, ändern Sie die Suchmethode auf der Root-Ebene nach der Installation des Servers auf Herkömmliche Suche.
- Wenn Sie sowohl die herkömmliche Suche als auch die intelligente Suche verwenden möchten, empfiehlt Trend Micro, die intelligente Suche als Suchmethode auf Root-Ebene beizubehalten und dann die Suchmethode für Domains zu ändern, auf die Sie die herkömmliche Suche anwenden möchten.

Netzwerkdatenverkehr

Bei der Planung der Bereitstellung sollten Sie den Netzwerkverkehr berücksichtigen, den Trend Micro Apex One erzeugt. Der Server erzeugt Verkehr, wenn er Folgendes tut:

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

Der Security Agent erzeugt Datenverkehr, wenn er Folgendes tut:

- Startet
- Aktualisiert Komponenten
- Aktualisiert die Einstellungen und installiert einen Hot Fix
- Durchsucht nach Sicherheitsrisiken

- Wechselt zwischen „Unabhängig“-Modus und „Normal“-Modus
- Wechselt zwischen herkömmlicher Suche und intelligenter Suche

Netzwerkverkehr während Komponenten-Updates

Trend Micro Apex One kommt es zu erheblichem Netzwerkverkehr beim Update einer Komponente. Um den bei Komponenten-Updates entstehenden Netzwerkverkehr zu verringern, dupliziert Trend Micro Apex One Komponenten. Anstatt bei der Aktualisierung die vollständige Pattern-Datei herunterzuladen, lädt Trend Micro Apex One nur die 'inkrementellen' Pattern (kleinere Versionen der vollständigen Pattern-Datei) herunter und führt diese nach dem Download mit der alten Pattern-Datei zusammen.

Security Agents regelmäßig aktualisiert, laden Sie nur das inkrementelle Muster herunter. Andernfalls laden sie die vollständige Pattern-Datei herunter.

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.

Agenten und Netzwerkverkehr aktualisieren

Wenn es Abschnitte im Netzwerk mit geringer Bandbreite oder starkem Datenverkehr zwischen Agents und dem Trend Micro Apex One-Server gibt, benennen Sie ausgewählte Trend Micro Apex OneAgents als Update-Agenten oder Aktualisierungsquellen für andere Agents. Dies hilft, die Last der Bereitstellung von Komponenten auf alle Agents zu verteilen.

Wenn Sie beispielsweise ein Remote-Büro mit 20 oder mehr endpunkte haben, benennen Sie einen Update-Agenten, um Updates vom Trend Micro Apex One-Server zu replizieren und als Verteilungspunkt für andere Agent endpunkte im lokalen Netzwerk zu fungieren. Weitere Informationen zu Update-Agenten finden Sie im *Administrator-Handbuch*.

Trend Micro Apex Central und Netzwerkverkehr

Trend Micro Apex Central™ verwaltet Produkte und Dienste von Trend Micro auf Gateways, Mail-Servern, File-Servern und Unternehmensdesktops.

Die webbasierte Management-Konsole des Trend Micro Apex Central bietet einen zentralen Überwachungspunkt für Produkte und Services im gesamten Netzwerk.

Verwenden Sie Trend Micro Apex Central, um mehrere Trend Micro Apex One-Server von einem einzigen Standort aus zu verwalten. Trend Micro Apex Central-Server mit schneller, zuverlässiger Internetverbindung können Komponenten vom Trend Micro ActiveUpdate Server herunterladen. Trend Micro Apex Central verteilt dann die Komponenten an einen oder mehrere Trend Micro Apex One-Server mit unzuverlässiger oder keiner Internetverbindung.

Weitere Informationen finden Sie in der Trend Micro Apex Central-Dokumentation.

Drittanbieter-Sicherheitssoftware

Entfernen Sie Sicherheitssoftware von Drittanbietern vom Endpunkt, auf dem die Trend Micro Apex One-Serverinstallation erfolgt. Diese Anwendungen können die erfolgreiche Installation des Trend Micro Apex One-Servers verhindern oder dessen Leistung beeinträchtigen. Installieren Sie den Trend Micro Apex One-Server und Security Agent sofort nach dem Entfernen der Sicherheitssoftware von Drittanbietern, um den Endpunkt vor Sicherheitsrisiken zu schützen.

Hinweis

Trend Micro Apex One kann die Serverkomponente eines Antivirusprodukts eines Drittanbieters nicht automatisch deinstallieren, aber die Agentenkomponente deinstallieren. Siehe das *Administratorhandbuch* für Details.

Active Directory

Alle Trend Micro Apex One-Server müssen Teil einer Active Directory-Domäne sein, um die Vorteile der rollenbasierten Verwaltung und der Einhaltung von Sicherheitsrichtlinien nutzen zu können.

Unbeaufsichtigte Installation

Installieren oder aktualisieren Sie mehrere Trend Micro Apex One-Server im Hintergrund, wenn die Server identische Installationseinstellungen verwenden.

Die Silent-Installation vorbereiten

Prozedur

1. Erstellen Sie eine Antwortdatei, indem Sie das Setup ausführen und die Installationsoptionen in einer `.iss`-Datei aufzeichnen. Alle Server, die mithilfe der Antwortdatei im Hintergrund installiert werden, verwenden diese Einstellungen.

   Wichtig

   - Das Setup zeigt nur Bildschirme für die lokale Installation an.
   - Für Neuinstallationen erstellen Sie eine Antwortdatei von jedem endpunkt, auf dem der Trend Micro Apex One-Server nicht installiert ist.

2. Führen Sie das Setup über die Eingabeaufforderung aus und weisen Sie das Setup auf den Speicherort der Antwortdatei hin, die für die stille Installation verwendet werden soll.

Konfiguration der Aufzeichnungseinstellungen in eine Antwortdatei

Dieses Verfahren installiert Trend Micro Apex One nicht. Es zeichnet nur die Setup-Konfiguration in einer Antwortdatei auf.

Prozedur

1. Laden Sie die `ApexOne.exe`-Datei herunter und extrahieren Sie den Inhalt.

2. Öffnen Sie ein Eingabeaufforderungsfenster und geben Sie das Verzeichnis der Trend Micro Apex Onesetup.exe-Datei ein.

   Zum Beispiel, "`CD C:\Apex One Installer\setup.exe`".

3. Geben Sie folgenden Befehl ein:

   ```
   setup.exe -r
   ```

   Der `-r`-Parameter veranlasst Setup, die Installation zu starten und die Installationsdetails in einer Antwortdatei aufzuzeichnen.

4. Führen Sie die Installationsschritte in der Einrichtung durch.

5. Nachdem Sie die Schritte abgeschlossen haben, überprüfen Sie die Antwortdatei `setup.iss` in `%windir%`.

Stille Installation ausführen

Prozedur

1. Kopieren Sie das Installationspaket und `setup.iss` auf das Ziel endpunkt.

2. Öffnen Sie im Ziel endpunkt ein Eingabeaufforderungsfenster und geben Sie das Verzeichnis des Installationspakets ein.

3. Geben Sie folgenden Befehl ein:

   ```
   setup.exe -s <-f1path>setup.iss <-f2path>setup.log.
   ```

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

   Wobei gilt:

   - `-s`: Veranlasst Setup, eine stille Installation durchzuführen
   - `<-f1path>setup.iss`: Speicherort der Antwortdatei. Wenn der Pfad Leerzeichen enthält, setzen Sie den Pfad in Anführungszeichen ("). Zum Beispiel `-f1"C:\osce script\setup.iss"`.

- `<-f2path>setup.log`: Speicherort der Protokolldatei, die nach der Installation von Setup erstellt wird. Wenn der Pfad Leerzeichen enthält, setzen Sie den Pfad in Anführungszeichen ("). Zum Beispiel `-f2"C:\osce log\setup.log"`.

4. Drücken Sie die EINGABETASTE.

   Setup installiert den Server stillschweigend auf dem endpunkt.

5. Um festzustellen, ob die Installation erfolgreich war:

   - Überprüfen Sie die Trend Micro Apex One-Programmverknüpfungen auf dem Ziel endpunkt. Wenn die Verknüpfungen nicht verfügbar sind, versuchen Sie die Installation erneut.
   - Melden Sie bei der Trend Micro Apex One-Web-Konsole an.

Das Installationsprogramm

Führen Sie das Setup-Programm aus, wenn Sie bereit sind, mit der Installation des Trend Micro Apex One-Servers zu beginnen.

Bevor Sie mit einer Neuinstallation des Trend Micro Apex One-Servers beginnen, stellen Sie sicher, dass Sie Ihre Umgebung ordnungsgemäß vorbereitet haben. Weitere Informationen zu Überlegungen bei der Neuinstallation finden Sie unter:

- *Überlegungen zur Neuinstallation auf Seite 2-2*
- *Erweiterte Funktionsanforderungen für Apex Central auf Seite 1-7*

Wenn Sie sicher sind, dass Sie bereit sind zu beginnen, folgen Sie den Anweisungen auf dem Bildschirm, um den Trend Micro Apex One-Server zu installieren.

Lizenzvereinbarung

Lesen Sie die Lizenzvereinbarung sorgfältig durch und akzeptieren Sie die Bedingungen der Lizenzvereinbarung, um mit der Installation fortzufahren.

Die Installation kann nicht fortgesetzt werden, ohne die Bedingungen der Lizenzvereinbarung zu akzeptieren.

Endpoint Prescan

Bevor die Trend Micro Apex One-Serverinstallation beginnt, kann das Setup den Zielendpunkt auf Viren und Malware durchsuchen. Das Setup durchsucht die anfälligsten Bereiche des Endpunkts, die Folgendes umfassen:

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

Das Setup kann die folgenden Aktionen gegen erkannte Virus/Malware und Trojaner-Programme ausführen:

- **Delete**: Löscht eine infizierte Datei
- **Säubern**: Reinigt eine bereinigbare Datei, bevor der vollständige Zugriff auf die Datei gewährt wird, oder lässt die angegebene nächste Aktion eine nicht bereinigbare Datei behandeln.
- **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. Virus/Malware kann beim Öffnen der umbenannten infizierten Datei ausgeführt werden.
- **Übergehen**: Ermöglicht vollen Zugriff auf die infizierte Datei, ohne etwas mit der Datei zu tun. Ein Benutzer kann die Datei kopieren/löschen/öffnen.

Wichtig

Während einer lokalen Upgrade-Installation fordert das Setup-Programm Sie auf, Ihre Einstellungen für Schutz vor Ransomware zu aktualisieren, um optimierten Schutz vor Ransomware-Bedrohungen zu erhalten.

Das Anwenden der aktualisierten Einstellungen ändert nur die Einstellungen auf Agenten, die bereits die Verhaltensüberwachung aktiviert haben.

Proxy-Server

Der Trend Micro Apex One-Server verwendet das HTTPS-Protokoll für die Kommunikation zwischen Agent und Server und um eine Verbindung zum Trend Micro ActiveUpdate Server herzustellen und Updates herunterzuladen. Wenn ein Proxy-Server den Internetverkehr im Netzwerk verwaltet, benötigt Trend Micro Apex One die Proxy-Einstellungen, um sicherzustellen, dass der Server Updates vom ActiveUpdate Server herunterladen kann.

Administratoren können die Proxy-Einstellungen während der Installation überspringen und diese nach der Installation über die Trend Micro Apex One Webkonsole festlegen.

Produktaktivierung

Geben Sie den Groß- und Kleinschreibung beachtenden Aktivierungscode ein, den Sie erhalten haben, um alle Trend Micro Apex One-Funktionen zu aktivieren.

Um die Aktivierungscodes zu erhalten, klicken Sie auf **Online registrieren**. Die Einrichtung öffnet die Registrierungswebsite Trend Micro. Nach dem Ausfüllen des Registrierungsformulars sendet Trend Micro eine E-Mail mit den Aktivierungscodes. Nach Erhalt der Codes fahren Sie mit dem Installationsprozess fort.

Produktversionen

Installieren Sie entweder eine Vollversion oder eine Testversion von Trend Micro Apex One. Beide Versionen erfordern einen unterschiedlichen

Aktivierungscode. Um einen Aktivierungscode zu erhalten, registrieren Sie das Produkt bei Trend Micro.

Tabelle 2-1. Versionsvergleich

Version	Beschreibung
Vollversion	Die Vollversion umfasst alle Produktfunktionen und technischen Support und bietet eine Nachfrist (in der Regel 30 Tage) nach Ablauf der Lizenz. Nach Ablauf der Nachfrist sind technischer Support und Komponenten-Updates nicht verfügbar. Die Scan-Engines durchsuchen endpunkte weiterhin mit veralteten Komponenten. Diese veralteten Komponenten können endpunkte möglicherweise nicht vollständig vor den neuesten Sicherheitsrisiken schützen. Erneuern Sie die Lizenz vor oder nach ihrem Ablauf durch den Kauf einer Wartungsverlängerung.
Testversion	Die Testversion umfasst alle Produktfunktionen. Sie können die Testversion jederzeit auf die Vollversion upgraden. Wenn am Ende des Testzeitraums kein Upgrade durchgeführt wird, Trend Micro Apex One deaktiviert Komponenten-Updates, Scannen und alle Agent-Funktionen.

Registrierungsschlüssel und Aktivierungscodes

Geben Sie während der Installation den Aktivierungscode ein, um alle Funktionen zu aktivieren.

Verwenden Sie den Registrierungsschlüssel, der mit dem Produkt geliefert wurde, um Aktivierungscodes zu erhalten (falls noch nicht erhalten). Die Einrichtung leitet automatisch zur Trend Micro-Website für die Produktregistrierung weiter.

Nach der Registrierung des Produkts sendet Trend Micro die Aktivierungscodes.

Kontaktieren Sie einen Vertriebsmitarbeiter von Trend Micro, um den Registrierungsschlüssel oder die Aktivierungscodes zu erhalten, falls keiner zum Zeitpunkt der Installation verfügbar ist.

Weitere Informationen finden Sie unter *Kontaktaufnahme mit Trend Micro auf Seite 7-3*.

Hinweis

Bei Fragen zur Registrierung siehe:

https://success.trendmicro.com/en-US/solution/KA-0007041.

Installationspfad

Akzeptieren Sie den Standardinstallationspfad oder geben Sie einen neuen an.

Serverkennung

Geben Sie an, ob Security Agents den Server-Computer durch seinen vollqualifizierten Domänennamen (FQDN), Hostnamen (Domänennamen) oder IP-Adresse identifiziert.

Die Kommunikation zwischen dem Server-Computer und Security Agents hängt von der angegebenen IP-Adresse ab. Eine Änderung der IP-Adresse führt dazu, dass Security Agents nicht mit dem Trend Micro Apex One-Server kommunizieren kann. Die einzige Möglichkeit, die Kommunikation wiederherzustellen, besteht darin, alle Security Agents neu bereitzustellen. Die gleiche Situation gilt, wenn der Server-Computer durch einen sich ändernden Host-Namen identifiziert wird.

In den meisten Netzwerken ändert sich die IP-Adresse des Server-Computers eher als sein Host-Name, daher ist es in der Regel vorzuziehen, den Server-Computer anhand eines Host-Namens zu identifizieren.

Tipp

Für Administratoren, die die IP-Adresse anstelle des Host-Namens verwenden, empfiehlt Trend Micro nicht, die IP-Adresse (vom DHCP-Server bezogen) nach der Installation zu ändern. Administratoren können weitere Kommunikationsprobleme mit Security Agents vermeiden, indem sie die IP-Adresskonfiguration auf Statisch (auf dem DHCP-Server) einstellen und dabei die gleiche IP-Adressinformation verwenden, die vom DHCP-Server bezogen wurde.

