Trend Micro Apex One™

Patch 18

Handbuch für Administratoren

Für Unternehmen und mittelständische Betriebe

für Mac

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

http://docs.trendmicro.com/en-us/enterprise/apex-one-(mac).aspx

Trend Micro, das Trend Micro T-Ball-Logo, Trend Micro Apex One, Worry-Free und TrendLabs sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Produkt- oder Firmennamen können Marken oder eingetragene Marken ihrer Eigentümer sein.

Copyright © 2025. Trend Micro Incorporated. Alle Rechte vorbehalten.

Dokument-Nr.: APGM1810082/251127

Release-Datum: Dezember 2025

Geschützt durch U.S. Patent-Nr.: Angemeldete Patente.

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.

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 (Mac) 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

Vorwort 1
Trend Micro Apex One (Mac) Dokumentation 2
Zielgruppe 2
Textkonventionen 3
Begriff 3

Kapitel 1: Einführung in Trend Micro Apex One (Mac)

Informationen zu Trend Micro Apex One (Mac) 1-2
Neu in dieser Version 1-2
Wichtigste Funktionen und Vorteile 1-2
Trend Micro Apex One (Mac) Server 1-4
Die Trend Micro Apex One (Mac)Security Agent 1-5

Kapitel 2: Server installieren

Server-Installationsvoraussetzungen 2-2
Update-Adresse 2-4
Installieren des Trend Micro Apex One (Mac) Servers 2-6
Produkt zum ersten Mal aktivieren 2-7
Tasks nach der Installation auf dem Server ausführen 2-8
Trend Micro Apex One (Mac) Server deinstallieren 2-8

Kapitel 3: Erste Schritte

Erste Schritte – Aufgaben 3-2
Die Webkonsole 3-2
Webkonsole öffnen 3-3

Sicherheitszusammenfassung 3-4

Agent-Struktur 3-5

Agent-Struktur – Allgemeine Tasks 3-6
Agent-Struktur – Besondere Tasks 3-7

Gruppen 3-9

Gruppen hinzufügen 3-10
Löschen einer Gruppe oder Security Agent 3-10
Gruppen umbenennen 3-11
Moving Security Agents 3-11
Agents in eine andere Gruppe verschieben 3-11
Security Agents auf einen anderen Server verschieben 3-12

Widgets 3-13

Widget für Agent-Konnektivität (Mac) 3-13
Widget für Agent-Konnektivität (Mac) als Tabelle 3-14
Widget für Agent-Konnektivität (Mac) als Kreisdiagramm 3-15
Widget für Agent-Updates (Mac) 3-16
Widget für erkannte Sicherheitsrisiken (Mac) 3-16

Trend Micro Smart Protection 3-17

Smart Feedback 3-20

Kapitel 4: Security Agent installieren

Voraussetzungen für die Installation des Agents 4-2

Methoden und Setup-Dateien zur Agent-Installation 4-3

Auf einem einzelnen Endpunkt installieren 4-5

Vorgänge nach der Agent-Installation 4-12

Agent-Deinstallation 4-21

Kapitel 5: Den Schutz auf dem neuesten Stand halten

Komponenten 5-2

Update-Übersicht 5-4

Server-Update 5-4
Update-Adresse des Servers konfigurieren 5-5
Proxy-Einstellungen für Server-Updates konfigurieren 5-6
Server-Update-Methoden 5-7
Server-Updates zeitlich planen 5-8
Server manuell aktualisieren 5-8
Agent-Updates 5-9
Automatisches Update des Agents konfigurieren 5-11
Agent-Update-Einstellungen konfigurieren 5-12
Agent-Updates aus dem Übersichtsfenster starten 5-14
Agent-Updates aus dem Agent-Verwaltung-Fenster starten 5-15

Kapitel 6: Endpunkte vor Sicherheitsrisiken schützen

Info über Sicherheitsrisiken 6-2
Viren und Malware 6-2
Spyware und Grayware 6-4
Suchmethodentypen 6-5
Standard-Suchmethode 6-5
Suchmethoden im Vergleich 6-5
Suchmethode ändern 6-6
Wechsel von der intelligenten Suche zur herkömmlichen Suche 6-7
Wechsel von der herkömmlichen Suche zur intelligenten Suche 6-9
Suchtypen 6-11
Echtzeitsuche 6-12
Einstellungen der Echtzeitsuche konfigurieren 6-12
Echtzeitsuche: Registerkarte "Ziel" 6-13
Echtzeitsuche: Registerkarte "Aktion" 6-14
Manuelle Suche 6-15
Einstellungen für manuelle Suche konfigurieren 6-16
Manuelle Suche: Registerkarte "Ziel" 6-17
Manuelle Suche: Registerkarte "Aktion" 6-18

Zeitgesteuerte Suche 6-19
Einstellungen für zeitgesteuerte Suche konfigurieren 6-20
Zeitgesteuerte Suche: Registerkarte "Ziel" 6-21
Zeitgesteuerte Suche: Registerkarte "Aktion" 6-22
Jetzt durchsuchen 6-25
Jetzt durchsuchen starten 6-25
Unterstützte komprimierte Dateitypen 6-26
Suchaktionen 6-27
Suchausschlüsse 6-28
Ausschlusslisten für die Suche konfigurieren 6-29
Cache-Einstellungen für die Suche 6-33
Zwischenspeicher-Einstellungen für Suchen konfigurieren 6-34
Ausnahmelisten 6-35
Liste der vertrauenswürdigen Programme konfigurieren 6-35
Protokolle zu Suchvorgängen anzeigen 6-36
Benachrichtigungen und Protokolle für Sicherheitsrisiken .. 6-37
Einstellungen der Administratorbenachrichtigungen konfigurieren 6-38
Benachrichtigungen bei Sicherheitsrisiken für Administratoren konfigurieren 6-38
Ausbruchsbenachrichtigungen für Administratoren konfigurieren 6-39
Sicherheitsrisiko-Protokolle anzeigen 6-41
Suchergebnis 6-42
Dateien, die nicht gesäubert werden können 6-44
Zähler für Sicherheitsrisiken zurücksetzen 6-45

Kapitel 7: Endpunkte vor webbasierten Angriffen schützen

Internet-Bedrohungen 7-2
Web Reputation 7-2

Einstellungen für Web Reputation konfigurieren 7-3
Liste 'Zulässige/Gesperrte URL' konfigurieren 7-7
Web Reputation-Protokolle anzeigen 7-8

Kapitel 8: Die Gerätesteuerung verwenden

Gerätesteuerung 8-2
Berechtigungen für Speichergeräte 8-2
Einstellungen der Gerätesteuerung konfigurieren 8-3
Gerätelisten-Tool 8-5
Das Gerätelisten-Tool ausführen 8-6
Konfigurieren von Benachrichtigungen zur Gerätesteuerung für Security Agents 8-6
Protokolle der Gerätesteuerung anzeigen 8-7

Kapitel 9: Server und Security Agents verwalten

Berechtigungen und andere Einstellungen 9-2
Agent-Eigenschutz konfigurieren 9-2
Certified Safe Software Service aktivieren 9-3
Vorausschauendes Maschinenlernen aktivieren 9-4
Aktualisierung des Servers und Security Agents 9-5
Server aktualisieren 9-5
Security Agents upgraden 9-7
Protokolle verwalten 9-8
Lizenzen verwalten 9-9
Server-Datenbank sichern 9-10
Serverdatenbank wiederherstellen 9-11

Trend Micro Apex Central und Control Manager-Integration in dieser Version 9-12
Leistungsindikatoren-Widget 9-13
Einstellungen für Serververbindungen konfigurieren 9-13
Leistungsindikatoren konfigurieren 9-13
Widget-Einstellungen konfigurieren 9-15
Agent-Server-Kommunikationseinstellungen konfigurieren 9-15
Inaktive Security Agents 9-17
Automatisches Entfernen von inaktiven Security Agents 9-18
Agent-Symbole 9-18