Eine andere Möglichkeit, die IP-Adresskonfiguration beizubehalten, besteht darin, die IP-Adresse nur für den Trend Micro Apex One-Server zu reservieren. Dies zwingt den DHCP-Server, Trend Micro Apex One dieselbe IP-Adresse zuzuweisen, selbst wenn DHCP aktiviert ist.

Wenn Sie statische IP-Adressen verwenden, identifizieren Sie den Server anhand seiner IP-Adresse. Wenn der Server-Computer über mehrere Netzwerkkarten (NICs) verfügt, sollten Sie außerdem eine der IP-Adressen anstelle des Host-Namens verwenden, um eine erfolgreiche Kommunikation zwischen Agent und Server sicherzustellen.

Webserver

Der Trend Micro Apex One-Webserver hostet die Webkonsole, ermöglicht dem Administrator das Ausführen von Konsolen-Common-Gateway-Interfaces (CGIs) und akzeptiert Befehle von Security Agents. Der Webserver konvertiert diese Befehle in Security Agent-CGIs und leitet sie an den Apex One Master Service weiter.

HTTP-Port

Der Webserver hört auf Security Agent-Anfragen am HTTP-Port und leitet diese Anfragen an den Apex One Master Service weiter. Dieser Dienst gibt Informationen an Security Agents am vorgesehenen Security Agent-Kommunikationsport zurück.

SSL-Unterstützung

Trend Micro Apex One verwendet Secure Sockets Layer (SSL) für die sichere Kommunikation zwischen der Webkonsole und dem Server. SSL bietet eine zusätzliche Schutzschicht gegen Hacker. Obwohl Trend Micro Apex One die auf der Webkonsole angegebenen Passwörter vor dem Senden an den Trend Micro Apex One-Server verschlüsselt, können Hacker das Paket dennoch abfangen und es ohne Entschlüsselung "wiederholen", um Zugriff auf die Konsole zu erhalten. SSL-Tunneling verhindert, dass Hacker Pakete, die das Netzwerk durchqueren, abfangen.

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

Bei der Auswahl von SSL erstellt das Setup automatisch ein SSL-Zertifikat, das für SSL-Verbindungen erforderlich ist. Das Zertifikat enthält Serverinformationen, einen öffentlichen Schlüssel und einen privaten Schlüssel.

Das SSL-Zertifikat sollte eine Gültigkeitsdauer zwischen 1 und 20 Jahren haben. Der Administrator kann das Zertifikat auch nach Ablauf weiterhin verwenden. Allerdings erscheint eine Warnmeldung jedes Mal, wenn eine SSL-Verbindung mit demselben Zertifikat aufgerufen wird.

Wie die Kommunikation über SSL funktioniert:

1. Der Administrator sendet Informationen von der Webkonsole über eine SSL-Verbindung an den Webserver.
2. Der Webserver antwortet der Webkonsole mit dem erforderlichen Zertifikat.
3. Der Browser führt den Schlüsselaustausch unter Verwendung der RSA-Verschlüsselung durch.
4. Die Webkonsole sendet Daten mit RC4-Verschlüsselung an den Webserver.

Obwohl die RSA-Verschlüsselung sicherer ist, verlangsamt sie den Kommunikationsfluss. Daher wird sie nur für den Schlüsselaustausch

verwendet, und RC4, eine schnellere Alternative, wird für den Datentransfer eingesetzt.

Webserver-Ports

Die folgende Tabelle listet die Standardportnummern für den Webserver auf.

TABELLE 2-2. Portnummern für den Trend Micro Apex One Webserver

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

Installation von Endpoint Sensor

Wenn Sie Trend Micro Apex Central integrieren und die Endpoint Sensor-Lizenz erworben haben, wählen Sie **Endpoint Sensor installieren**, um sicherzustellen, dass alle erforderlichen Endpoint Sensor-Dienste für Security Agents verfügbar sind.

Hinweis

Diese Funktion wird offiziell nur auf den folgenden Plattformen unterstützt:

- Windows 10

Die folgende Tabelle zeigt die Mindestanforderungen für die Installation des Endpoint Sensor-Dienstes auf.

VORGANG	VORAUSSETZUNGEN	ÜBERPRÜFUNG
Redis-Dienst	Der Trend Micro Apex One-Server-Computer darf keinen vorhandenen Redis-Dienst installiert haben. Sie müssen jeden vorhandenen Redis-Dienst deinstallieren und dem Installationsprogramm erlauben, einen neuen Dienst zu installieren.	Nachdem Sie auf **Weiter** auf dem **Installation von Endpoint Sensor**-Bildschirm geklickt haben

VORGANG	VORAUSSETZUNGEN	ÜBERPRÜFUNG
SQL Server-Version	• SQL Server 2017 • SQL Server 2016 SP1 **Hinweis** Diese Funktion unterstützt keine SQL Server Express-Versionen.	Nach dem Klicken auf **Weiter** auf dem Bildschirm **Setup der Apex One Datenbank**
Datenbankkonfiguration	**Full-Text and Semantic Extractions for Search** aktiviert Weitere Informationen zum Aktivieren von **Full-Text and Semantic Extractions for Search** finden Sie in Ihrer SQL Server-Dokumentation.	Nach dem Klicken auf **Weiter** auf dem Bildschirm **Setup der Apex One Datenbank**
	Zugriffsrechte auf die **tempdb**-Datenbank für Datenbankwartungsfunktionen	Keine

Hinweis

Wenn Sie den Endpoint Sensor-Dienst nicht installieren und einen unterstützten SQL Server mit **Full-Text and Semantic Extractions for Search** aktiviert auswählen, ist die einzige Möglichkeit, Endpoint Sensor später zu verwenden, zum Bildschirm **Uninstall or change a program** von Windows **Systemsteuerung** zu gehen.

Wählen Sie den Trend Micro Apex One Server aus und klicken Sie auf **Ändern**.

Setup der Apex One Datenbank

Wichtig

Wenn Sie planen, die Endpoint Sensor-Funktion zu nutzen, müssen Sie eine Datenbank auf einer ordnungsgemäß vorbereiteten und unterstützten Version von SQL Server erstellen.

Weitere Informationen finden Sie unter *Apex One Endpoint Sensor auf Seite 1-12*.

Prozedur

1. Wählen Sie den Speicherort der Apex One-Datenbank aus:
   - **Install/Create a new SQL Server Express instance**: Wählen Sie die Installation von SQL Server 2016 SP2 Express und erstellen Sie die „\OFFICESCAN“-Datenbankinstanz

     Wichtig

     Diese Option ist nicht verfügbar, wenn Sie sich entschieden haben, die Endpoint Sensor-Funktion zu installieren.
   - **SQL Server**: Wählen Sie die vorhandene SQL Server-Installation und die Datenbankinstanz aus, die Trend Micro Apex One verwenden soll.
2. Wählen Sie die **Datenbankauthentifizierung**-Methode aus.

   Wenn Sie das **Windows-Konto** verwenden, um sich beim Server anzumelden, wendet Trend Micro Apex One das **Benutzername** des aktuell angemeldeten Benutzers an.

Wichtig

Das Benutzerkonto muss der lokalen Administratorgruppe oder dem integrierten Active Directory (AD)-Administrator angehören, und Sie müssen die folgenden Richtlinien für die Zuweisung von Benutzerrechten mit der Konsole **Local Security Policy** oder **Group Policy Management** unter Windows konfigurieren:

- Als Dienst anmelden
- Als Batchauftrag anmelden
- Lokales Anmelden erlauben

Das Benutzerkonto muss außerdem über die folgenden Datenbankrollen verfügen:

- dbcreator

  Hinweis

  Nur erforderlich, wenn Sie eine neue Datenbankinstanz mit dem Setup-Programm erstellen.

- bulkadmin
- db_owner

3. Geben Sie im Abschnitt **Datenbankname** den Namen der Datenbankinstanz auf dem SQL Server an, die für die erforderlichen **Apex One**-Datenbank(en) verwendet werden soll.

Hinweis

- Die Option **Endpoint Sensor** wird nur angezeigt, wenn Sie sich entschieden haben, die Endpoint Sensor-Funktion zu installieren.
- Das Setup-Programm erstellt automatisch eine neue Datenbankinstanz, wenn die angegebene Datenbank auf dem SQL Server nicht existiert. Das konfigurierte Authentifizierungskonto muss die dbcreator-Berechtigung haben, um eine neue Datenbank zu erstellen.

Bereitstellung des Apex One Security Agent

Es gibt mehrere Methoden zur Installation oder Aktualisierung von Security Agents. Dieser Bildschirm listet die verschiedenen Bereitstellungsmethoden und die ungefähr benötigte Netzwerkbandbreite auf.

Verwenden Sie diesen Bildschirm, um die erforderliche Größe auf den Servern und den Bandbreitenverbrauch beim Bereitstellen von Security Agents auf den Zielendpunkten abzuschätzen.

Hinweis

Alle diese Installationsmethoden erfordern lokale Administrator- oder Domänen-Administratorrechte auf den Zielendpunkten.

Integrierten Smart Protection Server installieren

Die Einrichtung kann den integrierten Smart Protection Server auf dem Zielendpunkt installieren. Der integrierte Server bietet File Reputation-Dienste für Security Agents, die intelligente Suche verwenden, und Web Reputation-Dienste für Security Agents, die Web-Reputation-Richtlinien unterliegen. Verwalten Sie den integrierten Server über die Trend Micro Apex One-Webkonsole.

Wichtig

Diese Version von Trend Micro Apex One unterstützt sowohl HTTP- als auch HTTPS-Kommunikation für File Reputation-Abfragen und nur HTTP-Kommunikation für Web Reputation-Abfragen.

Trend Micro empfiehlt die Installation des eigenständigen Smart Protection Server, der die gleichen Funktionen wie der integrierte Server hat, aber mehr Security Agents bedienen kann. Der eigenständige Server wird separat installiert und verfügt über eine eigene Verwaltungskonsole. Weitere Informationen zum eigenständigen Server finden Sie im *Trend Micro Smart Protection Server Administrator's Guide*.

Tipp

Weil der integrierte Smart Protection Server und der Trend Micro Apex One Server auf demselben Endpunkt ausgeführt werden, kann bei sehr hohem Datenaufkommen die Leistung des Endpunkts für beide Server signifikant beeinträchtigt werden. Um den Datenverkehr zum Trend Micro Apex One Server 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 zur Konfiguration von Smart Protection Quellen für Security Agents finden Sie im *Administratorhandbuch*.

Integrierter Server nicht installiert

Bei einer Neuinstallation und wenn Sie sich entscheiden, den Integrierten Server nicht zu installieren:

- Herkömmliche Suche wird zur standardmäßigen Suchmethode.
- Beim Aktivieren von Web Reputation-Richtlinien in einem separaten Installationsbildschirm (für Details siehe *Web-Reputation-Dienste auf Seite 2-27*), kann Agents keine Web Reputation-Abfragen senden, da Trend Micro Apex One davon ausgeht, dass keine Smart Protection Server-Installation erfolgt ist.

Wenn ein eigenständiger Server nach der Installation von Trend Micro Apex One verfügbar ist, führen Sie die folgenden Aufgaben von der Trend Micro Apex One Webkonsole aus:

- Ändern Sie die Suchmethode auf intelligente Suche.
- Fügen Sie den eigenständigen Server zur Smart Protection-Quellenliste hinzu, damit Agents Datei- und Web Reputation-Abfragen an den Server senden kann.

Security Agent installieren

Wählen Sie die Installation von Security Agent auf dem Zielserver.

Das Security Agent-Programm bietet den tatsächlichen Schutz vor Sicherheitsrisiken. Daher muss der Trend Micro Apex One-Server-Computer ebenfalls das Security Agent-Programm haben, um gegen Sicherheitsrisiken geschützt zu sein. Die Wahl, das Security Agent während der Serverinstallation zu installieren, ist eine bequeme Möglichkeit, um sicherzustellen, dass der Server automatisch geschützt ist. Es entfällt auch die zusätzliche Aufgabe, das Security Agent nach der Serverinstallation zu installieren.

Hinweis

Installieren Sie das Security Agent auf anderen Endpunkten im Netzwerk nach der Serverinstallation.

Weitere Informationen finden Sie im *Administratorhandbuch*.

Wenn eine Trend Micro oder eine Endpoint-Sicherheitssoftware eines Drittanbieters derzeit auf dem Server-Computer installiert ist, kann Trend Micro Apex One möglicherweise die Software nicht automatisch deinstallieren und durch die Security Agent ersetzen. Wenden Sie sich an Ihren Support-Anbieter, um eine Liste der Software zu erhalten, die Trend Micro Apex One automatisch deinstalliert. Wenn die Software nicht automatisch deinstalliert werden kann, deinstallieren Sie sie manuell, bevor Sie mit der Installation von Trend Micro Apex One fortfahren.

Smart Feedback

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

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

Beispiele der Informationen, die an Trend Micro gesendet werden:

- Datei-Prüfsummen
- Websites, auf die zugegriffen wird
- Dateiinformationen, darunter Größe und Pfade
- Namen von ausführbaren Dateien

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

Tipp

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

Weitere Informationen über das Smart Protection Network finden Sie unter:

http://www.smartprotectionnetwork.com

Security Agent-Installation

Akzeptieren Sie die standardmäßigen Security Agent-Installationsoptionen oder geben Sie einen anderen Installationspfad an. Ändern Sie den Pfad, wenn auf dem Installationsverzeichnis nicht genügend Speicherplatz vorhanden ist.

Tipp

Trend Micro empfiehlt, die Standardeinstellungen zu verwenden.

Wenn Sie einen anderen Installationspfad angeben, geben Sie einen statischen Pfad ein oder verwenden Sie Variablen. Wenn der angegebene Pfad ein Verzeichnis enthält, das auf dem Security Agent nicht existiert, erstellt das Setup das Verzeichnis automatisch während der Security Agent-Installation.

Um einen statischen Security Agent-Installationspfad einzugeben, geben Sie den Laufwerkspfad einschließlich des Laufwerkbuchstabens ein. Zum Beispiel `C:\Program Files\Trend Micro\Security Agent`.

Hinweis

Die Änderung des Installationspfads von Security Agent ist nach Abschluss der Installation des Trend Micro Apex One-Servers nicht möglich. Alle installierten Security Agents verwenden denselben Installationspfad.

Beim Festlegen von Variablen für den Security Agent-Installationspfad verwenden Sie Folgendes:

- `$BOOTDISK`: Der Laufwerksbuchstabe der Festplatte, von der der Endpunkt standardmäßig startet `C:\`
- `$WINDIR`: Das Windows-Verzeichnis, standardmäßig `C:\Windows`

- `$ProgramFiles`: Das Verzeichnis Programmdateien wird automatisch in Windows eingerichtet und normalerweise standardmäßig für die Installation von Software verwendet `C:\Program Files`

Konfigurieren Sie auch auf diesem Bildschirm Folgendes:

- **Portnummer**: Der Trend Micro Apex One-Server verwendet den angegebenen Port, um mit Agents zu kommunizieren. Akzeptieren Sie den Standardwert oder geben Sie einen neuen Wert ein.

Apex One Firewall

Die Apex One Firewall schützt Security Agents und Server im Netzwerk mit Hilfe von Stateful-Inspection-Technologie, leistungsstarken Funktionen zur Netzwerksuche und Eliminierung. Erstellen Sie Regeln zum Filtern von Verbindungen nach IP-Adresse, Portnummer oder Protokoll und wenden Sie die Regeln dann auf verschiedene Benutzergruppen an.

Optional können Sie die Apex One Firewall deaktivieren und später über die Trend Micro Apex One Server-Webkonsole wieder aktivieren.

Optional aktivieren Sie die Apex One Firewall auf Serverplattformen. Wenn Sie ein Upgrade mit bereits aktivierter Apex One Firewall auf Serverplattformen durchführen, wählen Sie **Apex One Firewall aktivieren (auf Serverplattformen)**, damit Trend Micro Apex One die Apex One Firewall nach dem Upgrade nicht deaktiviert.

Anti-Spyware-Funktion

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

Trend Micro bietet den Bewertungsmodus an, um die Bewertung von Elementen zu ermöglichen, die Trend Micro als Spyware/Grayware erkennt. Administratoren können dann die geeignete Aktion konfigurieren. Beispielsweise können Sie Spyware/Grayware, die als Sicherheitsrisiko erkannt wird, zur Liste der zugelassenen Spyware/Grayware hinzufügen.

Nach der Installation konsultieren Sie den *Administratorhandbuch* für einige empfohlene Maßnahmen im Bewertungsmodus.

Konfigurieren Sie den Bewertungsmodus so, dass er nur für einen bestimmten Zeitraum wirksam ist, indem Sie die Anzahl der Wochen auf diesem Bildschirm angeben. Nach der Installation ändern Sie die Einstellungen des Bewertungsmodus über die Webkonsole (**Agents** > **Globale Agent-Einstellungen**, auf der **Secuirty Settings**-Registerkarte im **Nur Einstellungen der Spyware-/Grayware-Suche**-Abschnitt).

Web-Reputation-Dienste

Web Reputation-Richtlinien bestimmen, ob Trend Micro Apex One den Zugriff auf eine Website sperrt oder erlaubt. Einzelheiten zu den Richtlinien finden Sie im *Administrator-Handbuch*.

Durch Auswahl von **Web-Reputation-Dienste aktivieren (auf Desktopplattformen)** werden Richtlinien für interne und externe Agents auf Desktop-Plattformen aktiviert. Wählen Sie **Web-Reputation-Dienste aktivieren (auf Serverplattformen)**, wenn Server-Plattformen denselben Schutz vor Internet-Bedrohungen wie Desktop-Plattformen benötigen.

Security Agents verwenden die Standortkriterien, die in der Webkonsole im Fenster **Endpunktspeicherort** konfiguriert sind, um deren Standort und die anzuwendende Richtlinie zu bestimmen. Security Agents wechseln die Richtlinien mit jedem Standortwechsel.

Konfigurieren Sie die Einstellungen der Web Reputation-Richtlinie nach der Installation über die Webkonsole. Trend Micro Apex One Administratoren konfigurieren in der Regel eine strengere Richtlinie für externe Agents.

Web-Reputation-Richtlinien sind detaillierte Einstellungen in der Trend Micro Apex One Agent-Hierarchie. Erzwingen Sie bestimmte Richtlinien für alle Agents, Agent-Gruppen oder einzelne Agents.

Beim Aktivieren von Web Reputation-Richtlinien stellen Sie sicher, dass Sie Smart Protection Server (integriert oder eigenständig) installieren und sie der Smart Protection-Quellenliste in der Trend Micro Apex One Webkonsole hinzufügen. Security Agents senden Web Reputation-Abfragen an die Server, um die Sicherheit der von Benutzern aufgerufenen Websites zu überprüfen.

Hinweis

Der Integrierte Server wird mit dem Trend Micro Apex One-Server installiert. Weitere Informationen finden Sie unter *Integrierten Smart Protection Server installieren auf Seite 2-21*. Der eigenständige Server wird separat installiert.

Serverauthentifizierungszertifikat

Das Setup-Programm versucht, während der Installation vorhandene Authentifizierungszertifikate zu erkennen. Wenn ein vorhandenes Zertifikat existiert, ordnet Trend Micro Apex One die Datei automatisch auf dem **Serverauthentifizierungszertifikat**-Bildschirm zu. Wenn kein vorhandenes Zertifikat existiert, wählt Trend Micro Apex One standardmäßig die **Neues Authentifizierungszertifikat generieren**-Option.

Trend Micro Apex One verwendet die Verschlüsselung mit öffentlichem Schlüssel zum Authentifizieren der Kommunikation, die der Trend Micro Apex One Server auf Agents startet. Mit der Verschlüsselung mit öffentlichem Schlüssel bewahrt der Server einen privaten Schlüssel auf und verteilt einen öffentlichen Schlüssel an alle Agents. Die Agents überprüfen mit dem öffentlichen Schlüssel, ob die eingehende Kommunikation vom Server gestartet wurde und gültig ist. Die Agents antworten, falls die Überprüfung erfolgreich ist.

Hinweis

Trend Micro Apex One authentifiziert keine Kommunikationen, die Agents auf dem Server starten.

Trend Micro Apex One kann das Authentifizierungszertifikat während der Installation generieren, oder Administratoren können ein bereits vorhandenes Authentifizierungszertifikat von einem anderen Trend Micro Apex One-Server importieren.

Kennwort für das Administratorkonto

Geben Sie Passwörter an, um auf die Webkonsole zuzugreifen und das Security Agent zu entladen und zu deinstallieren.

Rufen Sie die Webkonsole auf

Während der Installation wird ein Root-Konto erstellt. Das Root-Konto hat vollen Zugriff auf alle Trend Micro Apex One Webkonsolenfunktionen. Die Anmeldung mit diesem Konto ermöglicht es dem Administrator auch, benutzerdefinierte Benutzerkonten zu erstellen, die andere Benutzer zur Anmeldung an der Webkonsole verwenden können. Benutzer können je nach den Zugriffsrechten ihrer Konten eine oder mehrere Webkonsolenfunktionen konfigurieren oder anzeigen.

Geben Sie ein Passwort an, das nur den Trend Micro Apex One Administratoren bekannt ist. Wenden Sie sich an Ihren Support-Anbieter, um Hilfe beim Zurücksetzen eines vergessenen Passworts zu erhalten.

Entladen und Deinstallieren des Security Agent

Geben Sie ein Passwort an, um eine unbefugte Deinstallation oder das Entladen des Security Agent zu verhindern. Deinstallieren oder entladen Sie das Security Agent nur, wenn es Probleme mit den Security Agent-Funktionen gibt, und installieren/neu laden Sie es umgehend.

Apex One Programmverknüpfungen

Akzeptieren Sie den Standardordnernamen, geben Sie einen neuen an oder wählen Sie einen vorhandenen Ordner aus, dem das Setup die Programmverknüpfungen hinzufügt.

Installationsinformationen

Dieser Bildschirm bietet eine Zusammenfassung der Installationseinstellungen. Überprüfen Sie die Installationsinformationen und klicken Sie auf **Zurück**, um Einstellungen oder Optionen zu ändern. Um die Installation zu starten, klicken Sie auf **Install.**

Der InstallShield Wizard ist abgeschlossen

Wenn die Installation abgeschlossen ist, lesen Sie die Readme-Datei für grundlegende Informationen über das Produkt und bekannte Probleme.

Stellen Sie den forensic-Ordner und die Datenbank, die Sie gesichert haben, an folgendem Speicherort wieder her:

```
<Apex One server installation folder>\PCCSRV\Private\
```

Administratoren können die Webkonsole starten, um die Trend Micro Apex One-Einstellungen zu konfigurieren.

Kapitel 3

Trend Micro Apex One upgraden

In diesem Kapitel werden die Schritte für das Upgrade von Trend Micro Apex One™ beschrieben.

Themen in diesem Kapitel:

Überlegungen zum Upgrade

Wichtig

Wenn Sie auf Trend Micro Apex One upgraden und Control Manager auf demselben Server-Computer installiert ist, hängt die Unterstützung für einen einzelnen Server-Computer für Trend Micro Apex One und Apex Central von den aktivierten Funktionen ab.

Für weitere Informationen navigieren Sie zu https://success.trendmicro.com/dcx/s/solution/000267022?language=en_US.

Diese Version von Trend Micro Apex OneService Pack 1 Patch 4 unterstützt Upgrades von Trend Micro Apex One.

Hinweis

Trend Micro empfiehlt dringend, alle verfügbaren Patches und Hotfixes auf Ihrem aktuellen Apex One-Server anzuwenden, bevor Sie ein Upgrade durchführen.

Besuchen Sie die folgende Website für eine vollständige Liste der Trend Micro Apex One Systemvoraussetzungen:

https://docs.trendmicro.com/en-us/home.aspx

Berücksichtigen Sie Folgendes beim Upgrade des Trend Micro Apex One Servers und der Security Agents:

- *IPv6-Unterstützung auf Seite 3-2*
- *Trend Micro Apex One Einstellungen und Konfigurationen auf Seite 3-3*
- *Bereitstellung der Suchmethode während des Upgrades auf Seite 3-5*

IPv6-Unterstützung

Für den Trend Micro Apex One Server und die Agent-Upgrades gelten folgende IPv6-Voraussetzungen:

- Der Server muss bereits einen IIS Webserver verwenden.
- 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 Agents ihre Verbindung mit dem Server. Wenn der Server über seine IPv4-Adresse identifiziert wird, kann der Server den Agent nicht an reine IPv6-Endpunkte 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 **`nslookup`**.

Trend Micro Apex One Einstellungen und Konfigurationen

Sichern Sie die Trend Micro Apex One-Datenbank und wichtige Konfigurationsdateien, bevor Sie den Trend Micro Apex One-Server aktualisieren.

Tipp

Diese Version von Trend Micro Apex One bietet einen Sicherungsmechanismus für Rollback-Zwecke. Führen Sie ein manuelles Datenbank-Backup durch, wenn Sie nicht vorhaben, das automatische Backup während der Installation zu verwenden.

Die Trend Micro Apex One Datenbank und Konfigurationsdateien sichern und wiederherstellen

Prozedur

1. Stoppen Sie den Trend Micro Apex One Master-Dienst über die Microsoft Management Console.
2. Stoppen Sie den Trend Micro Apex One Apex Central-Agentendienst.
3. Stoppen Sie den Trend Micro Apex One Plug-in Manager-Dienst.

4. Stoppen Sie den World Wide Web Publishing Dienst.
5. Sichern Sie die folgenden Datenbankdateien manuell, die unter `<Server installation folder>\PCCSRV\Admin\Utility\SQ` gefunden wurden:
   - `libSQLDatabaseUpgrade.dll`
   - `oscedbt.exe`
6. Sichern Sie die folgenden Dateien und Ordner manuell, die sich unter `<Server installation folder>\PCCSRV` befinden:

   Hinweis

   Sichern Sie diese Dateien und Ordner, um Trend Micro Apex One nur bei Upgrade-Problemen zurückzusetzen.

   - `ofcscan.ini`: Diese Datei enthält globale Agent-Einstellungen
   - `ous.ini`: Diese Datei enthält die Liste der Update-Adressen für die Verteilung von Antiviren-Komponenten
   - `Private` Ordner: Dieser Ordner enthält die Einstellungen der Firewall und der Update-Quellen
   - `Web\tmOPP` Ordner: Dieser Ordner enthält die Ausbruchsprävention – Einstellungen
   - `Pccnt\Common\OfcPfw*.dat`: Diese Datei enthält die Einstellungen der Firewall
   - `Download\OfcPfw*.dat`: Diese Datei enthält die Einstellungen zur Verteilung der Firewall
   - `Log`ordner: Dieser Ordner enthält Systemereignisse und die Verbindungsüberprüfungsprotokolle
   - `Virus`ordner: Enthält Dateien in Quarantäne
   - `HTTPDB`-Ordner: Enthält die Trend Micro Apex One-Datenbank
7. Aktualisieren Sie den Trend Micro Apex One-Server.

Hinweis

Wenn Sie auf Upgrade-Probleme stoßen, kopieren Sie die Sicherungsdateien aus Schritt 6 in den `<Server installation folder>\PCCSRV`-Ordner auf dem Zielendpunkt und starten Sie die folgenden Dienste neu:

- World Wide Web Publishing-Dienst
- Trend Micro Apex One Plug-in Manager Service
- Trend Micro Apex One Apex Central-Agentendienst
- Trend Micro Apex One Master Service

Bereitstellung der Suchmethode während des Upgrades

In dieser Trend Micro Apex One-Version können Administratoren Security Agents so konfigurieren, dass entweder die intelligente Suche oder die herkömmliche Suche verwendet wird.

Beim Upgrade von Trend Micro Apex One von einer früheren Version, behalten oder passen Sie die Suchmethode für jede Domain je nach gewählter Upgrade-Methode an. Berücksichtigen Sie Folgendes:

- Wenn Sie planen, den Trend Micro Apex One-Server direkt auf dem Server-Computer zu aktualisieren, ist es nicht notwendig, Änderungen an der Suchmethode über die Webkonsole vorzunehmen, da die Agenten ihre Suchmethode – Einstellungen nach der Aktualisierung beibehalten.
- Beim Planen eines Upgrades von Security Agents durch Verschieben auf den Trend Micro Apex OneService Pack 1 Patch 4-Server:
  - Wählen Sie im Trend Micro Apex OneService Pack 1 Patch 4-Server die manuelle Agenten-Gruppierung. Diese Methode der Agenten-Gruppierung ermöglicht die Erstellung neuer Domänen.

Hinweis

Bei Verwendung der automatischen Agent-Gruppierung aktivieren Sie diese erst, nachdem alle Agents aktualisiert wurden, um sicherzustellen, dass alle Suchmethode – Einstellungen während der Agent-Aktualisierung beibehalten werden.

- Duplizieren Sie die Domänenstruktur und die Suchmethode – Einstellungen in einer früheren Version des Trend Micro Apex One-Servers in den Trend Micro Apex OneService Pack 1 Patch 4-Server. Wenn die Domänenstruktur und die Suchmethode – Einstellungen auf den beiden Servern nicht identisch sind, können einige Security Agents, die auf den Trend Micro Apex OneService Pack 1 Patch 4-Server wechseln, ihre ursprünglichen Suchmethode – Einstellungen möglicherweise nicht anwenden.

Vor Upgrades des Servers und der Agents

Bevor Sie den Apex One-Server und -Agenten aktualisieren, beachten Sie Folgendes:

1. Erstellen Sie manuell ein Backup des folgenden forensic-Ordners und der Datenbank für Prävention vor Datenverlust auf dem Apex One-Server:

   - `<Apex One server installation folder>\PCCSRV\Private\DLPForensicData`
   - `<Apex One server installation folder>\PCCSRV\Private\DLPForensicDataTracker.db`

   Wichtig

   Notieren Sie sich den Dateispeicherort. Stellen Sie nach Abschluss des Upgrades den forensischen Ordner und die Datenbank im selben Speicherort wieder her.

2. Das Installationspaket enthält Updates für die Firewall-Treiber. Wenn Sie die Apex One Firewall in Ihrer aktuellen Serverversion aktiviert

haben, kann die Bereitstellung des Pakets die folgenden Störungen des Endpunkt-Agenten verursachen:

- Wenn das Update des Allgemeinen Firewall-Treibers startet, werden die Agenten-Endpunkte vorübergehend vom Netzwerk getrennt. Benutzer werden vor der Trennung nicht benachrichtigt.

  Eine Option in der Apex One-Webkonsole, die standardmäßig aktiviert ist, verschiebt das Update des Allgemeinen Firewall-Treibers, bis der Agent-Endpunkt neu gestartet wird. Um Verbindungsprobleme zu vermeiden, stellen Sie sicher, dass diese Option aktiviert ist.

  Um den Status dieser Option zu überprüfen:

  a. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen** und klicken Sie auf die Registerkarte **Sicherheitseinstellungen**.

  b. Gehen Sie zum Abschnitt **Firewall-Einstellungen**. Die Option ist **Update the Apex One firewall driver only after a system restart**.

- Nach der Bereitstellung des Pakets existiert die vorherige Version des TDI-Treibers weiterhin auf dem Agent-Endpunkt, und die neue Version wird erst geladen, wenn der Endpunkt neu gestartet wird. Benutzer werden wahrscheinlich Probleme mit dem Security Agent haben, wenn sie nicht sofort neu starten.