Kapitel 10: Hilfe anzeigen

Fehlerbehebung 10-2
Zugriff auf die Webkonsole 10-2
Server-Deinstallation 10-4
Agent-Installation 10-5
Kommunikation zwischen Agent und Server 10-6
Allgemeiner Agent-Fehler 10-7
Technischer Support 10-8
Ressourcen zur Fehlerbehebung 10-8
Support-Portal verwenden 10-9
Bedrohungsenzyklopädie 10-9
Kontaktaufnahme mit Trend Micro 10-10
Beschleunigung des Support-Anrufs 10-11
Verdächtige Inhalte an Trend Micro senden 10-11
Email Reputation Services 10-11
File-Reputation-Dienste 10-12
Web Reputation-Dienste 10-12
Andere Ressourcen 10-12
Download-Center 10-12

Anhang A: IPv6-Unterstützung in Trend Micro Apex One (Mac)

IPv6-Unterstützung für Trend Micro Apex One (Mac) Server und Security Agents A-2

Trend Micro Apex One (Mac)Security Agent IPv6-Anforderungen A-2

Einschränkungen eines reinen IPv6-Servers A-2

Einschränkungen bei reinen IPv6-Agents A-3

IPv6-Adressen konfigurieren A-4

Fenster mit Anzeige von IP-Adressen A-5

Stichwortverzeichnis

Stichwortverzeichnis IN-1

Vorwort

Vorwort

Willkommen beim Trend Micro Apex One (Mac) Administratorhandbuch. Dieses Dokument enthält die Installationsanleitung für Trend Micro Apex One (Mac) Server und Agents sowie Informationen über die ersten Schritte und die Verwaltung von Server und Agents.

Trend Micro Apex One (Mac) Dokumentation

Die Dokumentation zu Trend Micro Apex One (Mac) umfasst Folgendes:

Dokumentation	Beschreibung
Administratorhandbuch	Ein PDF-Dokument mit Installationsanleitungen für Trend Micro Apex One (Mac) Server und Agents sowie Informationen über die ersten Schritte und die Verwaltung von Server und Agents.
Hilfe	HTML-Dateien mit praktischen Tipps, Benutzerhinweisen und Angaben zu den einzelnen Feldern
Readme-Datei	Enthält eine Liste bekannter Probleme und grundlegende Installationshinweise. Sie kann auch neueste Produktinformationen enthalten, die in anderen Dokumenten nicht zur Verfügung stehen.
Wissensdatenbank	Eine Online-Datenbank mit Informationen zur Problemlösung und Fehlerbehebung. Sie enthält die aktuellsten Hinweise zu bekannten Softwareproblemen. Die Wissensdatenbank finden Sie im Internet unter folgender Adresse: http://success.trendmicro.com

Die Produktdokumentation können Sie unter den folgenden Adresse anzeigen und herunterladen:

http://docs.trendmicro.com/en-us/enterprise/apex-one-(mac).aspx

Zielgruppe

Die Dokumentation zu Trend Micro Apex One (Mac) richtet sich an folgende Benutzer:

- Trend Micro Apex One (Mac) Administratoren: Verantwortlich für die Verwaltung von Trend Micro Apex One (Mac), einschließlich Installation und Verwaltung von Server und Security Agent. Es wird davon ausgegangen, dass diese Benutzer über umfassende Kenntnisse über Netzwerke und Server-Verwaltung verfügen.
- Endbenutzer: Benutzer, die den Trend Micro Apex One (Mac)Security Agent auf einem Endpunkt installiert haben. Die Computerkenntnisse

dieser Benutzergruppe reichen vom Anfänger bis zum erfahrenen Anwender.

Textkonventionen

Damit Sie Informationen leicht finden und einordnen können, kommen in der Dokumentation zu Trend Micro Apex One (Mac) folgende Konventionen zur Anwendung:

TABELLE 1. Textkonventionen

KONVENTION	BESCHREIBUNG
NUR GROSSBUCHSTABEN	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Befehlsschaltflächen, Registerkarten, Optionen und Tasks
Kursivdruck	Referenzen zu anderen Dokumenten oder neuen technischen Komponenten
<Text>	Text in spitzen Klammern soll durch Benutzerangaben ersetzt werden. Beispiel: `C:\Programme\<Dateiname>` kann `C:\Programme\beispiel.jpg` sein.
Hinweis	Enthält Konfigurationshinweise oder -empfehlungen
Tipp	Enthält Angaben zu bewährten Methoden und Trend Micro Empfehlungen
Warnung!	Enthält Warnungen zu Vorgängen, die Endpunkten im Netzwerk schaden können

Begriff

Die folgende Tabelle enthält offizielle Begriffe, die in der gesamten Trend Micro Apex One (Mac) Dokumentation verwendet werden:

Begriff	Beschreibung
Agent oder Security Agent	Das auf einem Endpunkt installierte Trend Micro Apex One (Mac)Security Agent Programm
Endpunkt	Der Computer, auf dem der Security Agent installiert ist
Agent-Benutzer (oder Benutzer)	Die Person, die den Security Agent auf dem Endpunkt verwaltet
Server	Trend Micro Apex One (Mac) Server-Programm
Server-Computer	Computer, auf dem der Trend Micro Apex One (Mac) Server installiert ist
Administrator (oder Trend Micro Apex One (Mac) Administrator)	Person, die den Trend Micro Apex One (Mac) Server verwaltet
Konsole	Die Benutzeroberfläche zur Konfiguration und Verwaltung der Einstellungen für den Trend Micro Apex One (Mac) Server und den Security Agent Die Konsole für das Server-Programm wird "Webkonsole" und die Konsole für das Security Agent-Programm wird "Agent-Konsole" genannt.
Sicherheitsrisiko	Oberbegriff für Viren, Malware, Spyware/Grayware und Internet-Bedrohungen
Produktdienst	Trend Micro Apex One (Mac) Dienst, der von der Microsoft Management Console (MMC) aus verwaltet wird
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 `/Library/Application Support/TrendMicro`

Begriff	Beschreibung
`Installationsordner des Servers`	Ordner auf dem Server-Computer, der die Programmdateien des Trend Micro Apex One (Mac) Servers enthält. Nach der Installation von Trend Micro Apex One (Mac) Server wird der Ordner im gleichen Verzeichnis wie der Apex One Server-Ordner erstellt. Wenn Sie die Standardeinstellungen bei der Installation von Apex One Server übernehmen, ist der Server-Installationsordner einer der folgenden: • `C:\Program Files\Trend Micro\OfficeScan\Addon\TMSM` • `C:\Program Files\Trend Micro\Apex One\Addon\TMSM` • `C:\Program Files (x86)\Trend Micro\OfficeScan\Addon\TMSM` • `C:\Program Files (x86)\Trend Micro\Apex One\Addon\TMSM`
Dualstapel	Entität, die sowohl IPv4- als auch IPv6-Adressen hat. Zum Beispiel: • Ein Dualstapel-Endpunkt ist ein Endpunkt mit IPv4- und IPv6-Adressen. • Ein Dualstapel-Agent ist ein Agent, der auf einem Dualstapel-Endpunkt installiert ist. • Ein Dualstapel-Proxy-Server wie beispielsweise DeleGate kann IPv4- in IPv6-Adressen konvertieren und umgekehrt.
Reine IPv4	Ein Gerät, das nur über IPv4-Adressen verfügt
Reine IPv6	Ein Gerät, das nur über IPv6-Adressen verfügt

Kapitel 1

Einführung in Trend Micro Apex One (Mac)

Dieses Kapitel führt in Trend Micro Apex One™ (Mac) ein und bietet einen Überblick über seine Funktionen und Fähigkeiten.