  Wenn die Option zur Anzeige der Aufforderung zum Neustart in der Webkonsole aktiviert ist, werden die Benutzer aufgefordert, neu zu starten. Benutzer, die sich jedoch entscheiden, den Neustart zu verschieben, werden nicht erneut aufgefordert. Wenn die Option deaktiviert ist, werden die Benutzer überhaupt nicht benachrichtigt.

  Die Option zur Anzeige der Aufforderung zum Neustart ist standardmäßig aktiviert. Um den Status dieser Option zu überprüfen:

  - a. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen** und klicken Sie auf die Registerkarte **Agent Kontrolle**.

b. Gehen Sie zum Abschnitt **Warneinstellungen**. Die Option ist **Eine Benachrichtigung anzeigen, wenn der Endpunkt zum Laden eines Kerneltreibers neu gestartet werden muss**.

3. Der Apex One-Server kann nicht auf diese Version aktualisiert werden, wenn:

   - Der Agent führt das Login-Skript (`AutoPcc.exe`) zum Zeitpunkt des Server-Upgrades aus. Stellen Sie sicher, dass kein Agent das Login-Skript ausführt, bevor Sie den Server aktualisieren.
   - Der Server führt datenbankbezogene Aufgaben aus. Überprüfen Sie vor dem Upgrade den Status der Serverdatenbank (`DbServer.exe`). Öffnen Sie beispielsweise den Windows Task-Manager und vergewissern Sie sich, dass die CPU-Auslastung für `DbServer.exe` 00 beträgt. Wenn die CPU-Auslastung höher ist, warten Sie, bis die Auslastung 00 beträgt, was darauf hinweist, dass datenbankbezogene Aufgaben abgeschlossen sind. Wenn Sie ein Upgrade durchführen und auf Upgrade-Probleme stoßen, ist es möglich, dass Datenbankdateien gesperrt wurden. Starten Sie in diesem Fall den Server-Computer neu, um die Dateien zu entsperren, und führen Sie dann ein weiteres Upgrade durch.

Verwenden Sie eine der folgenden Upgrade-Methoden:

- *Upgrade-Methode 1: Automatische Agentenaktualisierung deaktivieren auf Seite 3-8*
- *Upgrade-Methode 2: Upgrade von Update-Agenten auf Seite 3-11*
- *Upgrade-Methode 3: Verschieben Sie die Agents auf den Trend Micro Apex OneService Pack 1 Patch 4-Server auf Seite 3-17*
- *Upgrade-Methode 4: Automatisches Agenten-Upgrade aktivieren auf Seite 3-20*

Upgrade-Methode 1: Automatische Agentenaktualisierung deaktivieren

Durch das Deaktivieren des automatischen Agenten-Upgrades ist es möglich, zuerst den Server zu aktualisieren und dann die Agenten in Gruppen zu

aktualisieren. Verwenden Sie diese Upgrade-Methode, wenn Sie eine große Anzahl von Agenten aktualisieren.

Teil 1: Update-Einstellungen auf dem Trend Micro Apex One-Server konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen** und gehen Sie zur Registerkarte **Andere Einstellungen**.
4. Wählen Sie in der Dropdown-Liste **Security Agents only update the following components** den Eintrag **Pattern Files** aus.
5. Klicken Sie auf **Auf alle Agents anwenden**.

   Es kann eine Weile dauern, bis die Einstellungen in einer komplexen Netzwerkumgebung und bei einer großen Anzahl von Agenten auf die Online-Agenten übertragen werden. Planen Sie vor dem Upgrade ausreichend Zeit ein, damit die Einstellungen auf alle Agenten übertragen werden können. Security Agents, die die Einstellungen nicht anwenden, werden automatisch aktualisiert.

Teil 2: Aktualisieren Sie den Trend Micro Apex One Server

Siehe *Lokales Upgrade durchführen auf Seite 3-22* für Details zum Upgrade des Trend Micro Apex One-Servers.

Konfigurieren Sie die Trend Micro Apex One-Servereinstellungen mithilfe der Webkonsole unmittelbar nach Abschluss der Installation und vor dem Upgrade der Agenten.

Für detaillierte Anweisungen zur Konfiguration der Trend Micro Apex One-Einstellungen lesen Sie im *Administratorhandbuch* oder in der *Server-Online-Hilfe* nach.

Teil 3: Upgrade Security Agents

Prozedur

1. Gehen Sie zu **Updates** > **Agents** > **Automatisches Update** und stellen Sie sicher, dass die folgenden Optionen aktiviert sind:
   - **Komponenten-Update auf den Agents sofort nach dem Download einer neuen Komponente auf dem Apex One Server starten**
   - **Agents beginnen nach dem Neustart und dem Herstellen einer Verbindung zum Apex One Server mit dem Komponenten-Update (mit Ausnahme unabhängiger Agents)**
2. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
3. Wählen Sie im Agentenbaum die Agenten aus, die Sie aktualisieren möchten. Sie können einen oder mehrere Domänen oder einzelne/alle Agenten innerhalb einer Domäne auswählen.
4. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen** und gehen Sie zur Registerkarte **Andere Einstellungen**.
5. Wählen Sie in der Dropdown-Liste **Security Agents only update the following components** den Eintrag **Alle Komponenten (einschließlich Hotfixes und Agent-Programm)** aus.
6. Klicken Sie auf **Speichern**.
7. Überprüfen Sie die Upgrade-Ergebnisse.
   - *Online-Agenten auf Seite 3-15*
   - *Offline Agents auf Seite 3-17*
   - *Unabhängige (Roaming) Agenten auf Seite 3-17*
8. Starten Sie die Agentenendpunkte neu, um die Aktualisierung der Agenten abzuschließen.

9. Wiederholen Sie Schritt 2 bis Schritt 8, bis alle Agenten aktualisiert wurden.

Upgrade-Methode 2: Upgrade von Update-Agenten

Verwenden Sie diese Upgrade-Methode, wenn Sie eine große Anzahl von Agenten haben, die von Update Agents aktualisieren. Diese Agenten werden von ihren jeweiligen Update Agents aktualisiert.

Security Agents, die nicht von Update Agents aktualisiert werden, werden vom Apex One-Server aktualisiert.

Teil 1: Update-Einstellungen auf dem Trend Micro Apex One-Server konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents auszuwählen.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen** und gehen Sie zur Registerkarte **Andere Einstellungen**.
4. Wählen Sie in der Dropdown-Liste **Security Agents only update the following components** den Eintrag **Pattern Files** aus.
5. Klicken Sie auf **Auf alle Agents anwenden**.

   Es kann eine Weile dauern, bis die Einstellungen in einer komplexen Netzwerkumgebung und bei einer großen Anzahl von Agenten auf die Online-Agenten übertragen werden. Planen Sie vor dem Upgrade ausreichend Zeit ein, damit die Einstellungen auf alle Agenten übertragen werden können. Security Agents, die die Einstellungen nicht anwenden, werden automatisch aktualisiert.

Teil 2: Aktualisieren Sie den Trend Micro Apex One Server

Siehe *Lokales Upgrade durchführen auf Seite 3-22* für Details zum Upgrade des Trend Micro Apex One-Servers.

Konfigurieren Sie die Trend Micro Apex One-Servereinstellungen mithilfe der Webkonsole unmittelbar nach Abschluss der Installation und vor dem Upgrade der Agenten.

Für detaillierte Anweisungen zur Konfiguration der Trend Micro Apex One-Einstellungen lesen Sie im *Administratorhandbuch* oder in der *Server-Online-Hilfe* nach.

Teil 3: Update-Agenten-Upgrade durchführen

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Wählen Sie im Agentenbaum die Update-Agenten zum Upgrade aus.

   Tipp

   Um Update Agents einfach zu finden, wählen Sie eine Domäne aus, gehen Sie zum **Agent tree view** oben im Agentenbaum und wählen Sie dann **Update agent view**.

3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen** und gehen Sie zur Registerkarte **Andere Einstellungen**.
4. Wählen Sie in der Dropdown-Liste **Security Agents only update the following components** den Eintrag **Alle Komponenten (einschließlich Hotfixes und Agent-Programm)** aus.
5. Klicken Sie auf **Speichern**.
6. Navigieren Sie zu **Updates** > **Agents** > **Manuelles Update**.
7. Wählen Sie die Option **Agents manuell auswählen** aus und klicken Sie auf **Auswählen**.

8. Wählen Sie im sich öffnenden Agentenbaum die zu aktualisierenden Update-Agenten aus.

Tipp

Um Update Agents einfach zu finden, wählen Sie eine Domäne aus, gehen Sie zum **Agent tree view** oben im Agentenbaum und wählen Sie dann **Update agent view**.

9. Klicken Sie oben in der Agent-Hierarchie auf **Update starten**.
10. Überprüfen Sie die Upgrade-Ergebnisse.
    - Online-Update-Agenten werden sofort nach dem Start des Komponenten-Updates aktualisiert.
    - Upgrade der Update Agents, die offline sind, wird ausgeführt, wenn sie wieder online sind.
    - Unabhängige (ehemals Roaming-) Update-Agenten werden aktualisiert, wenn sie online gehen oder, wenn der Update-Agent Berechtigungen für zeitgesteuerte Updates hat, wenn das zeitgesteuerte Update ausgeführt wird.
11. Starten Sie die Endpunkte der Update-Agenten neu, um die Aktualisierung der Agenten abzuschließen.
12. Wiederholen Sie Schritt 1 bis Schritt 11, bis alle Update-Agenten aktualisiert wurden.

Teil 4: Einstellungen des Update-Agenten konfigurieren

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Wählen Sie im Agentenbaum die Update-Agenten zum Upgrade aus.

Tipp

Um Update Agents einfach zu finden, wählen Sie eine Domäne aus, gehen Sie zum **Agent tree view** oben im Agentenbaum und wählen Sie dann **Update agent view**.

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

   Warten Sie, bis der Update-Agent das Agentenprogramm heruntergeladen hat, bevor Sie mit Teil 5 fortfahren.
7. Wiederholen Sie Schritt 1 bis Schritt 6, bis alle Update-Agenten die erforderlichen Einstellungen angewendet haben.

Teil 5: Upgrade Security Agents

Prozedur

1. Gehen Sie zu **Updates** > **Agents** > **Automatisches Update** und stellen Sie sicher, dass die folgenden Optionen aktiviert sind:
   - **Komponenten-Update auf den Agents sofort nach dem Download einer neuen Komponente auf dem Apex One Server starten**
   - **Agents beginnen nach dem Neustart und dem Herstellen einer Verbindung zum Apex One Server mit dem Komponenten-Update (mit Ausnahme unabhängiger Agents)**
2. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.

3. Wählen Sie im Agentenbaum die Agenten aus, die Sie aktualisieren möchten. Sie können einen oder mehrere Domänen oder einzelne/alle Agenten innerhalb einer Domäne auswählen.
4. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen** und gehen Sie zur Registerkarte **Andere Einstellungen**.
5. Wählen Sie in der Dropdown-Liste **Security Agents only update the following components** den Eintrag **Alle Komponenten (einschließlich Hotfixes und Agent-Programm)** aus.
6. Klicken Sie auf **Speichern**.
7. Überprüfen Sie die Upgrade-Ergebnisse.
   - *Online-Agenten auf Seite 3-15*
   - *Offline Agents auf Seite 3-17*
   - *Unabhängige (Roaming) Agenten auf Seite 3-17*
8. Starten Sie die Agentenendpunkte neu, um die Aktualisierung der Agenten abzuschließen.
9. Wiederholen Sie Schritt 2 bis Schritt 8, bis alle Agenten aktualisiert wurden.

Upgrade-Ergebnisse

Online-Agenten

Hinweis

Starten Sie die Agenten-Endpunkte nach dem Upgrade neu.

- Automatisches Upgrade

  Online-Agenten beginnen mit dem Upgrade, wenn eines der folgenden Ereignisse eintritt:

  - Der Trend Micro Apex One-Server lädt eine neue Komponente herunter und benachrichtigt die Agenten zur Aktualisierung.

- Der Agent lädt neu.
- Der Agent startet neu und verbindet sich dann mit dem Trend Micro Apex One-Server.
- Zeitgesteuerte Updates werden auf dem Agenten-Endpunkt ausgeführt (nur für Agenten mit Berechtigungen für zeitgesteuerte Updates).

- Manuelles Upgrade

  Wenn keines der oben genannten Ereignisse eingetreten ist, führen Sie eine der folgenden Aufgaben aus, um die Agenten sofort zu aktualisieren:

  - Erstellen und bereitstellen eines EXE- oder MSI-Security Agent-Pakets.

    Hinweis

    Siehe den *Administratorhandbuch* für Anweisungen zur Erstellung des Agentenpakets.

  - Weisen Sie die Benutzer an, **Jetzt aktualisieren** auf dem Agenten-Endpunkt auszuführen.
  - Klicken Sie mit der rechten Maustaste auf `AutoPcc.exe`, und wählen Sie **Run as administrator** aus.
  - Manuelles Agenten-Update initiieren.

  Um manuelles Update zu starten:

  1. Navigieren Sie zu **Updates** > **Agents** > **Manuelles Update**.
  2. Wählen Sie die Option **Agents manuell auswählen** aus und klicken Sie auf **Auswählen**.
  3. Wählen Sie im sich öffnenden Agentenbaum die Agenten aus, die aktualisiert werden sollen.
  4. Klicken Sie oben in der Agent-Hierarchie auf **Initiate Component Update**.

Offline Agents

Offline Agents Upgrade, wenn sie online werden.

Unabhängige (Roaming) Agenten

Unabhängige Agenten (früher als Roaming-Agenten bezeichnet) werden aktualisiert, wenn sie online gehen oder, wenn der Agent Berechtigungen für zeitgesteuerte Updates hat, wenn das zeitgesteuerte Update ausgeführt wird.

Upgrade-Methode 3: Verschieben Sie die Agents auf den Trend Micro Apex OneService Pack 1 Patch 4-Server

Führen Sie eine Neuinstallation des Trend Micro Apex OneService Pack 1 Patch 4-Servers durch und verschieben Sie dann die Agents auf diesen Server. Wenn Sie die Agents verschieben, werden sie automatisch auf Trend Micro Apex OneService Pack 1 Patch 4 aktualisiert.

Teil 1: Führen Sie eine Neuinstallation des Apex One-Servers durch und konfigurieren Sie dann die Update-Einstellungen

Prozedur

1. Führen Sie eine Neuinstallation des Trend Micro Apex OneService Pack 1 Patch 4-Servers durch.

   Weitere Informationen finden Sie unter *Das Installationsprogramm auf Seite 2-10*.

2. Melden Sie sich an der Webkonsole an.

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

   - **Komponenten-Update auf den Agents sofort nach dem Download einer neuen Komponente auf dem Apex One Server starten**
   - **Agents beginnen nach dem Neustart und dem Herstellen einer Verbindung zum Apex One Server mit dem Komponenten-Update (mit Ausnahme unabhängiger Agents)**

4. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
5. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents auszuwählen.
6. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen** und gehen Sie zur Registerkarte **Andere Einstellungen**.
7. Wählen Sie in der Dropdown-Liste **Security Agents only update the following components** den Eintrag **Alle Komponenten (einschließlich Hotfixes und Agent-Programm)** aus.
8. Klicken Sie auf **Auf alle Agents anwenden**.
9. Notieren Sie die folgenden Trend Micro Apex OneService Pack 1 Patch 4 Serverinformationen. Geben Sie diese Informationen auf dem vorherigen Apex One-Server an, wenn Sie Agenten verschieben:
   - Endpunktname oder IP-Adresse
   - Server-Listening-Port

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

Teil 2: Upgrade Security Agents

Prozedur

1. Auf der Webkonsole des vorherigen Servers navigieren Sie zu **Updates** > **Übersicht**.
2. Klicken Sie auf **Benachrichtigung abbrechen**. Diese Funktion löscht die Benachrichtigungswarteschlange des Servers, wodurch Probleme beim Verschieben von Clients/Agenten auf den Trend Micro Apex One-Server verhindert werden.