Informationen zu Trend Micro Apex One (Mac)

Trend Micro Apex One™ (Mac) bietet modernsten Schutz für Endpunkte vor Sicherheitsrisiken, kombinierten Bedrohungen und plattformunabhängigen webbasierten Angriffen.

Trend Micro Apex One (Mac) Server ist ein Plug-in-Programm, das in Trend Micro Produkte wie Apex One und Worry-Free Business Security integriert und über das Plug-in Manager-Framework installiert wird. Trend Micro Apex One (Mac) Server stellt Security Agents für Endpunkte bereit.

Neu in dieser Version

Trend Micro Apex One (Mac) bietet die folgenden neuen Funktionen und Verbesserungen.

Funktion/ Verbesserung	Beschreibung
Plattform-Unterstützung	Trend Micro Apex One (Mac)Security Agent kann jetzt auf macOS 26 Tahoe Endpunkten installiert werden.
Sicherheitsmodul-Verbesserung	Diese Version von Trend Micro Apex One (Mac) aktualisiert das iCore-Modul zur Verbesserung der Produktsicherheit.

Wichtigste Funktionen und Vorteile

Trend Micro Apex One (Mac) bietet die folgenden Funktionen und Vorteile:

TABELLE 1-1. Wichtigste Funktionen und Vorteile

FUNKTION	VORTEILE
intelligente Suche	Trend Micro Apex One (Mac) verwendet die Smart Scan, um den Suchvorgang effizienter zu gestalten. Diese Technologie basiert darauf, dass eine Vielzahl von zuvor auf dem lokalen Endpunkt gespeicherten Signaturen auf Smart Protection Quellen ausgelagert werden. Mit dieser Methode werden sowohl das System als auch das Netzwerk von der stetig zunehmenden Anzahl an Signatur-Updates auf Endpunktsysteme entlastet. Informationen über die intelligente Suche und die Verteilung auf Security Agents finden Sie unter *Suchmethodentypen auf Seite 6-5*.
Damage Cleanup Services	Damage Cleanup Services™ beseitigen vollautomatisch dateibasierte und Netzwerkviren sowie überreste von Viren und Würmern (Trojanern, Virendateien) auf Computern. Zur Abwehr von Bedrohungen und Störungen durch Trojaner verfügen die Damage Cleanup Services über folgende Funktionen: • Entdeckt und entfernt aktive Trojaner • Beendet durch Trojaner ausgelöste Prozesse • Repariert von Trojanern geänderte Systemdateien • Löscht von Trojanern hinterlassene Dateien und Anwendungen Die Damage Cleanup Services werden automatisch im Hintergrund ausgeführt. Es ist deshalb keine Konfiguration erforderlich. Die Benutzer bemerken nichts von diesem Vorgang. In einigen Fällen fordert Trend Micro Apex One (Mac) den Benutzer auf, den Endpunkt neu zu starten, um den Vorgang zum Entfernen eines Trojaners abzuschließen.
Schutz vor Sicherheitsrisiken	Trend Micro Apex One (Mac) schützt Endpunkte vor Sicherheitsrisiken, indem Dateien durchsucht werden und dann eine spezifische Aktion für jedes entdeckte Sicherheitsrisiko durchgeführt wird. Wird eine große Anzahl von Sicherheitsrisiken innerhalb kurzer Zeit erkannt, deutet dies auf einen Virenausbruch hin. Trend Micro Apex One (Mac) benachrichtigt Sie über jeden Ausbruch, sodass Sie sofort entsprechende Maßnahmen ergreifen können, wie z. B. die betroffenen Endpunkte von der Schadsoftware zu befreien und sie so lange zu isolieren, bis keine Bedrohung mehr von ihnen ausgeht.

Funktion	Vorteile
Web Reputation	Web Reputation schützt Endpunkte innerhalb oder außerhalb des Unternehmensnetzwerks proaktiv vor bösartigen und potenziell gefährlichen Websites. Web Reputation durchbricht die Infektionskette und verhindert den Download bösartigen Codes. Sie können die Glaubwürdigkeit der Websites und Webseiten überprüfen, indem Sie Apex One in den Smart Protection Server oder das Trend Micro Smart Protection Network integrieren.
Zentrale Verwaltung	Eine webbasierte Management-Konsole ermöglicht dem Administrator einen übersichtlichen Zugriff auf alle Security Agents im Netzwerk. Über die Webkonsole wird außerdem die automatische Verteilung von Sicherheitsrichtlinien, Pattern-Dateien und Software-Updates auf allen Security Agent koordiniert. Der Administrator kann das Netzwerk remote verwalten und Einstellungen für einzelne Agents oder Agent-Gruppen vornehmen.

Trend Micro Apex One (Mac) Server

Der Trend Micro Apex One (Mac) Server ist der zentrale Speicherort für Informationen über alle vorhandenen Security Agent-Konfigurationen, Sicherheitsrisiko-Protokolle und Updates.

Der Server erfüllt zwei wichtige Funktionen:

- Überwacht und verwaltet die Security Agents
- Lädt Komponenten herunter, die von Security Agents benötigt werden. Standardmäßig lädt der Trend Micro Apex One (Mac) Server Komponenten vom Trend Micro ActiveUpdate Server herunter und verteilt sie dann auf die Security Agents.

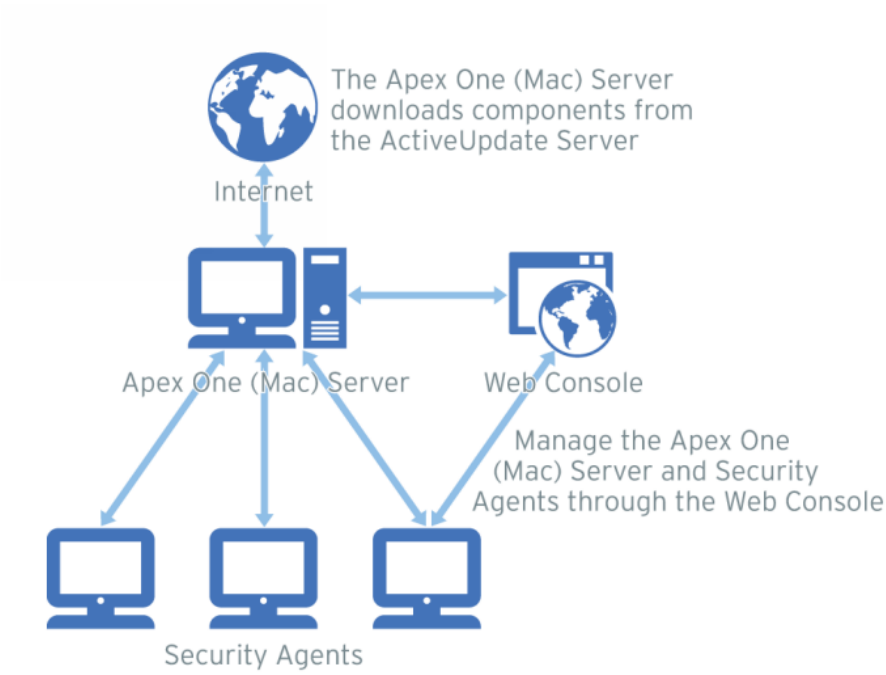


ABBILDUNG 1-1. Funktionsweise von Trend Micro Apex One (Mac) Server

Trend Micro Apex One (Mac) ermöglicht eine bidirektionale Kommunikation zwischen dem Server und Security Agents in Echtzeit. Sie können die Security Agents über eine browserbasierte Webkonsole verwalten, die Sie von einer beliebigen Stelle des Netzwerks aus aufrufen können. Der Server kommuniziert mit Security Agents über das ActiveMQ™ Protokoll.

Die Trend Micro Apex One (Mac)Security Agent

Schützen Sie Endpunkte vor Sicherheitsrisiken, indem Sie das Trend Micro Apex One (Mac)Security Agent auf jedem Endpunkt installieren. Das Security Agent bietet drei Suchtypen:

- Echtzeitsuche

- Zeitgesteuerte Suche
- Manuelle Suche

Der Security Agent meldet sich beim übergeordneten Trend Micro Apex One (Mac)-Server, von dem er installiert wurde. Der Security Agent sendet Ereignisse und Statusinformationen in Echtzeit an den Server. Security Agents kommunizieren mit dem Server über das ActiveMQ-Protokoll.

Kapitel 2

Server installieren

In diesem Kapitel werden die Systemvoraussetzungen und die Installationsschritte für Trend Micro Apex One (Mac) Server beschrieben.

Server-Installationsvoraussetzungen

Wichtig

Bevor Sie Apex One (Mac) Patch 2 und höher installieren oder aktualisieren, stellen Sie sicher, dass das Zertifikat für Microsoft-Internetinformationsdienste (IIS) nicht abgelaufen ist.

Weitere Informationen finden Sie unter https://success.trendmicro.com/solution/000283033.

Nachfolgend sind die Systemvoraussetzungen für die Installation von Trend Micro Apex One (Mac) Server aufgeführt:

TABELLE 2-1. Server-Installationsvoraussetzungen

RESSOURCE	VORAUSSETZUNGEN
Apex One-Server	2019 oder später
OfficeScan Server	XG oder höher
Plug-in Manager	2.0 und höher
RAM	Mindestens 1 GB, 2 GB empfohlen

Ressource	Voraussetzungen

Verfügbarer Speicherplatz	• Mindestens 7 GB, wenn der OfficeScan Server auf dem Systemlaufwerk installiert wird (in der Regel Laufwerk C:)
	• Mindestens 5 GB, wenn der Apex One Server auf dem Systemlaufwerk installiert wird (in der Regel Laufwerk C:)
	• Falls der OfficeScan- oder Apex One-Server nicht auf dem Systemlaufwerk installiert wird:
	  • Mindestens 7 GB auf dem Laufwerk, auf dem der OfficeScan Server installiert wird. Der Trend Micro Apex One (Mac) Server wird auf diesem Laufwerk installiert.
	  • Mindestens 5 GB auf dem Laufwerk, auf dem der Apex One Server installiert wird. Der Trend Micro Apex One (Mac) Server wird auf diesem Laufwerk installiert.
	  • Mindestens 7 GB auf dem Systemlaufwerk. Vom Trend Micro Apex One (Mac) Server genutzte Programme von Drittanbietern werden auf diesem Laufwerk installiert.

Ressource	Voraussetzungen

Andere	• Microsoft™ .NET Framework 3.5 und 4.6.1
	• Microsoft Windows™ Installer 3.1 und höher
	• Die folgenden Programme anderer Hersteller werden automatisch installiert, wenn sie nicht vorhanden sind:
	  • Microsoft SQL Server 2008 R2 Express, 2016 Express oder 2016 SP1 Express
	  • Apache™ ActiveMQ 5.15.4
	  • Microsoft Visual C++ 2017 Redistributable
	
	Hinweis
	• Die Installation der Java-Laufzeitumgebung (JRE) ist erforderlich, wenn Sie Trend Micro Apex One (Mac) auf einem OfficeScan-Server installieren.
	• Installieren Sie JRE 1.8 oder höher, um eine möglichst hohe Leistung zu erzielen. Installieren Sie je nach dem Betriebssystem des Hostcomputers JRE für Windows x86 oder JRE für Windows x64.

Update-Adresse

Bevor Sie Trend Micro Apex One (Mac) Server installieren, überprüfen Sie die Update-Adresse von Plug-in Manager in der OfficeScan oder Apex One Webkonsole unter **Updates** > **Server** > **Update-Adresse**. Die Update-Adresse kann eine der folgenden sein:

Tabelle 2-2. Mögliche Update-Adressen

Ausgewählte Update-Adresse	Beschreibung und Anleitung
`ActiveUpdate Server`	Der Trend Micro ActiveUpdate Server ist die Standard-Update-Adresse. Für die Verbindung zu diesem Server ist eine Internet-Verbindung erforderlich. Verbindet sich der Security Server über einen Proxy-Server mit dem Internet, stellen Sie sicher, dass die Internet-Verbindung über die Proxy-Einstellungen hergestellt werden kann.
`Andere Update-Adresse`	Wenn Sie verschiedene Update-Adressen angegeben haben: • Stellen Sie sicher, dass sich der Servercomputer mit der ersten Update-Adresse auf der Liste verbinden kann. Ist dies nicht der Fall, stellt der Servercomputer auch keine Verbindung zu den anderen Update-Adressen her. • Überprüfen Sie, ob die erste Update-Adresse die neueste Version der Komponentenliste von Plug-in Manager (`OSCE_AOS_COMP_LIST.xml`) und das Installationspaket für Trend Micro Apex One (Mac) enthält. Wenden Sie sich an Ihren Support-Anbieter, um Unterstützung beim Einrichten einer Update-Adresse zu erhalten.
`Intranet-Site, die eine Kopie der aktuellen Datei enthält`	Wenn es sich bei der Update-Adresse um eine Intranet-Site handelt: • Überprüfen Sie, ob der Servercomputer mit der Update-Adresse verbunden ist. • Überprüfen Sie, ob die Update-Adresse die neueste Version der Komponentenliste von Plug-in Manager (`OSCE_AOS_COMP_LIST.xml`) und das Installationspaket für Trend Micro Apex One (Mac) enthält. Wenden Sie sich an Ihren Support-Anbieter, um Unterstützung beim Einrichten einer Intranet-Adresse zu erhalten.

Installieren des Trend Micro Apex One (Mac) Servers

Wichtig

Bevor Sie Apex One (Mac) Patch 2 und höher installieren oder aktualisieren, stellen Sie sicher, dass das Zertifikat für Microsoft-Internetinformationsdienste (IIS) nicht abgelaufen ist.

Weitere Informationen finden Sie unter https://success.trendmicro.com/solution/000283033.

Prozedur

1. Führen Sie Folgendes NUR dann aus, wenn Sie Trend Micro Apex One (Mac) auf einem Server mit einer Domänencontroller-Rolle installieren:
   a. Wechseln Sie in den Ordner `<server installation folder>\PCCSRV\Admin\Utility\SQL`.
   b. Öffnen Sie die Datei `InstallCfgFile.ini` mit Hilfe eines Texteditors.
   c. Ändern Sie den Wert von `SQLSVCACCOUNT` von `NT AUTHORITY\NETWORK SERVICE` in `NT AUTHORITY\SYSTEM`.
   d. Speichern Sie die Datei.
2. Öffnen Sie die Apex One oder OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
3. Navigieren Sie zum Bereich **Trend Micro Apex One (Mac)** und klicken Sie auf **Download**.

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

   Plug-in Manager lädt das Paket nach `<server installation folder>\PCCSRV\Download` herunter.

`<server installation folder>` ist normalerweise `C:\Program Files\Trend Micro\OfficeScan` oder `C:\Program Files\Trend Micro\Apex One`.

4. Verfolgen Sie den Download-Fortschritt.

   Sie können während des Downloads zu anderen Fenstern navigieren.

   Wenn beim Herunterladen des Pakets Probleme auftreten, überprüfen Sie über die Apex One oder OfficeScan Webkonsole die Server-Update-Protokolle. Klicken Sie im Hauptmenü auf **Protokolle** > **Server-Updates**.

5. Klicken Sie nach Abschluss des Download-Vorgangs auf **Installieren**, um Trend Micro Apex One (Mac) zu installieren.

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

   Die Installation beginnt.