Warnung!

Führen Sie die folgenden Schritte sofort aus. Wenn die Benachrichtigungswarteschlange des Servers aktualisiert wird, bevor Sie Clients/Agenten verschieben, könnten Clients/Agenten möglicherweise nicht erfolgreich verschoben werden.

3. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
4. Wählen Sie im Agentenbaum die Agenten aus, die Sie aktualisieren möchten. Wählen Sie nur Online-Agenten aus, da Offline- und Roaming-Agenten nicht verschoben werden können.
5. Agenten wie folgt verschieben:
   a. Klicken Sie auf **Agent-Hierarchie verwalten** > **Agent verschieben**.
   b. Geben Sie den Trend Micro Apex One-Server-Computername/IP-Adresse und den Server-Listening-Port unter **Move selected agent(s) online to another Apex One server** an.
6. Klicken Sie auf **Verschieben**.

Upgrade-Ergebnisse

- Online-Agenten beginnen sich zu bewegen und zu aktualisieren.
- Tipps zur Verwaltung von Offline- und unabhängigen (ehemals Roaming-) Agenten:
  - Deaktivieren Sie den unabhängigen (früher Roaming-) Modus auf den Agenten, um sie zu aktualisieren.
  - Für Offline-Agents weisen Sie die Benutzer an, eine Verbindung zum Netzwerk aufzubauen, sodass die Agents online gehen können. Weisen Sie im Fall von Agents, die seit längerer Zeit offline sind, die Benutzer an, den Agent vom Endpunkt zu deinstallieren und anschließend mit Hilfe einer geeigneten Agent-Installationsmethode (wie dem Agent Packager), die im *Administratorhandbuch* beschrieben wird, den Security Agent zu installieren.

Hinweis

Starten Sie die Agentenendpunkte neu, um die Aktualisierung der Agenten abzuschließen.

Upgrade-Methode 4: Automatisches Agenten-Upgrade aktivieren

Nach dem Upgrade des Trend Micro Apex One-Servers auf diese Version benachrichtigt der Server sofort alle von ihm verwalteten Agenten, dass sie ein Upgrade durchführen sollen.

Wenn der Server eine geringe Anzahl von Agenten verwaltet, sollten Sie in Betracht ziehen, den Agenten ein sofortiges Upgrade zu ermöglichen. Es ist möglich, die zuvor besprochenen Upgrade-Methoden zu verwenden.

Teil 1: Update-Einstellungen auf dem Trend Micro Apex One-Server konfigurieren

Prozedur

1. Gehen Sie zu **Updates** > **Agents** > **Automatisches Update** und stellen Sie sicher, dass die folgenden Optionen aktiviert sind:
   - **Initiate component update on agents immediately after the Apex One server downloads a new component.**
   - **Agents beginnen nach dem Neustart und dem Herstellen einer Verbindung zum Apex One Server mit dem Komponenten-Update (mit Ausnahme unabhängiger Agents)**
2. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
3. Klicken Sie in der Agent-Hierarchie auf das Root-Domänen-Symbol (), um alle Agents auszuwählen.
4. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen** und gehen Sie zur Registerkarte **Andere Einstellungen**.
5. Wählen Sie in der Dropdown-Liste **Security Agents only update the following components** den Eintrag **Pattern Files** aus.

6. Klicken Sie auf **Auf alle Agents anwenden**.

   Es kann eine Weile dauern, bis die Einstellungen in einer komplexen Netzwerkumgebung und bei einer großen Anzahl von Agenten auf die Online-Agenten übertragen werden. Planen Sie vor dem Upgrade ausreichend Zeit ein, damit die Einstellungen auf alle Agenten übertragen werden können. Security Agents, die die Einstellungen nicht anwenden, werden automatisch aktualisiert.

Teil 2: Aktualisieren Sie den Trend Micro Apex One Server

Siehe *Lokales Upgrade durchführen auf Seite 3-22* für Details zum Upgrade des Trend Micro Apex One-Servers.

Hinweis

Um den Upgrade-Prozess zu beschleunigen, entladen Sie Security Agent, bevor Sie einen Trend Micro Apex One-Server mit Windows Server 2008 Standard 64-Bit aktualisieren.

Konfigurieren Sie die Trend Micro Apex One-Servereinstellungen mithilfe der Webkonsole unmittelbar nach Abschluss der Installation und vor dem Upgrade der Agenten.

Für detaillierte Anweisungen zur Konfiguration der Trend Micro Apex One-Einstellungen lesen Sie im *Administratorhandbuch* oder in der *Server-Online-Hilfe* nach.

Upgrade-Ergebnisse

- Online-Agenten werden sofort nach Abschluss des Server-Upgrades aktualisiert.
- Upgrade der Agents, die offline sind, wird ausgeführt, wenn sie wieder online sind.
- Unabhängige (ehemals roaming) Agenten werden aktualisiert, wenn sie online gehen oder, wenn der Agent Berechtigungen für zeitgesteuerte Updates hat, wenn das zeitgesteuerte Update ausgeführt wird.

Hinweis

Starten Sie die Agentenendpunkte neu, um die Aktualisierung der Agenten abzuschließen.

Lokales Upgrade durchführen

Während eines lokalen Upgrades wendet Trend Micro Apex One die Einstellungen an, die von der vorherigen Trend Micro Apex One-Serverversion verwendet wurden. Ein begrenzter Satz von Bildschirmen wird angezeigt, der es Ihnen ermöglicht, die neuen Funktionen zu konfigurieren, die von Trend Micro Apex OneService Pack 1 Patch 4 angeboten werden.

Wichtig

Bevor Sie den Apex One-Server aktualisieren, erstellen Sie ein Backup des folgenden forensic-Ordners und der Datenbank für Prävention vor Datenverlust:

- `<Apex One server installation folder>\PCCSRV\Private\DLPForensicData`
- `<Apex One server installation folder>\PCCSRV\Private\DLPForensicDataTracker.db`

Notieren Sie sich den Dateispeicherort. Stellen Sie nach Abschluss des Upgrades den forensischen Ordner und die Datenbank im selben Speicherort wieder her.

Lizenzvereinbarung

Lesen Sie die Lizenzvereinbarung sorgfältig durch und akzeptieren Sie die Bedingungen der Lizenzvereinbarung, um mit der Installation fortzufahren. Die Installation kann nicht fortgesetzt werden, ohne die Bedingungen der Lizenzvereinbarung zu akzeptieren.

Forensic-Daten

Erstellen Sie manuell ein Backup des folgenden forensic-Ordners und der Datenbank für Prävention vor Datenverlust auf dem Apex One-Server:

- `<Apex One server installation folder>\PCCSRV\Private\DLPForensicData`
- `<Apex One server installation folder>\PCCSRV\Private\DLPForensicDataTracker.db`

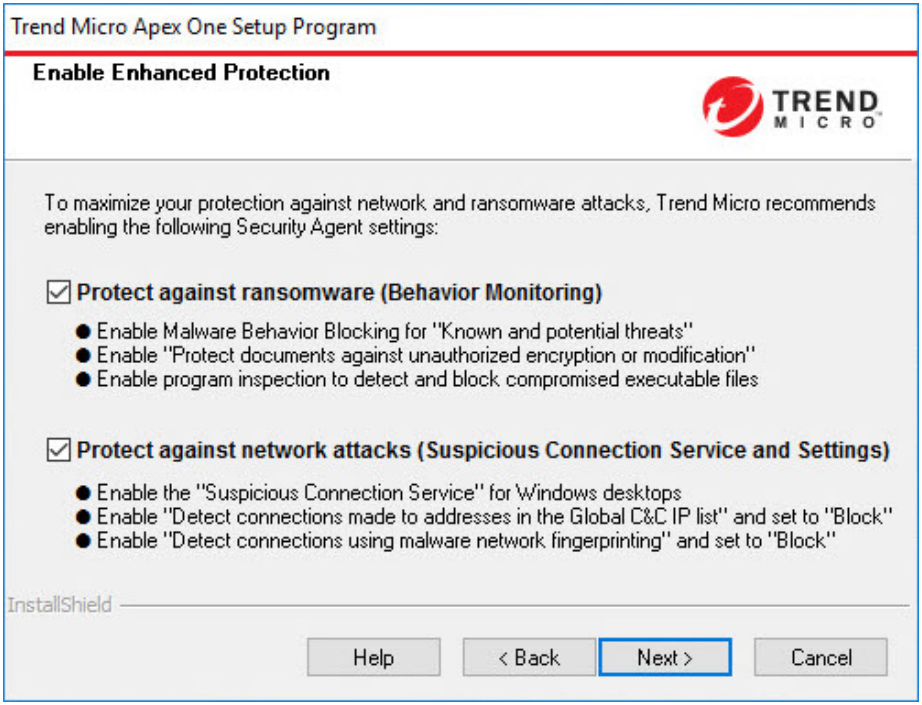
Wichtig

Notieren Sie sich den Dateispeicherort. Stellen Sie nach Abschluss des Upgrades den forensischen Ordner und die Datenbank im selben Speicherort wieder her.

Security Agent-Upgrades

Das Setup-Programm bewertet die Ressourcen des Zielendpunkts. Bei Upgrade-Szenarien erscheint ein Warnbildschirm, wenn eine frühere Version des Security Agent-Programms auf dem Zielendpunkt vorhanden ist.

Erweiterten Schutz aktivieren



Trend Micro empfiehlt, Ransomware- und Netzwerkschutz auf allen Security Agents zu aktivieren.

In der folgenden Tabelle sind die Trend Micro Apex One Web-Konsolenfunktionen aufgeführt, die für jede Einstellung aktiviert sind.

Einstellung	Speicherort der Web-Konsole	Funktionen
Schutz vor Ransomware	**Agents** > **Agent-Verwaltung>Einstellungen** > **Einstellungen der Verhaltensüberwachung** > **Regeln** > **Sperrung des Malware-Verhaltens**-Abschnitt	• **Sperrung des Malware-Verhaltens aktivieren** • **Threats to block: Known and potential threats** • **Dokumente vor nicht autorisierter Verschlüsselung oder Veränderung schützen** • **Programmüberprüfung zum Erkennen und Sperren gefährdeter ausführbarer Dateien aktivieren** **Wichtig** Das Aktivieren von **Schutz vor Ransomware** aktiviert nicht automatisch den Unauthorized Change Prevention Service. Wenn Sie den Dienst deaktiviert haben, müssen Sie den Unauthorized Change Prevention Service manuell aktivieren, bevor Security Agents vor Ransomware-Angriffen schützen kann.
Schutz vor Netzwerkangriffen	**Agents** > **Agent-Verwaltung>Einstellungen** > **Zusätzliche Diensteinstellungen** > **Verdächtiger Verbindungsdienst**-Abschnitt	Aktiviert den Verdächtig-Verbindungsdienst auf **Windows-Desktops**

Einstellung	Speicherort der Web-Konsole	Funktionen
	Agents > **Agent-Verwaltung>Einstellungen** > **Einstellungen für verdächtige Verbindungen**	• **Detect network connections made to addresses in the Global C&C IP list: Block** • **Detect connections using malware network fingerprinting: Block**

Datenbanksicherung

Während der Upgrades bietet das Setup-Programm die Option, die Trend Micro Apex One-Datenbank zu sichern, bevor auf die neueste Version von Trend Micro Apex One aktualisiert wird. Diese Sicherungsinformationen können für Rollback-Zwecke verwendet werden.

Hinweis

Das Sicherungspaket benötigt möglicherweise mehr als 300 MB freien Speicherplatz auf der Festplatte.

Installation von Endpoint Sensor

Wenn Sie Trend Micro Apex Central integrieren und die Endpoint Sensor-Lizenz erworben haben, wählen Sie **Endpoint Sensor installieren**, um sicherzustellen, dass alle erforderlichen Endpoint Sensor-Dienste für Security Agents verfügbar sind.

Hinweis

Diese Funktion wird offiziell nur auf den folgenden Plattformen unterstützt:

- Windows 10

Die folgende Tabelle zeigt die Mindestanforderungen für die Installation des Endpoint Sensor-Dienstes auf.

VORGANG	VORAUSSETZUNGEN	ÜBERPRÜFUNG
Redis-Dienst	Der Trend Micro Apex One-Server-Computer darf keinen vorhandenen Redis-Dienst installiert haben. Sie müssen jeden vorhandenen Redis-Dienst deinstallieren und dem Installationsprogramm erlauben, einen neuen Dienst zu installieren.	Nachdem Sie auf **Weiter** auf dem **Installation von Endpoint Sensor**-Bildschirm geklickt haben
SQL Server-Version	• SQL Server 2017 • SQL Server 2016 SP1 **Hinweis** Diese Funktion unterstützt keine SQL Server Express-Versionen.	Nach dem Klicken auf **Weiter** auf dem Bildschirm **Setup der Apex One Datenbank**
Datenbankkonfiguration	**Full-Text and Semantic Extractions for Search** aktiviert Weitere Informationen zum Aktivieren von **Full-Text and Semantic Extractions for Search** finden Sie in Ihrer SQL Server-Dokumentation.	Nach dem Klicken auf **Weiter** auf dem Bildschirm **Setup der Apex One Datenbank**
	Zugriffsrechte auf die **tempdb**-Datenbank für Datenbankwartungsfunktionen	Keine

Hinweis

Wenn Sie den Endpoint Sensor-Dienst nicht installieren und einen unterstützten SQL Server mit **Full-Text and Semantic Extractions for Search** aktiviert auswählen, ist die einzige Möglichkeit, Endpoint Sensor später zu verwenden, zum Bildschirm **Uninstall or change a program** von Windows **Systemsteuerung** zu gehen.

Wählen Sie den Trend Micro Apex One Server aus und klicken Sie auf **Ändern**.

Setup der Apex One Datenbank

Wichtig

Wenn Sie planen, die Endpoint Sensor-Funktion zu nutzen, müssen Sie eine Datenbank auf einer ordnungsgemäß vorbereiteten und unterstützten Version von SQL Server auswählen.

Weitere Informationen finden Sie unter *Apex One Endpoint Sensor auf Seite 1-12*.

Prozedur

1. Neben **SQL Server** wählen Sie die vorhandene SQL Server-Installation und die Datenbankinstanz aus, die Trend Micro Apex One verwenden soll.
2. Die Authentifizierungsmethode der Datenbank auswählen.

   Wenn Sie das **Windows-Konto** verwenden, um sich beim Server anzumelden, wendet Trend Micro Apex One das **Benutzername** des aktuell angemeldeten Benutzers an.

   domain_name\user_name oder user_name

Wichtig

Das Benutzerkonto muss der lokalen Administratorgruppe oder dem integrierten Active Directory (AD)-Administrator angehören, und Sie müssen die folgenden Richtlinien für die Zuweisung von Benutzerrechten mit der Konsole **Local Security Policy** oder **Group Policy Management** unter Windows konfigurieren:

- Als Dienst anmelden
- Als Batchauftrag anmelden
- Lokales Anmelden erlauben

Das Benutzerkonto muss außerdem über die folgenden Datenbankrollen verfügen:

- dbcreator
- bulkadmin
- db_owner

3. Geben Sie den **Database name** von Trend Micro Apex One auf dem SQL Server an.
4. Klicken Sie auf **Weiter**.

Wichtig

Wenn Sie die Installation der Endpoint Sensor-Dienste ausgewählt haben, überprüft das Setup-Programm sofort, ob die ausgewählte SQL Server-Datenbank ordnungsgemäß konfiguriert ist und die Mindestanforderungen erfüllt. Wenn die SQL Server-Datenbank die Anforderungen nicht erfüllt, müssen Sie eine andere SQL Server-Datenbank auswählen oder zurückgehen und die Installation des Endpoint Sensors nicht auswählen.

Bereitstellung des Apex One Security Agent

Es gibt mehrere Methoden zur Installation oder Aktualisierung von Security Agents. Dieser Bildschirm listet die verschiedenen Bereitstellungsmethoden und die ungefähr benötigte Netzwerkbandbreite auf.

Verwenden Sie diesen Bildschirm, um die erforderliche Größe auf den Servern und den Bandbreitenverbrauch beim Bereitstellen von Security Agents auf den Zielendpunkten abzuschätzen.

Hinweis

Alle diese Installationsmethoden erfordern lokale Administrator- oder Domänen-Administratorrechte auf den Zielendpunkten.

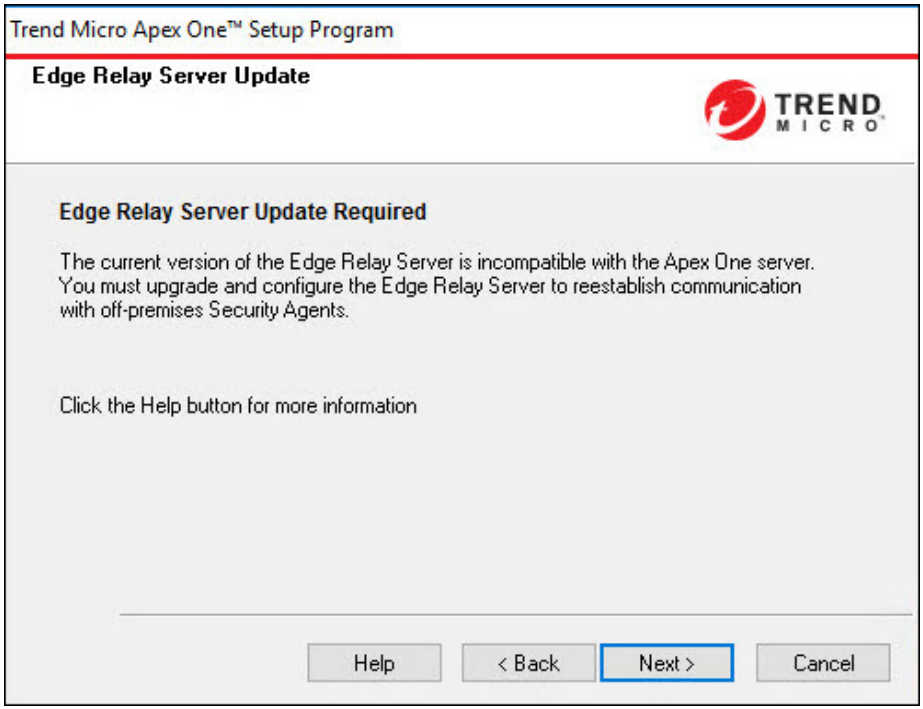
Installationsinformationen

Dieser Bildschirm bietet eine Zusammenfassung der Installationseinstellungen. Überprüfen Sie die Installationsinformationen und klicken Sie auf **Zurück**, um Einstellungen oder Optionen zu ändern. Um die Installation zu starten, klicken Sie auf **Install.**

Update des Edge-Relais-Servers

Wichtig

Wird nur angezeigt, wenn der vorherige Trend Micro Apex One-Server einen registrierten Edge-Relais-Server hatte.



Trend Micro Apex One unterstützt die älteren OfficeScan-Versionen des Edge-Relais-Servers nicht. Sie müssen einen neuen Edge-Relais-Server installieren oder Ihren bestehenden Edge-Relais-Server aktualisieren, um Security Agents außerhalb des Firmengeländes zu schützen.

Nach der Installation oder Aktualisierung des Edge-Relais-Servers müssen alle Security Agents, die Sie mit dem Edge-Relais-Server verwalten möchten, direkt mit dem Apex One-Server verbinden, um die neuesten Einstellungen des Edge-Relais-Servers zu erhalten.

Weitere Informationen zur Installation oder Aktualisierung des Edge-Relais-Servers finden Sie im *Apex One Administrator-Handbuch*.

Der InstallShield Wizard ist abgeschlossen

Wenn die Installation abgeschlossen ist, lesen Sie die Readme-Datei für grundlegende Informationen über das Produkt und bekannte Probleme.

Stellen Sie den forensic-Ordner und die Datenbank, die Sie gesichert haben, an folgendem Speicherort wieder her:

```
<Apex One server installation folder>\PCCSRV\Private\
```

Administratoren können die Webkonsole starten, um die Trend Micro Apex One-Einstellungen zu konfigurieren.

Kapitel 4

Aufgaben nach der Installation

Führen Sie die folgenden Aufgaben aus, nachdem die Installation des Trend Micro Apex One-Servers abgeschlossen ist.

Themen in diesem Kapitel:

Überprüfung der Serverinstallation oder -aktualisierung

Überprüfen Sie nach Abschluss der Installation oder Aktualisierung das Folgende:

TABELLE 4-1. Zu überprüfende Elemente nach der Installation von Trend Micro Apex One

ZU ÜBERPRÜFENDES ELEMENT	DETAILS
Trend Micro Apex One-Serververknüpfungen	Die Trend Micro Trend Micro Apex One-Serververknüpfungen erscheinen im Windows **Start**-Menü auf dem Server-Computer.
Programmliste	Trend Micro Trend Micro Apex One Server ist in der **Add/Remove Programs**-Liste in der Systemsteuerung des Server-Computers aufgeführt.
Trend Micro Apex One Web-Konsole	Geben Sie die folgende URL im Internet Explorer-Browser ein: • HTTPS-Verbindung: `https://<Apex One server name>:<port number>/officescan` Wo `<Apex One server name>` der Name oder die IP-Adresse des Trend Micro Apex One Servers ist. Der Anmeldebildschirm der Webkonsole wird angezeigt.

Zu überprüfendes Element	Details
Apex One-Serverdienste	Die folgenden Apex One Serverdienste werden in der Microsoft Management Console aufgeführt: • Apex One Active Directory-Integration Service: Dieser Dienst zeigt an, ob die Active Directory-Integration und die rollenbasierte Verwaltung ordnungsgemäß funktionieren. • Apex One Apex Central Agent: Der Status für diesen Dienst sollte "Gestartet" sein, wenn der Trend Micro Apex One-Server bei Apex Central registriert wurde. • Apex One Deep Discovery Service: Der Status für diesen Dienst sollte "Gestartet" sein. • Apex One Master-Dienst: Der Status für diesen Dienst sollte "Gestartet" sein. • Apex One Log Receiver-Dienst: Der Status für diesen Dienst sollte "Gestartet" sein. • Apex One Plug-in Manager: Der Status für diesen Dienst sollte "Gestartet" sein. • Trend Micro Smart Protection Abfragen-Handler: Der Status für diesen Dienst sollte "Gestartet" sein. • Trend Micro Smart Protection Server: Der Status für diesen Dienst sollte "Gestartet" sein. • Trend Micro Local Web Classification Server: Der Status für diesen Dienst sollte "Gestartet" sein, wenn der Web Reputation-Dienst während der Installation aktiviert wurde.
Apex One-Serverprozesse	Wenn Sie den Windows Task-Manager öffnen, wird DBServer.exe ausgeführt.
Server-Installationsprotokoll	Die Server-Installationsprotokolldatei, OFCMAS.LOG, befindet sich in `%windir%`.

Zu überprüfendes Element	Details

Registrierungsschlüssel	Der folgende Registrierungsschlüssel existiert:
	• Für 32-Bit-Plattformen:
	`HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan`
	• Für 64-Bit-Plattformen:
	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\TrendMicro\OfficeScan`

Ordner "Programm"	Die Apex One-Serverdateien befinden sich unter `<Server installation folder>`.

Überprüfung der Installation des integrierten Smart Protection Servers

Trend Micro Apex One installiert während einer Neuinstallation automatisch den integrierten Smart Protection Server.

Prozedur

1. Auf der Server-Webkonsole navigieren Sie zu **Administration** > **Smart Protection** > **Smart Protection Quellen**.
2. Klicken Sie auf den Link **Standardliste**.
3. Auf dem daraufhin angezeigten Bildschirm klicken Sie auf **Integrierter Smart Protection Server**.
4. Klicken Sie auf dem angezeigten Bildschirm auf **Verbindung testen**.

   Die Verbindung mit dem Integrierten Server sollte erfolgreich sein.

Den Trend Micro Apex One Server aktualisieren

Nach der Installation von Trend Micro Apex One die Komponenten auf dem Server aktualisieren.

Hinweis

In diesem Abschnitt wird das Durchführen eines manuellen Updates beschrieben. Informationen zu zeitgesteuerten Updates und Update-Konfigurationen finden Sie in der *Server-Online-Hilfe*.

Prozedur

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

   Der **Manuelles Update**-Bildschirm erscheint und zeigt die aktuellen Komponenten, ihre Versionsnummern und die neuesten Aktualisierungsdaten an.
3. Wählen Sie die zu aktualisierenden Komponenten aus.
4. Klicken Sie auf **Update**. Der Server überprüft den Update-Server auf aktualisierte Komponenten. Der Fortschritt und Status des Updates werden angezeigt.

Überprüfung der Standardeinstellungen

Trend Micro Apex One wird mit den Standardeinstellungen installiert. Wenn diese Einstellungen nicht Ihren Sicherheitsanforderungen entsprechen, ändern Sie die Einstellungen in der Webkonsole. Weitere Informationen zu den in der Webkonsole verfügbaren Einstellungen finden Sie in der *Server-Online-Hilfe* und im *Administratorhandbuch*.

Sucheinstellungen

Trend Micro Apex One bietet mehrere Arten von Durchsuchungen, um endpunkte vor Sicherheitsrisiken zu schützen. Ändern Sie die Scan-Einstellungen in der Webkonsole, indem Sie zu **Agents** > **Agent-Verwaltung** gehen und auf **Einstellungen** > **{Scan Type}** klicken.

Agent Einstellungen

Trend Micro Apex One bietet mehrere Arten von Einstellungen, die für alle Agents gelten, die beim Server registriert sind, oder für alle Agents mit einem bestimmten Privileg. Ändern Sie Agent-Einstellungen über die Webkonsole, indem Sie zu **Agents** > **Globale Agent-Einstellungen** gehen.

Agent Berechtigungen

Standard Agent-Berechtigungen umfassen das Anzeigen des System-Tray-Symbols auf dem Security Agentendpunkt. Ändern Sie die Standard-Agent-Berechtigungen über die Webkonsole.

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

Trend Micro Apex One beim Trend Micro Apex Central registrieren

Wenn ein Trend Micro Apex Central-Server neu installierte Trend Micro Apex One-Server verwaltet, registrieren Sie Trend Micro Apex One nach der Installation bei Trend Micro Apex Central.

Hinweis

Trend Micro Apex Central-Registrierung gilt nur für neu installierte Trend Micro Apex One-Server.

Navigieren Sie in der Trend Micro Apex One Web-Konsole zu **Administration** > **Einstellungen** > **Apex Central**.

Siehe die *Trend Micro Apex One Server-Hilfe* oder das *Trend Micro Apex One Administrator-Handbuch* für das Verfahren.

Kapitel 5

Deinstallieren von Trend Micro Apex One

In diesem Kapitel werden die Schritte zur Deinstallation des Trend Micro Apex One Servers beschrieben.

Themen in diesem Kapitel:

Deinstallationsüberlegungen

Bei Problemen mit Trend Micro Apex One verwenden Sie das Deinstallationsprogramm, um den Trend Micro Apex One-Server sicher aus dem endpunkt zu entfernen. Bevor Sie den Server deinstallieren, verschieben Sie die von ihm verwalteten Agents auf einen anderen Trend Micro Apex One-Server.

Vor der Deinstallation des Trend Micro Apex One Servers

Verwenden Sie das Deinstallationsprogramm, um den Trend Micro Apex One-Server sicher zu entfernen.

Bevor Sie den Server deinstallieren, verschieben Sie das von ihm verwaltete Agents auf einen anderen Trend Micro Apex One-Server mit derselben Version. Erwägen Sie, die Serverdatenbank und Konfigurationsdateien zu sichern, um den Server später neu zu installieren.

Verschieben von Agenten auf einen anderen Server

Die Trend Micro Apex One Webkonsole bietet eine Option, um Agents, die vom Server verwaltet werden, auf einen anderen Server zu verschieben.

Prozedur

1. Zeichnen Sie die folgenden Informationen für den anderen Server auf. Diese Informationen sind notwendig, wenn die Agenten verschoben werden.

   - Endpunktname oder IP-Adresse
   - Server-Listening-Port

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

2. Auf der Webkonsole des zu deinstallierenden Servers navigieren Sie zu **Agents** > **Agent-Verwaltung**.

3. Wählen Sie in der Agent-Hierarchie die Agents zum Verschieben aus und klicken Sie dann auf **Agent-Hierarchie verwalten** > **Agent verschieben**.
4. Unter **Ausgewählte(n) Agent(s) auf einen anderen Apex One Server verschieben** geben Sie den Server-Computername/IP-Adresse und den Server-Listening-Port des anderen Trend Micro Apex One-Servers an.
5. Klicken Sie auf **Verschieben**.

Wenn alle Agenten verschoben wurden und bereits von dem anderen Server verwaltet werden, ist es sicher, den Trend Micro Apex One-Server zu deinstallieren.

Die Trend Micro Apex One Konfigurationsdateien sichern und wiederherstellen

Sichern Sie wichtige Konfigurationsdateien, bevor Sie den Trend Micro Apex One-Server deinstallieren.

Hinweis

Während des Deinstallationsprozesses gibt Trend Micro Apex One Ihnen die Möglichkeit, die SQL-Datenbank nicht zu löschen.

Prozedur

1. Stoppen Sie den Apex One Master Service über die Microsoft Management Console.
2. Sichern Sie die folgenden Dateien und Ordner unter `<Server installation folder>\PCCSRV` manuell:
   - `ofcscan.ini`: Enthält globale Agent-Einstellungen
   - `ous.ini`: Diese Datei enthält die Liste der Update-Adressen für die Verteilung von Antiviren-Komponenten
   - Persönlicher Ordner: Enthält die Einstellungen der Firewall und der Update-Quellen

- `Web\tmOPP folder`: Enthält Ausbruchsprävention – Einstellungen
- `Pccnt\Common\OfcPfw*.dat`: Diese Datei enthält die Einstellungen der Firewall
- `Download\OfcPfw.dat`: Diese Datei enthält die Einstellungen zur Verteilung der Firewall
- Protokollordner: Dieser Ordner enthält Systemereignisse und die Verbindungsüberprüfungsprotokolle
- Virus-Ordner: Enthält Dateien in Quarantäne

3. Deinstallieren Sie den Trend Micro Apex One Server.

   Weitere Informationen finden Sie unter *Den Trend Micro Apex One Server deinstallieren auf Seite 5-4*.

4. Führen Sie eine Erstinstallation durch.

   Weitere Informationen finden Sie unter *Das Installationsprogramm auf Seite 2-10*.

5. Nachdem die Installation abgeschlossen ist, öffnen Sie die Microsoft Management Console (`services.msc`).

6. Klicken Sie mit der rechten Maustaste auf **Apex One Master Service** und dann auf **Beenden**.

7. Kopieren Sie die Sicherungsdateien nach `<Server installation folder>\PCCSRV folder` auf den Zielendpunkt.

8. Apex One Master Service neu starten.

Den Trend Micro Apex One Server deinstallieren

Verwenden Sie das Deinstallationsprogramm, um den Trend Micro Apex One-Server und den integrierten Smart Protection Server zu deinstallieren.