7. Verfolgen Sie den Installationsfortschritt. Nach der Installation wird das Fenster Plug-in Manager neu geladen.

Produkt zum ersten Mal aktivieren

Prozedur

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

2. Navigieren Sie zum Bereich **Trend Micro Apex One (Mac)** und klicken Sie auf **Programm verwalten**.

3. Geben Sie den Aktivierungscode für das Produkt ein und klicken Sie auf **Speichern**. Achten Sie bei der Eingabe auf Groß- und Kleinschreibung.

   Wenn Sie über keinen Aktivierungscode verfügen, klicken Sie auf **Online registrieren**, um auf die Trend Micro Registrierungswebsite zuzugreifen. Nach Abschluss der Registrierung erhalten Sie von Trend Micro eine E-Mail mit dem Aktivierungscode. Sie können dann mit der Aktivierung fortfahren.

Wenn Sie die Lizenz einer Testversion aktiviert haben, führen Sie ein Upgrade auf die Vollversion aus, bevor die Lizenz abläuft.

4. Klicken Sie im Fenster der Lizenzdetails auf **Starten**, um die Webkonsole zu öffnen.
5. Klicken Sie auf **Starten**, um die Webkonsole zu öffnen.

Tasks nach der Installation auf dem Server ausführen

Prozedur

1. Prüfen Sie, dass die folgenden Dienste auf der Microsoft Management Console angezeigt werden:
   - **ActiveMQ für Apex One (Mac)**
   - **Apex One (Mac) Hauptdienst**
2. Prüfen Sie im Windows Task Manager, dass der folgende Prozess ausgeführt wird: **TMSMMainService.exe**
3. Prüfen Sie im Registrierungs-Editor, dass der folgende Registrierungsschlüssel vorhanden ist: `HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_TMSM`
4. Stellen Sie sicher, dass sich die Trend Micro Apex One (Mac) Serverdateien im <*Server-Installationsordner*> befinden.

Trend Micro Apex One (Mac) Server deinstallieren

Prozedur

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

2. Navigieren Sie zum Bereich Trend Micro Apex One (Mac) und klicken Sie auf **Deinstallieren**.
3. Verfolgen Sie den Deinstallationsfortschritt. Sie können während der Deinstallation zu anderen Fenstern navigieren. Nach Abschluss der Deinstallation kann der Trend Micro Apex One (Mac) Server wieder installiert werden.

Hinweis

Die von Trend Micro Apex One (Mac) genutzte Java Runtime Environment (JRE) wird vom Deinstallationspaket nicht entfernt. Falls sie von keiner anderen Anwendung benötigt wird, können Sie die JRE manuell entfernen.

Kapitel 3

Erste Schritte

In diesem Kapitel werden die ersten Schritte mit Trend Micro Apex One (Mac) und Einstellungen für die Erstkonfiguration beschrieben.

Erste Schritte – Aufgaben

„Erste Schritte – Aufgaben“ bietet einen umfassenden Überblick über die Verfahren, die erforderlich sind, um Trend Micro Apex One (Mac) so schnell wie möglich auszuführen.

Prozedur

1. Agent-Server-Kommunikationseinstellungen konfigurieren.

   Weitere Informationen finden Sie unter *Agent-Server-Kommunikationseinstellungen konfigurieren auf Seite 9-15*.

2. Wenn eine Firewall auf dem Computer verwendet wird, auf dem Sie den Trend Micro Apex One (Mac) Server installiert haben, stellen Sie sicher, dass die Firewall den Datenverkehr über den Listening-Port für die Kommunikation zwischen Agent und Server nicht blockiert.

   Falls auf dem Endpunkt die Apex One Security Agent Firewall aktiviert wurde, fügen Sie eine Richtlinienausnahme hinzu, die eingehenden und ausgehenden Datenverkehr über den Listening-Port zulässt.

3. Installieren Sie den Trend Micro Apex One (Mac)Security Agent auf Endpunkten.

   Weitere Informationen finden Sie unter *Security Agent installieren auf Seite 4-1*.

Die Webkonsole

Die Webkonsole ist die zentrale Stelle zur Überwachung von Security Agents und zur Konfiguration der Einstellungen, die von Security Agents übernommen werden. Sie enthält verschiedene Standardeinstellungen und -werte, die Sie entsprechend Ihren Sicherheitsanforderungen und -voraussetzungen konfigurieren können.

Über die Webkonsole können Sie folgende Aktionen ausführen:

- Verwalten Sie Security Agents auf Endpunkten installiert

- Organisieren Sie Security Agents in logische Gruppen zur gleichzeitigen Konfiguration und Verwaltung
- Auf einem oder mehreren Endpunkten die Virensucheinstellungen festlegen und die Suche starten
- Konfigurieren Sie Sicherheitsrisiko-Benachrichtigungen und sehen Sie sich die von Security Agents gesendeten Protokolle an
- Ausbruchskriterien und -benachrichtigungen konfigurieren

Webkonsole öffnen

Vorbereitungen

Sie können die Webkonsole über jeden Endpunkt im Netzwerk öffnen, der über die folgende Ausstattung verfügt:

- Monitor mit einer Mindestauflösung von 1024 x 768 bei 256 Farben oder mehr
- Webbrowser:
  - Microsoft Internet Explorer 10
  - Microsoft Edge
  - Microsoft Edge Chromium
  - Firefox
  - Chrome
  - Safari

Prozedur

1. Geben Sie im Webbrowser die URL des Apex One- oder OfficeScan-Servers ein.
2. Geben Sie den Benutzernamen und das Kennwort ein, um sich am Apex One oder OfficeScan Server anzumelden.
3. Klicken Sie im Hauptmenü auf **Plug-ins**.

4. Navigieren Sie zum Bereich **Trend Micro Apex One (Mac)** und klicken Sie auf **Programm verwalten**.

Sicherheitszusammenfassung

Das Fenster **Übersicht** wird angezeigt, wenn Sie die Trend Micro Apex One (Mac)-Webkonsole öffnen oder im Hauptmenü auf **Übersicht** klicken.

Tipp

Aktualisieren Sie dieses Fenster regelmäßig, um die aktuellsten Informationen zu erhalten.

Agents

Im Bereich **Agents** werden folgende Informationen angezeigt:

- Der Verbindungsstatus aller Security Agents mit dem Trend Micro Apex One (Mac)-Server. Durch Klicken auf einen Link wird der Agentenbaum geöffnet, in dem Sie Einstellungen für die Security Agents konfigurieren können.
- Anzahl der entdeckten Sicherheitsrisiken und Internet-Bedrohungen
- Anzahl der Endpunkte mit entdeckten Sicherheitsrisiken und Internet-Bedrohungen. Durch Klicken auf eine Anzahl wird die Agent-Struktur geöffnet und eine Liste der Endpunkte angezeigt, auf denen Sicherheitsrisiken und Internet-Bedrohungen entdeckt wurden. In der Agent-Struktur können Sie folgende Tasks ausführen:
  - Wählen Sie ein oder mehrere Security Agents aus, klicken Sie auf **Protokolle** > **Sicherheitsrisiko-Protokolle**, und geben Sie dann die Protokollkriterien an. Überprüfen Sie in dem angezeigten Bildschirm die **Ergebnisse**-Spalte, um festzustellen, ob die Suchaktionen bei den Sicherheitsrisiken erfolgreich durchgeführt wurden.

    Eine Liste aller Suchergebnisse finden Sie unter *Suchergebnis auf Seite 6-42*.

- Wählen Sie einen oder mehrere Security Agents aus, klicken Sie auf **Protokolle** > **Web Reputation-Protokolle** und geben Sie die Protokollkriterien an. Prüfen Sie im daraufhin angezeigten Fenster die Liste der gesperrten Websites. Websites, die nicht gesperrt werden sollen, können der Liste der zulässigen URLs hinzugefügt werden.

  Weitere Informationen finden Sie unter *Liste 'Zulässige/Gesperrte URL' konfigurieren auf Seite 7-7*.

Status des Fundes

Die Tabelle **Status des Fundes** enthält die Gesamtanzahl erkannter Sicherheitsrisiken und Internetbedrohungen sowie die Anzahl der betroffenen Endpunkte.

Update-Status

In der Tabelle **Update-Status** sind Informationen über die Komponenten von Trend Micro Apex One (Mac) und das Security Agent-Programm enthalten, das Endpunkte vor Sicherheitsrisiken schützt.

Tasks in dieser Tabelle:

- Aktualisieren Sie nicht aktuelle Komponenten sofort.

  Weitere Informationen finden Sie unter *Agent-Updates aus dem Übersichtsfenster starten auf Seite 5-14*.

- Aktualisieren Sie Security Agents auf die neueste Programmversion oder Build, wenn Sie kürzlich den Server aktualisiert haben.

  Eine Anleitung für Agent-Upgrades finden Sie unter *Aktualisierung des Servers und Security Agents auf Seite 9-5*.

Agent-Struktur

Die Trend Micro Apex One (Mac) Agent-Struktur zeigt alle Security Agents an, die der Server derzeit verwaltet. Alle Security Agents gehören einer bestimmten Gruppe an. Verwenden Sie die Menüeinträge über der Agent-

Struktur, um eine Konfiguration gleichzeitig für alle Security Agents einer Gruppe zu konfigurieren, zu verwalten und anzuwenden.

Agent-Struktur – Allgemeine Tasks

Die folgende Übersicht enthält die allgemeinen Tasks, die Sie in der Agent-Struktur durchführen können:

Prozedur

- Klicken Sie auf das Stammsymbol ( ), um alle Gruppen und Agents auszuwählen. Wenn Sie zuerst das Stammsymbol und anschließend einen Menüeintrag über der Agent-Struktur auswählen, wird ein Fenster mit den Konfigurationseinstellungen angezeigt. In diesem Fenster können Sie eine der folgenden allgemeinen Optionen auswählen:
  - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf neu zu einer vorhandenen/zukünftigen Gruppe hinzukommende Agents an. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
  - **Nur auf zukünftige Gruppen anwenden**: Wendet Einstellungen nur auf Agents an, die zu zukünftigen Gruppen hinzugefügt wurden. Bei dieser Option werden die Einstellungen nicht auf neue Agents angewendet, die zu einer vorhandenen Gruppe hinzukommen.
- Klicken Sie zur Auswahl mehrerer aufeinander folgender Gruppen oder Agents auf die erste Gruppe oder den ersten Agent des Bereichs. Halten Sie die Umschalttaste gedrückt und klicken Sie dann auf die letzte Gruppe oder den letzten Agent des Bereichs.
- Um mehrere nicht unmittelbar aufeinander folgende Gruppen oder Agents auszuwählen, halten Sie die Strg-Taste gedrückt und klicken auf die gewünschten Gruppen oder Agents.
- Sie können nach einem bestimmten zu verwaltenden Agent suchen, indem Sie den vollständigen Namen des Endpunkts oder einen Teil des Namens im Textfeld **Nach Endpunkten suchen** eingeben. In der Agent-Struktur wird eine Liste mit übereinstimmenden Agent-Namen angezeigt.

- Sie können Agents durch Klicken auf den Spaltennamen nach den Informationen in den Spalten sortieren.
- Zeigen Sie die Gesamtanzahl der Agents unter der Agent-Struktur an.
- Klicken Sie auf die Schaltfläche **Exportieren** (Export), um die Liste und den Status für Agents aus der Agent-Struktur in eine Datei im `csv`.-Format zu exportieren.

Agent-Struktur – Besondere Tasks

Über der Agent-Struktur befinden sich Menüeinträge, mit denen Sie folgende Tasks durchführen können:

Menüschaltfläche	Aufgabe
Tasks	• Agent-Komponenten aktualisieren. Weitere Informationen finden Sie unter *Agent-Updates auf Seite 5-9*. • "Jetzt durchsuchen" auf Endpunkten ausführen. Weitere Informationen finden Sie unter *Jetzt durchsuchen auf Seite 6-25*.

Menüschaltfläche	Aufgabe

Einstellungen	• Konfigurieren Sie die Suchmethode.
	Weitere Informationen finden Sie unter *Suchmethodentypen auf Seite 6-5*.
	• Sucheinstellungen konfigurieren.
	  • *Manuelle Suche auf Seite 6-15*
	  • *Echtzeitsuche auf Seite 6-12*
	  • *Zeitgesteuerte Suche auf Seite 6-19*
	  • *Suchausschlüsse auf Seite 6-28*
	  • *Cache-Einstellungen für die Suche auf Seite 6-33*
	• Web Reputation-Einstellungen konfigurieren.
	Weitere Informationen finden Sie unter *Einstellungen für Web Reputation konfigurieren auf Seite 7-3*.
	• Konfigurieren Sie den Agent-Eigenschutz.
	Weitere Informationen finden Sie unter *Agent-Eigenschutz konfigurieren auf Seite 9-2*.
	• Einstellungen der Gerätesteuerung konfigurieren
	Weitere Informationen finden Sie unter *Einstellungen der Gerätesteuerung konfigurieren auf Seite 8-3*.
	• Aktualisierungseinstellungen konfigurieren.
	Weitere Informationen finden Sie unter *Agent-Update-Einstellungen konfigurieren auf Seite 5-12*.
	• Liste der vertrauenswürdigen Programme konfigurieren.
	Weitere Informationen finden Sie unter *Liste der vertrauenswürdigen Programme konfigurieren auf Seite 6-35*.
	• Die Einstellung für das Vorausschauende Maschinenlernen konfigurieren.
	Weitere Informationen finden Sie unter *Vorausschauendes Maschinenlernen aktivieren auf Seite 9-4*.

Menüschaltfläche	Aufgabe
Protokolle	Sehen Sie Protokolle ein und setzen Sie Statistiken zurück. • *Sicherheitsrisiko-Protokolle anzeigen auf Seite 6-41* • *Web Reputation-Protokolle anzeigen auf Seite 7-8* • *Protokolle zu Suchvorgängen anzeigen auf Seite 6-36* • *Protokolle der Gerätesteuerung anzeigen auf Seite 8-7* • *Zähler für Sicherheitsrisiken zurücksetzen auf Seite 6-45*
Agent-Struktur verwalten	Trend Micro Apex One (Mac) Gruppen verwalten. Weitere Informationen finden Sie unter *Gruppen auf Seite 3-9*.

Gruppen

Eine Gruppe in Trend Micro Apex One (Mac) ist eine Menge von Agents, die dieselbe Konfiguration teilen und dieselben Aufgaben ausführen. Indem Sie Agents in Gruppen organisieren, können Sie eine Konfiguration gleichzeitig für alle Agents der Gruppen konfigurieren, verwalten und anwenden.

Agents können einfacher verwaltet werden, wenn Sie diese nach Abteilungszugehörigkeit oder Aufgabenbereich gruppieren. Sie können stärker gefährdete Clients in einer Gruppe zusammenfassen, damit Sie für alle einen höheren Schutz konfigurieren können. Sie können Gruppen hinzufügen oder umbenennen, Agents in eine andere Gruppe oder auf einen anderen Server verschieben oder Agents permanent entfernen. Ein aus der Agent-Struktur entfernter Agent wird nicht automatisch vom Endpunkt deinstalliert. Der Agent kann noch immer serverabhängige Funktionen durchführen, wie das Update der Komponenten. Der Server weiß jedoch nicht, dass der Agent vorhanden ist, und kann ihm daher keine Konfigurationen oder Benachrichtigungen senden.

Wenn ein Agent vom Endpunkt deinstalliert wurde, wird er nicht automatisch aus der Agent-Struktur entfernt, und sein Verbindungsstatus wird in "Offline" geändert. Sie müssen den Agent manuell aus der Agent-Struktur entfernen.