Wenn Sie Probleme mit dem Deinstallationsprogramm haben, deinstallieren Sie den Server manuell.

Hinweis

Anweisungen zur Deinstallation von Security Agent finden Sie im *Administratorhandbuch*.

Deinstallation des Trend Micro Apex One Servers mit dem Deinstallationsprogramm

Prozedur

1. Führen Sie das Deinstallationsprogramm aus. Es gibt zwei Möglichkeiten, auf das Deinstallationsprogramm zuzugreifen.
   - Methode A
     a. Klicken Sie auf dem Trend Micro Apex One-Server-Computer auf **Start** > **Programs** > **Trend Micro Apex One Server** > **Apex One deinstallieren**. Ein Bestätigungsbildschirm wird angezeigt.
     b. Klicken Sie auf **Ja**. Das Programm zur Deinstallation des Servers fordert Sie zur Eingabe des Administratorkennworts auf.
     c. Geben Sie das Administrator-Passwort ein und klicken Sie auf **OK**. Das Deinstallationsprogramm des Servers beginnt mit dem Entfernen der Serverdateien. Eine Bestätigungsnachricht erscheint.
     d. Klicken Sie auf **OK**, um das Deinstallationsprogramm zu schließen.
   - Methode B
     a. Doppelklicken Sie auf das Trend Micro Apex One-Serverprogramm auf dem **Windows Add/Remove Programs**-Bildschirm.
     b. Klicken Sie auf **Systemsteuerung** > **Add or Remove Programs**. Suchen Sie den "Trend Micro Apex One Server" und doppelklicken Sie darauf. Befolgen Sie die Anweisungen

auf dem Bildschirm, bis Sie zur Eingabe des Administrator-Passworts aufgefordert werden.

c. Geben Sie das Administrator-Passwort ein und klicken Sie auf **OK**. Das Deinstallationsprogramm des Servers beginnt mit dem Entfernen der Serverdateien. Eine Bestätigungsnachricht erscheint.

d. Klicken Sie auf **OK**, um das Deinstallationsprogramm zu schließen.

Den Trend Micro Apex One Server manuell deinstallieren

Teil 1: Deinstallation des integrierten Smart Protection Servers

Prozedur

1. Öffnen Sie die Microsoft Management Console und stoppen Sie den Apex One Master Service.
2. Öffnen Sie ein Befehlszeilenfenster, und gehen Sie dann zu `<Server installation folder>\PCCSRV`.
3. Führen Sie folgenden Befehl aus:

   ```
   SVRSVCSETUP.EXE -uninstall
   ```

   Dieser Befehl deinstalliert Trend Micro Apex One-bezogene Dienste, entfernt jedoch keine Konfigurationsdateien oder die Trend Micro Apex One-Datenbank.
4. Gehen Sie zu `<Server installation folder>\PCCSRV\private` und öffnen Sie `ofcserver.ini`.
5. Ändern Sie die folgenden Einstellungen:

TABELLE 5-1. ofcserver.ini Einstellungen

EINSTELLUNG	ANWEISUNG
`WSS_INSTALL=1`	Ändern Sie 1 in 0

Einstellung	Anweisung
WSS_ENABLE=1	Diese Zeile löschen
WSS_URL=https://<computer_name>:4345/tmcss/	Diese Zeile löschen

6. Navigieren Sie zu <Server installation folder>\PCCSRV und öffnen Sie OfUninst.ini. Löschen Sie die folgenden Zeilen:

```
[WSS_WEB_SERVER]

ServerPort=8082

IIS_VhostName=Smart Protection Server (Integrated)

IIS_VHostIdx=5
```

Hinweis

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

```
ROOT=/tmcss,C:\Program Files\Trend
Micro\OfficeScan\PCCSRV\WSS\isapi,,<value>
```

```
[WSS_SSL]

SSLPort=<SSL port>
```

7. Open a command prompt and then go to <Server installation folder>\PCCSRV.

8. Führen Sie die folgenden Befehle aus:

```
Svrsvcsetup -install

Svrsvcsetup -enablessl

Svrsvcsetup -setprivilege
```

9. Überprüfen Sie, ob die folgenden Elemente entfernt wurden:

- Trend Micro Smart Protection Server-Dienst von der Microsoft Management Console
- Leistungsindikatoren bei Smart Protection Server
- Smart Protection Server (integriert) Website

Teil 2: Deinstallation des Apex One-Servers

Prozedur

1. Öffnen Sie den Registrierungs-Editor und führen Sie die folgenden Schritte aus:

   Warnung!

   Die nächsten Schritte erfordern das Löschen von Registrierungsschlüsseln. Unsachgemäße Änderungen an der Registrierung können zu ernsthaften Systemproblemen führen. Erstellen Sie immer eine Sicherungskopie, bevor Sie Änderungen an der Registrierung vornehmen. Weitere Informationen finden Sie in der Hilfe zum Registrierungseditor.

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

   b. Überprüfen Sie, ob der `ofcservice`-Hive gelöscht wurde.

   c. Gehen Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\OfficeScan\` und löschen Sie den `OfficeScan`-Hive.

      Für 64-Bit endpunkte ist der Pfad `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfficeScan\`.

   d. Gehe zu `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\`. Lösche den Ordner `OfficeScan Management Console-<Server Name>`.

2. Gehen Sie zum Ordner `<Server installation folder>\PCCSRV` und heben Sie die Freigabe des Ordners `PCCSRV` auf.
3. Starten Sie den Server-Computer neu.
4. Gehen Sie zu `<Server installation folder>\PCCSRV` und löschen Sie den Ordner `PCCSRV`.
5. Löschen Sie die Trend Micro Apex One-Website aus der Internet Information Services (IIS)-Konsole.
   a. Öffnen Sie die IIS-Konsole.
   b. Erweitern Sie `ServerName`.
   c. Wenn Sie Trend Micro Apex One auf einer separaten Website installiert haben, gehen Sie zum Ordner `Web Sites` und löschen Sie dann Trend Micro Apex One.
   d. Wenn Sie Trend Micro Apex One-virtuelle Verzeichnisse unter der Standardwebsite installiert haben, gehen Sie zu `Default Web Site` und löschen Sie dann das Trend Micro Apex One-virtuelle Verzeichnis.

Kapitel 6

Ressourcen zur Fehlerbehebung

Dieses Kapitel beschreibt Ressourcen, die Sie zur Fehlerbehebung möglicher Probleme mit dieser Version von Trend Micro Apex One verwenden können.

Themen in diesem Kapitel:

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 Trend Micro Apex One Server-GUID und überträgt diese Informationen zusammen mit der gesendeten Datei. Die Bereitstellung der GUID stellt sicher, dass Trend Micro ein Feedback zu den zur Bewertung eingereichten Dateien abgeben kann.

Case Diagnostic Tool

Wenn in einem Produkt eines Kunden ein Problem auftritt, sammelt das Trend Micro Case Diagnostic Tool (CDT) Informationen, die zum Debuggen erforderlich sind. Es schaltet den Debugstatus des Produkts automatisch ein und aus und erfasst die je nach der Kategorie des Problems benötigten Dateien. Diese Informationen werden von Trend Micro zur Behebung von Problemen genutzt, die im Zusammenhang mit dem Produkt auftreten.

Um dieses Tool und die entsprechende Dokumentation zu erhalten, wenden Sie sich an Ihren Support-Anbieter.

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 einigen wenigen Ziel-Workstations ausgeführt werden, um Leistungsprobleme beim realen Einsatz der Verhaltensüberwachung und Gerätesteuerung zu vermeiden.

Hinweis

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

Identifizierung systemintensiver Anwendungen

Prozedur

1. Kontaktieren Sie den Technischen Support von Trend Micro, um eine Kopie des Trend Micro Performance Tuning Tool zu erhalten.
2. Entpacken Sie die Datei `TMPerfTool.zip`, um `TMPerfTool.exe` zu extrahieren.
3. Platzieren Sie `TMPerfTool.exe` im `<Client installation folder>` oder im selben Ordner wie `TMBMCLI.dll`.
4. Klicken Sie mit der rechten Maustaste auf `TMPerfTool.exe`, und wählen Sie **Als Administrator ausführen**.
5. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung, und klicken Sie dann auf **OK**.
6. Klicken Sie auf **Analyze**. Das Tool beginnt mit der Überwachung der CPU-Auslastung und des Ereignisladens.

Ein systemintensiver Prozess wird rot hervorgehoben.

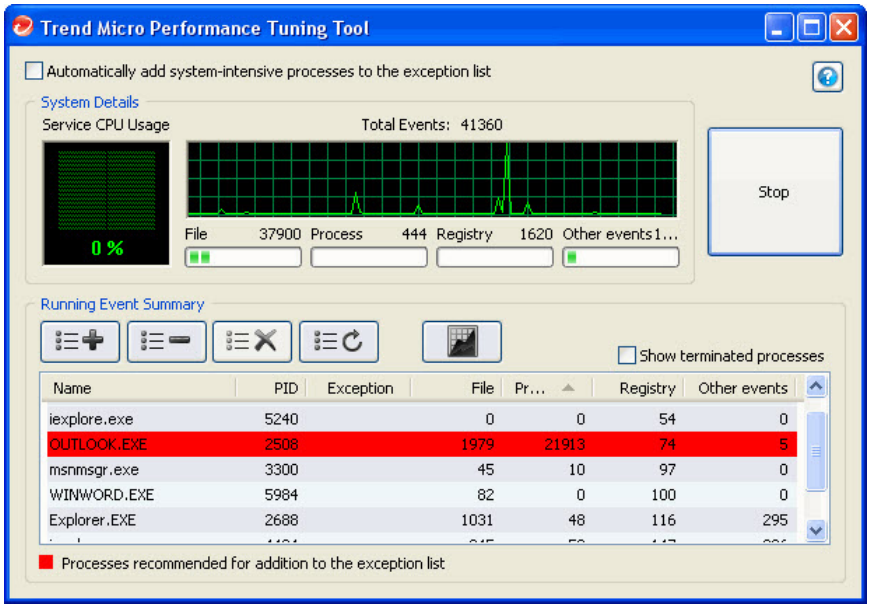


ABBILDUNG 6-1. Systemintensiver Prozess hervorgehoben

7. Wählen Sie einen systemintensiven Prozess, und klicken Sie auf die Schaltfläche **Add to the exception list (allow)** ( ).

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 **Remove from the exception list** ( ).

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 **Generate report** (), und speichern Sie anschließend die .xml-Datei.

d. Überprüfen Sie die Anwendungen, die einen Konflikt verursachen, und fügen Sie sie zur Ausschlussliste der Verhaltensüberwachung hinzu. Einzelheiten finden Sie im *Administrator-Handbuch*.

Installationsprotokolle

Verwenden Sie die Installationsprotokolldateien, die Trend Micro Apex One automatisch erstellt, um Installationsprobleme zu beheben.

TABELLE 6-1. Installationsprotokolldateien

PROTOKOLLDATEI	DATEINAME	SPEICHERORT
Protokoll der lokalen Serverinstallation/-aktualisierung	OFCMAS.LOG	%windir%
Protokoll der Server-Remote-Installation/-Aktualisierung	OFCMAS.LOG (Auf dem endpunkt, auf dem Sie Setup gestartet haben) OFCMAS.LOG (Auf dem Ziel-endpunkt)	%windir%
Security Agent Installationsprotokoll	OFCNT.LOG	%windir% (für alle Installationsmethoden außer bei MSI-Paket) %temp% (für die Installation mit einem MSI-Paket)

Server-Debugprotokolle

Aktivieren Sie das Debug-Logging, bevor Sie die folgenden Serveraufgaben ausführen:

- Den Server deinstallieren und dann erneut installieren.
- Trend Micro Apex One 8.0 auf eine neue Version upgraden.

- Remote-Installation/-Upgrade durchführen (die Debug-Protokollierung ist auf dem endpunkt aktiviert, auf dem das Setup ausgeführt wird, und nicht auf dem Remote-endpunkt).

Warnung!

Debug-Protokolle können die Serverleistung beeinträchtigen und viel Speicherplatz in Anspruch nehmen. Aktivieren Sie Debug-Protokolle nur, wenn nötig, und deaktivieren Sie sie danach sofort wieder. Entfernen Sie die Protokolldatei, wenn die Dateigröße zu groß wird.

Aktivieren des Debug-Loggings auf dem Trend Micro Apex One Server Computer

Option 1:

Prozedur

1. Melden Sie sich an der Webkonsole an.
2. Klicken Sie im Banner der Webkonsole auf "**A**" in "Apex". Dadurch wird der Bildschirm **Debug-Protokoll - Einstellungen** geöffnet.
3. Geben Sie die Debug-Protokolleinstellungen an.
4. Klicken Sie auf **Speichern**.
5. Überprüfen Sie die Protokolldatei (`ofcdebug.log`) am Standardort: `<Server installation folder>\PCCSRV\Log`.

Option 2:

Prozedur

1. Kopieren Sie den Ordner "LogServer" aus `<Server installation folder>\PCCSRV\Private` nach `C:\`.
2. Erstellen Sie eine Datei mit dem Namen `ofcdebug.ini` und dem folgenden Inhalt:

```
[debug]

DebugLevel=9

DebugLog=C:\LogServer\ofcdebug.log

debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

3. Speichern Sie `ofcdebug.ini` unter `C:\LogServer`.
4. Führen Sie die entsprechende Aufgabe durch (d. h. den Server installieren, auf eine neue Version upgraden oder eine Remote-Installation/ein Remote-Upgrade durchführen).
5. Überprüfen Sie `ofcdebug.log` unter `C:\LogServer`.

Hinweis

Wenn das Security Agent auf dem Trend Micro Apex One-Server vorhanden ist, gibt der Agent auch seine Debug-Protokolle in den Debug-Protokollen des Servers aus.

Agent -Debugprotokolle

Debug-Protokollierung vor der Installation des Security Agent aktivieren.

Warnung!

Debug-Protokolle können die Agent-Leistung beeinträchtigen und viel Speicherplatz in Anspruch nehmen. Aktivieren Sie Debug-Protokolle nur, wenn nötig, und deaktivieren Sie sie danach sofort wieder. Löschen Sie die Protokolldatei, wenn sie zu groß wird.

Debug-Protokollierung auf dem Security Agent aktivieren

Prozedur

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

   ```
   [Debug]