Gruppen hinzufügen

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie auf **Agent-Struktur verwalten** > **Gruppe hinzufügen**.
3. Geben Sie einen Namen für die Gruppe ein, die Sie hinzufügen möchten.
4. Klicken Sie auf **Hinzufügen**.

   Die neue Gruppe wird nun in der Agent-Struktur angezeigt.

Löschen einer Gruppe oder Security Agent

Vorbereitungen

Bevor Sie eine Gruppe löschen, überprüfen Sie, ob Security Agents zur Gruppe gehören und verschieben Sie dann die Security Agents in eine andere Gruppe.

Details zum Verschieben von Agents finden Sie unter *Agents in eine andere Gruppe verschieben auf Seite 3-11*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Wählen Sie in der Agent-Hierarchie bestimmte Gruppen oder Security Agents aus.
3. Klicken Sie auf **Agent-Struktur verwalten** > **Gruppe/Agent entfernen**.
4. Klicken Sie auf **OK**, um das Löschen zu bestätigen.

Gruppen umbenennen

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Wählen Sie in der Agent-Struktur die Gruppe aus, die Sie umbenennen möchten.
3. Klicken Sie auf **Agent-Struktur verwalten** > **Gruppe umbenennen**.
4. Geben Sie einen neuen Namen für die Gruppe ein.
5. Klicken Sie auf **Umbenennen**.

   Der neue Gruppenname wird nun in der Agent-Struktur angezeigt.

Moving Security Agents

Sie können Security Agents in eine andere Agentengruppe oder auf den Trend Micro Apex One (Mac) Server verschieben.

Agents in eine andere Gruppe verschieben

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Wählen Sie in der Agent-Struktur einen oder mehrere Agents aus.
3. Klicken Sie auf **Agent-Hierarchie verwalten** > **Agent verschieben**.
4. Wählen Sie **Ausgewählte Agents in andere Gruppe verschieben**.
5. Wählen Sie die Gruppe aus dem Listenfeld aus.
6. Legen Sie fest, ob die Einstellungen der neuen Gruppe auf die Agents angewendet werden sollen.

Tipp

Sie können Agents auch per Drag & Drop in eine andere Gruppe innerhalb der Agent-Struktur verschieben.

7. Klicken Sie auf **Verschieben**.

Security Agents auf einen anderen Server verschieben

Hinweis

- Sie können Security Agents nur auf einen anderen Trend Micro Apex One (Mac)-Server mit derselben oder einer höheren Version verschieben.
- Wenn Sie Security Agents von einem lokalen Trend Micro Apex One (Mac) Server auf einen SaaS-Server (Server as a Service) (oder umgekehrt) verschieben, stellen Sie sicher, dass Trend Micro Apex One (Mac)Security Agents über den Listening-Port mit dem Server kommunizieren können und dass keine Anwendung genau diesen Port auf den Security Agent Endpunkten verwendet.

  Die folgende Tabelle enthält die Listening-Ports.

  TABELLE 3-1. Kommunikationsports zwischen Agent und Server

SERVERVARIANTE	LISTENING-PORT
Lokal	• Für Security Agent Version 3.5.3xxx oder später: 4343 • Für Security Agent Version 3.5.2xxx oder früher: 61617
SaaS	443

  Weitere Informationen finden Sie unter *Agent-Server-Kommunikationseinstellungen konfigurieren auf Seite 9-15*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Im Agentenbaum einen oder mehrere Security Agents auswählen.
3. Klicken Sie auf **Agent-Hierarchie verwalten** > **Agent verschieben**.
4. Wählen Sie **Ausgewählte Agents auf anderen Server verschieben:**.
5. Geben Sie den Namen oder die Adresse des Servers und die HTTPS-Portnummer ein.
6. Wählen Sie **Verschieben von Offline-Agents erzwingen**, um offline Security Agents auf den angegebenen Server zu verschieben.

   Hinweis

   Wenn ein offline Security Agent nach 7 Tagen nicht online ist, bleibt das Security Agent auf dem ursprünglichen Server und wird nicht auf den angegebenen Server verschoben.

7. Klicken Sie auf **Verschieben**.

Widgets

Verwalten Sie Trend Micro Apex One (Mac) Widgets auf dem Apex One Dashboard. Die Widgets stehen nach der Aktivierung von Trend Micro Apex One (Mac) zur Verfügung.

Informationen über das Arbeiten mit Widgets finden Sie in der Dokumentation zu Apex One.

Widget für Agent-Konnektivität (Mac)

Das Widget für Agent-Konnektivität (Mac) zeigt den Status der Verbindung zwischen den Agents und dem Trend Micro Apex One (Mac) Server an. Daten werden in einer Tabelle und einem Kreisdiagramm dargestellt. Über die Anzeigesymbole ( ) können Sie zwischen Tabelle und Kreisdiagramm umschalten.

Widget für Agent-Konnektivität (Mac) als Tabelle

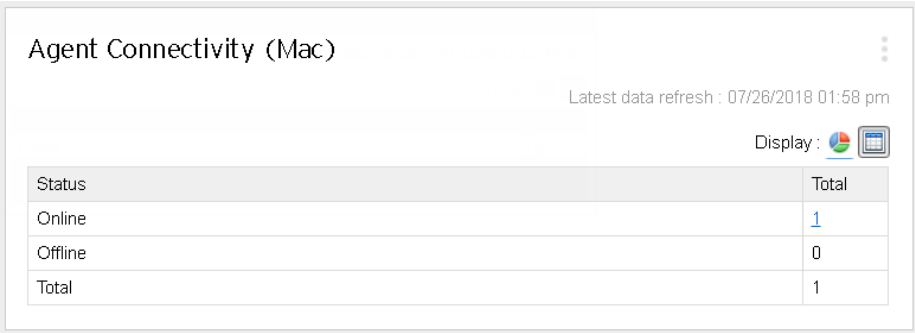


ABBILDUNG 3-1. Widget für Agent-Konnektivität (Mac) als Tabelle

Wenn die Anzahl der Agents in einem bestimmten Status 1 oder mehr beträgt, können Sie auf die Anzahl klicken, um die betreffenden Agents in der Agent-Struktur von Trend Micro Apex One (Mac) anzuzeigen. Anschließend können Sie Tasks für diese Agents starten oder ihre Einstellungen ändern.

Widget für Agent-Konnektivität (Mac) als Kreisdiagramm

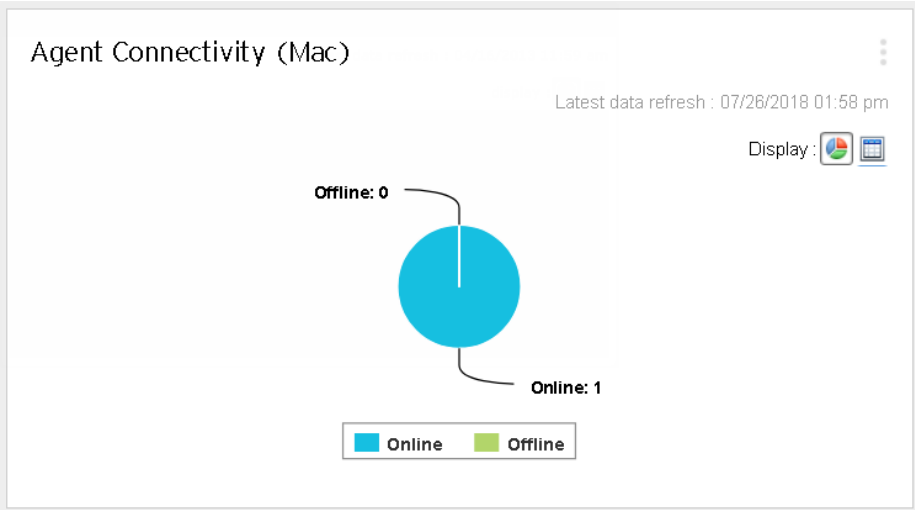


ABBILDUNG 3-2. Widget für Agent-Konnektivität (Mac) als Kreisdiagramm

Das Kreisdiagramm zeigt die Anzahl der im jeweiligen Status befindlichen Agents an, stellt aber keine Links zur Agent-Struktur von Trend Micro Apex One (Mac) bereit. Wenn Sie auf einen Staus klicken, wird er getrennt vom – oder wieder zusammen mit dem – Rest des Diagramms angezeigt.