   Debuglog=C:\ofcdebug.log

   debuglevel=9

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1
   ```

2. Senden Sie die Datei `ofcdebug.ini` an die Agentenbenutzer, und weisen Sie sie an, die Datei auf dem Laufwerk `C:\` zu speichern.

   `LogServer.exe` wird automatisch ausgeführt, jedes Mal wenn der Agent-Endpunkt startet.

3. Um das Debug-Logging zu starten, laden Sie den Security Agent neu oder starten Sie den Endpunkt neu.

   Weisen Sie die Benutzer an, das `LogServer.exe`-Befehlsfenster, das beim Start des Endpunkts geöffnet wird, NICHT zu schließen, da dies Trend Micro Apex One dazu veranlasst, das Debug-Logging zu stoppen. Wenn Benutzer das Befehlsfenster schließen, können sie das Debug-Logging erneut starten, indem sie `LogServer.exe` in `\Security Agent\Temp` ausführen.

4. Für jeden Agenten-Endpunkt, überprüfen Sie `ofcdebug.log` in `C:\`.

5. Deaktivieren Sie die Debug-Protokollierung für den Security Agent, indem Sie `ofcdebug.ini` löschen.

Kapitel 7

Technischer Support

Erfahren Sie mehr über die folgenden Themen:

Ressourcen zur Fehlerbehebung

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

Support-Portal verwenden

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

Prozedur

1. Gehen Sie zu https://success.trendmicro.com.
2. Wählen Sie unter den verfügbaren Produkten aus oder klicken Sie auf die entsprechende Schaltfläche, um nach Lösungen zu suchen.
3. Mit dem Feld **Support durchsuchen** können Sie nach verfügbaren Lösungen suchen.
4. Falls Sie keine Lösung finden, klicken Sie auf **Support kontaktieren** und wählen Sie den gewünschten Support aus.

   Tipp

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

   https://success.trendmicro.com/en-US/contactus/

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

Bedrohungsenzyklopädie

Die meiste Malware besteht heutzutage aus komplexen Bedrohungen, bei denen zwei oder mehr Technologien miteinander kombiniert werden, um Computer-Sicherheitsprotokolle zu umgehen. Trend Micro bekämpft

diese komplexe Malware mit Produkten, die eine benutzerdefinierte Verteidigungsstrategie verfolgen. Die Bedrohungsenzyklopädie enthält eine ausführliche Liste mit Namen und Symptomen von verschiedenen kombinierten Bedrohungen, wie etwa bekannte Malware, Spam, bösartige URLs und bekannte Schwachstellen.

Auf https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware finden Sie weitere Informationen zu folgenden Themen:

- Malware und bösartige mobile Codes, die zum jeweiligen Zeitpunkt aktiv und im Umlauf sind
- Seiten mit Bedrohungsinformationen, die eine umfassende Ressource für Internet-Angriffe darstellen
- Beratung zu Internet-Bedrohungen bezüglich gezielten Angriffen und Sicherheitsbedrohungen
- Informationen zu Internet-Angriffen und Online-Trends
- Wöchentliche Malware-Berichte

Kontaktaufnahme mit Trend Micro

Sie erreichen Ihre Trend Micro Ansprechpartner in den Vereinigten Staaten telefonisch:

Adresse	Trend Micro Deutschland GmbH Parkring 29 85748 Garching
Telefon	+49 (0)89 8393 29700
Website	• https://www.trendmicro.com • https://success.trendmicro.com/en-US/contactus/

- Weltweite Support-Büros:

  https://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro Produktdokumentation:

  https://docs.trendmicro.com

Beschleunigung des Support-Anrufs

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

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

Verdächtige Inhalte an Trend Micro senden

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

Email Reputation Services

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

https://servicecentral.trendmicro.com/en-us/ers/

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

https://success.trendmicro.com/en-US/solution/KA-0001177

File-Reputation-Dienste

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

https://success.trendmicro.com/en-US/solution/KA-0002449

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

Web Reputation-Dienste

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

https://global.sitesafety.trendmicro.com/

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

Andere Ressourcen

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

Download-Center

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

https://www.trendmicro.com/download/

Falls ein Patch nicht angewendet wurde (Patches sind datiert), öffnen Sie die Readme-Datei, um festzustellen, ob er für Ihre Umgebung relevant ist. In der Readme-Datei finden Sie außerdem Installationsanweisungen.

Anhang A

Beispielbereitstellung

In diesem Abschnitt wird erläutert, wie Trend Micro Apex One basierend auf der Netzwerktopologie und den verfügbaren Netzwerkressourcen bereitgestellt wird. Verwenden Sie dies als Referenz bei der Planung der Bereitstellung von Trend Micro Apex One in Ihrer Organisation.

Basisnetzwerk

Abbildung 1 zeigt ein einfaches Netzwerk mit dem Trend Micro Apex One-Server und Agents, die direkt verbunden sind. Die meisten Unternehmensnetzwerke haben diese Konfiguration, bei der die LAN- (und/oder WAN-) Zugriffsgeschwindigkeit 10Mbps, 100Mbps oder 1Gbps beträgt. In diesem Szenario ist das endpunkt, das die Trend Micro Apex One-

Systemvoraussetzungen erfüllt und über ausreichende Ressourcen verfügt, ein idealer Kandidat für die Installation des Trend Micro Apex One-Servers.

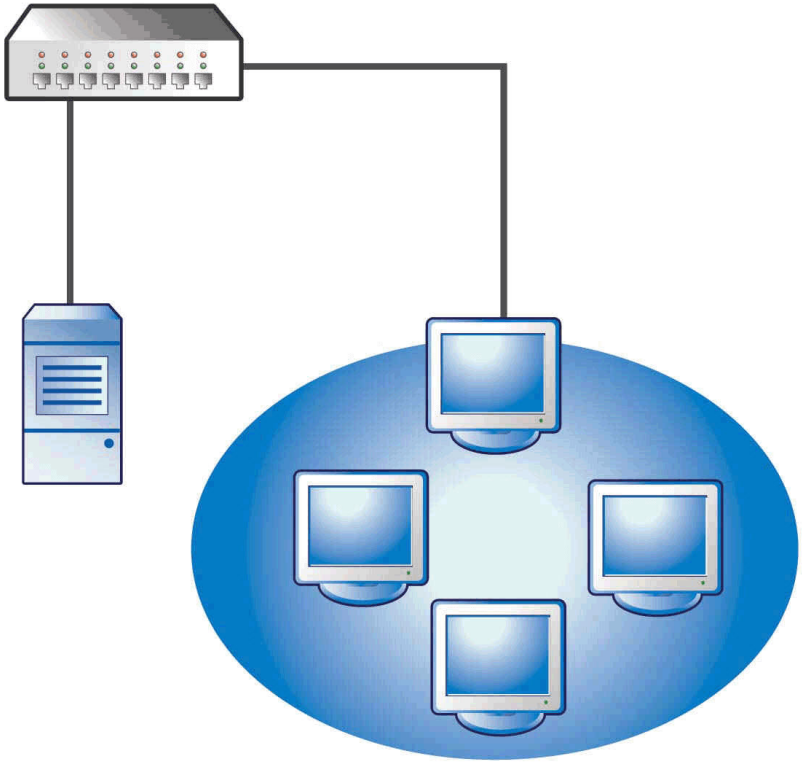


ABBILDUNG A-1. Grundlegende Netzwerktopologie

Mehrfachstandort-Netzwerk

Für ein Netzwerk mit mehreren Zugangspunkten und mehreren entfernten Standorten mit unterschiedlichen Bandbreiten:

- Analysieren Sie die Konsolidierungspunkte in Bezug auf Büros und Netzwerkbandbreite.
- Bestimmen Sie die aktuelle Bandbreitennutzung für jedes Büro.

Dies bietet ein klareres Bild, wie Trend Micro Apex One am besten eingesetzt werden kann. Abbildung 1 zeigt eine Netzwerk-Topologie mit mehreren Standorten.

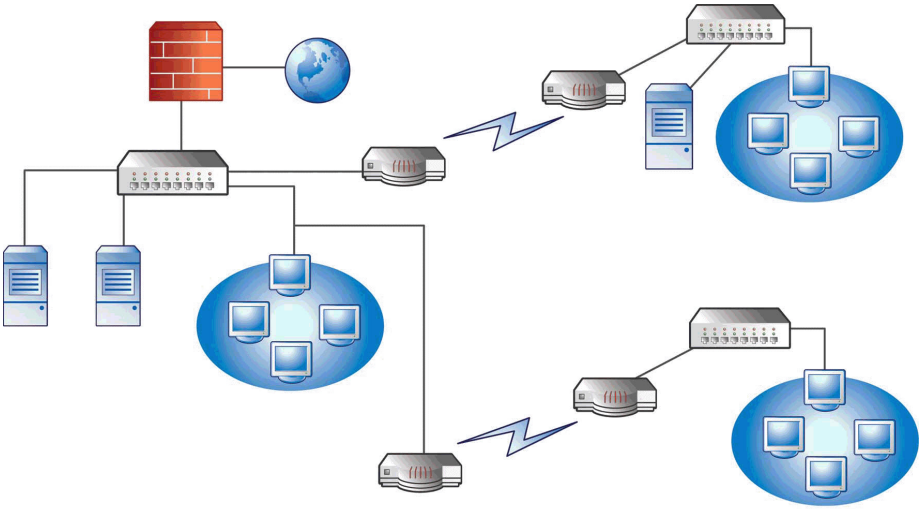


ABBILDUNG A-2. Netzwerktopologie mit mehreren Standorten

Netzwerkinformationen:

- Der WAN-Link der Remote-Site 1 weist während der Geschäftszeiten eine durchschnittliche Auslastung von etwa 70 Prozent auf. An diesem Standort gibt es 35 Agenten-Endpunkte.
- Die WAN-Verbindung des Remote-Standorts 2 liegt während der Geschäftszeiten durchschnittlich bei einer Auslastung von etwa 40 Prozent. An diesem Standort gibt es 9 Agenten-Endpunkte.

- Server 3 fungiert nur als Datei- und Druckserver für die Gruppe am Remote-Standort 1. Dieser Endpunkt ist ein möglicher Kandidat für die Installation des Trend Micro Apex One-Servers, könnte jedoch den zusätzlichen Verwaltungsaufwand nicht wert sein. Alle Server laufen unter Windows Server 2012. Das Netzwerk verwendet Active Directory, hauptsächlich für die Netzwerk-Authentifizierung.
- Alle Agentenendpunkte in der Hauptniederlassung, Remote-Standort 1 und Remote-Standort 2 laufen unter Windows Server 2012 oder Windows 7.

Vorbereitung eines Netzwerks mit mehreren Standorten

Prozedur

1. Identifizieren Sie den Endpunkt, auf dem der Trend Micro Apex One Server installiert werden soll.
2. Identifizieren Sie die verfügbaren Agent-Installationsmethoden und beseitigen Sie Methoden, die nicht den Anforderungen entsprechen. Siehe das *Administratorhandbuch* für weitere Informationen zu den Agent-Installationsmethoden.

   Mögliche Installationsmethoden:

   - Anmeldeskript-Setup

     Das Anmeldeskript-Setup funktioniert gut, wenn kein WAN vorhanden ist, da der lokale Datenverkehr keine Rolle spielt. Da jedoch mehr als 50 MB Daten an jeden Endpunkt übertragen werden, ist diese Option nicht praktikabel.

   - Remote-Installation von der Webkonsole

     Diese Methode ist gültig für alle mit dem LAN verbundenen Endpunkte im Hauptbüro. Da diese Endpunkte alle Windows Server 2012 ausführen, ist es einfach, das Paket auf die Endpunkte zu verteilen.

     Aufgrund der niedrigen Verbindungsgeschwindigkeit zwischen den beiden entfernten Standorten kann diese Bereitstellungsmethode

die verfügbare Bandbreite beeinträchtigen, wenn die Bereitstellung von Trend Micro Apex One während der Geschäftszeiten erfolgt. Nutzen Sie die gesamte Verbindungskapazität, um Trend Micro Apex One außerhalb der Geschäftszeiten bereitzustellen, wenn die meisten Menschen nicht mehr arbeiten. Wenn Benutzer jedoch ihre Endpunkte deaktivieren, ist die Bereitstellung von Trend Micro Apex One auf diesen Endpunkten nicht erfolgreich.

- Security Agent Paketbereitstellung

  Security Agent-Paketbereitstellung scheint die beste Option für die Bereitstellung an entfernten Standorten zu sein. Allerdings gibt es an Remote-Standort 2 keinen lokalen Server, um diese Option ordnungsgemäß zu unterstützen. Bei eingehender Betrachtung aller Optionen bietet diese Option die beste Abdeckung für die meisten Endpunkte.

Bereitstellung der Hauptniederlassung

Die einfachste Agent Bereitstellungsmethode, die in der Hauptniederlassung implementiert werden kann, ist die Remote-Installation über die Trend Micro Apex One Webkonsole. Siehe das *Administratorhandbuch* für das Verfahren.

Bereitstellung der Remote-Site 1

Die Bereitstellung an Remote-Standort 1 erfordert die Konfiguration des Microsoft Distributed File System (DFS). Für weitere Informationen über DFS, siehe http://support.microsoft.com/?kbid=241452. Nach der Konfiguration von DFS muss Server 3 am Remote-Standort 1 DFS aktivieren, um die bestehende DFS-Umgebung zu replizieren oder eine neue zu erstellen.

Eine geeignete Bereitstellungsmethode ist die Erstellung des Agent-Pakets im Microsoft Installer Package (MSI)-Format und die Bereitstellung des Agent-Pakets auf dem DFS. Siehe das *Administratorhandbuch* für das Verfahren. Da das Paket während des nächsten zeitgesteuerten Updates auf Server 3 repliziert wird, hat die Bereitstellung des Agent-Pakets minimale Auswirkungen auf die Bandbreite.

Sie können das Agent-Paket auch über Active Directory bereitstellen. Weitere Informationen finden Sie im *Administrator-Handbuch*.

Minimierung der Auswirkungen von Komponenten-Updates über das WAN hinweg

Prozedur

1. Weisen Sie einen Agent zu, der als Update-Agent auf Remote-Site 1 fungiert.
   a. Anmelden bei der Webkonsole und navigieren zu **Agents** > **Agent-Verwaltung**.
   b. In der Agent-Hierarchie wählen Sie die Agent als Update-Agent aus und klicken Sie auf **Einstellungen** > **Update-Agent-Einstellungen**.
2. Wählen Sie das Agents in Remote Site 1 aus, das Komponenten vom Update-Agenten aktualisiert.
   a. Navigieren Sie zu **Updates** > **Server** > **Update-Adresse**.
   b. Wählen Sie **Benutzerdefinierte Update-Adresse** aus und klicken Sie auf **Hinzufügen**.
   c. Geben Sie im angezeigten Bildschirm den IP-Adressbereich des endpunkte in Remote Site 1 ein.
   d. Wählen Sie **Update source** und wählen Sie dann den vorgesehenen Update-Agenten aus der Dropdown-Liste aus.

Bereitstellung der Remote-Site 2

Das Hauptproblem an Remote-Standort 2 ist die geringe Bandbreite. Allerdings sind 60 Prozent der Bandbreite während der Geschäftszeiten frei, wenn etwa 154 Kbit Bandbreite verfügbar sind.

Der beste Weg, um Security Agent zu installieren, ist die Verwendung desselben Agent-Pakets im MSI-Format, das in Remote Site 1 verwendet wird. Da jedoch kein verfügbarer Server vorhanden ist, können Sie kein verteiltes Dateisystem (DFS) verwenden.

Eine Möglichkeit besteht darin, Drittanbieter-Management-Tools zu verwenden, die es Administratoren ermöglichen, freigegebene Verzeichnisse auf entfernten endpunkte zu konfigurieren oder zu erstellen, ohne physischen Zugriff darauf zu haben. Nachdem das freigegebene Verzeichnis auf einem einzelnen endpunkt erstellt wurde, erfordert das Kopieren des Agent-Pakets in das Verzeichnis weniger Aufwand als die Installation des Agent auf neun endpunkte.

Verwenden Sie eine andere Active Directory-Richtlinie, aber geben Sie erneut nicht die DFS-Freigabe als Quelle an.

Diese Methoden halten den Installationsverkehr innerhalb des lokalen Netzwerks und minimieren den Verkehr über das WAN.

Um die Auswirkungen von Komponenten-Updates über das WAN zu minimieren, benennen Sie einen Agent als Update-Agent. Siehe *Bereitstellung der Remote-Site 1 auf Seite A-6* für weitere Informationen.

Stichwortverzeichnis

T

U

W

TREND MICRO DEUTSCHLAND GMBH

Parkring 29 85748 Garching Deutschland
Telefon: +49 (0)89 8393 29700
E-Mail: salesinfo_dach@trendmicro.com

www.trendmicro.com

Artikelnummer: APGM410021/250825