Widget für Agent-Updates (Mac)

Das Widget für Agent-Updates (Mac) zeigt die Komponenten und Programme an, mit denen Endpunkte vor Sicherheitsbedrohungen geschützt werden.

Agent Updates (Mac)

Online Agents : 0, Smart Scan : 2, Conventional Scan : 0 — Latest data refresh : 05/21/2020 10:40 am

Expand All | Collapse All

Components	Current Version	Updated	Outdated	Update Rate
Virus Pattern	15.881.00	0	0	0
Spyware Active-monitoring Pattern	2.291.00	0	0	0
Virus Scan Engine (64-bit)	11.000.1006	0	0	0
Damage Cleanup Engine (64-bit)	1.500.1031	2	0	100
Advanced Threat Scan Engine (64-bit)	12.000.1009	2	0	100
Smart Scan Agent Pattern	15.879.00	2	0	100
Damage Cleanup Template	0.011.11	2	0	100
Mac Heuristic Pattern	1.492.00	2	0	100
Program	**Current Version**	**Upgraded**	**Not Upgraded**	**Upgrade Rate**
Apex One (Mac) Security Agent	3.5.2201	2	0	100

ABBILDUNG 3-3. Widget für Agent-Updates (Mac)

In diesem Widget können Sie Folgendes ausführen:

- Die aktuelle Version der einzelnen Komponenten anzeigen
- In der Spalte **Nicht aktuell** die Anzahl der Agents mit nicht aktuellen Komponenten einsehen. Falls Agents vorliegen, die aktualisiert werden müssen, starten Sie das Update, indem Sie auf die Anzahl klicken.
- Beim Agent-Programm können Sie die nicht aktualisierten Agents anzeigen, indem Sie auf den Anzahl-Link klicken.

Hinweis

Die Links öffnen die Webkonsole von Trend Micro Apex One (Mac), in der Sie weitere Tasks ausführen können.

Widget für erkannte Sicherheitsrisiken (Mac)

Das Widget für erkannte Sicherheitsrisiken (Mac) zeigt die Anzahl der erkannten Sicherheitsrisiken und Internet-Bedrohungen an.

Wenn die Anzahl infizierter Endpunkte 1 oder mehr beträgt, können Sie auf die Anzahl klicken, um die betreffenden Agents in der Agent-Struktur von Trend Micro Apex One (Mac) anzuzeigen. Anschließend können Sie Tasks für diese Agents starten oder ihre Einstellungen ändern.

Trend Micro Smart Protection

Trend Micro™Smart Protection ist eine cloudbasierte Content-Security-Infrastruktur der neuesten Generation zum Schutz vor Sicherheitsrisiken und Bedrohungen aus dem Internet. Sie umfasst sowohl lokale als auch gehostete Lösungen und bietet umfassenden Schutz im Netzwerk, zu Hause oder unterwegs. Über schlanke Agents erhalten die Benutzer Zugriff zu einer einzigartigen Kombination aus E-Mail-, Web- und File-Reputationstechnologien sowie Bedrohungsdatenbanken in der Cloud. Je mehr Produkte, Dienste und Benutzer auf das Netzwerk zugreifen, desto weiter werden die stets automatisch aktualisierten Schutzfunktionen ausgebaut. So entsteht eine Art digitale „Nachbarschaftswache“ in Echtzeit.

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

Smart Protection Services

Smart Protection Services beinhalten:

- **File-Reputation-Dienste**: File-Reputation-Dienste lagern eine Vielzahl von zuvor auf den Agent-Endpunkten gespeicherten Anti-Malware-Signaturen auf Smart Protection Quellen aus.
- **Web-Reputation-Dienste**: Web-Reputation-Dienste ermöglicht es lokalen Smart Protection Quellen, Daten über die Zuverlässigkeit von URLs zu hosten, die früher ausschließlich von Trend Micro gehostet wurden. Beide Technologien beanspruchen weniger Bandbreite, wenn Pattern aktualisiert oder die Gültigkeit eines URL überprüft wird.

  Details finden Sie unter *Web Reputation auf Seite 7-2*

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

  Details finden Sie unter *Smart Feedback auf Seite 3-20*

Smart Protection-Quellen

Die Bereitstellung der File-Reputation-Dienste und Web-Reputation-Dienste erfolgt durch **Smart Protection Quellen**, und zwar durch das **Trend Micro Smart Protection Network** und **Smart Protection Server**.

Trend Micro Smart Protection Network ist eine global skalierte, internetbasierte Infrastruktur, die sich an Benutzer ohne direkten Zugang zu ihrem Unternehmensnetzwerk richtet.

Smart Protection Server sind Server für Benutzer, die über direkten Zugriff auf das lokale Unternehmensnetzwerk verfügen. Zur Steigerung der Effizienz werden die Smart Protection-Dienste von lokalen Servern im Unternehmensnetzwerk vor Ort bereitgestellt.

Smart Protection Quelle für externe Security Agents

Externe Agents (d. h. Security Agents, die keine funktionsfähige Verbindung mit dem Trend Micro Apex One (Mac) oder OfficeScan-Server aufrechterhalten können) senden Web Reputation-Abfragen an das Smart Protection Network. Zum Versand von Abfragen ist allerdings eine Internetverbindung erforderlich.

Aktivieren Sie im Fenster der Web Reputation-Dienste die Web Reputation Richtlinie für externe Agents. Detaillierte Anweisungen dazu finden Sie unter *Einstellungen für Web Reputation konfigurieren auf Seite 7-3*.

Smart Protection-Quellen für interne Security Agents

Interne Agents (d. h. Security Agents mit funktionsfähiger Verbindung zum Trend Micro Apex One (Mac) oder OfficeScan Server) können Abfragen entweder an den Smart Protection Server oder an das Smart Protection Network senden.

Quelle	Details
Smart Protection Server	Smart Protection Server sind eine geeignete Quelle, wenn Sie aufgrund von Datenschutzbedenken Web Reputation-Abfragen nur innerhalb des Unternehmensnetzwerks zulassen möchten.
Smart Protection Network	Entscheiden Sie sich für das Smart Protection Network als Quelle, wenn Ihre Ressourcen nicht ausreichen, um Smart Protection Server ordnungsgemäß einzurichten und zu pflegen.

Smart Protection Server als Quelle für interne Security Agents

Mit dieser Option senden Trend Micro Apex One (Mac)Security Agents Anfragen an die für Apex One oder OfficeScan konfigurierten Smart Protection Server Security Agents.

Hinweis

Wenn auf Ihrem Trend Micro Apex One (Mac) Server OfficeScan installiert ist, aktualisieren Sie OfficeScan auf Apex One Version 2019 oder höher.

Wenn Sie bereits mit OfficeScan XG oder höher arbeiten, lesen Sie die folgenden Richtlinien, um Security Agents den Versand von Abfragen an Smart Protection Server zu ermöglichen:

1. Richten Sie die Smart Protection-Umgebung ein, falls Sie das nicht bereits erledigt haben. Anweisungen und Empfehlungen zur Einrichtung der Umgebung erhalten Sie in der Dokumentation zu OfficeScan:
2. Gehen Sie in der Webkonsole des OfficeScan Servers zum Fenster der Web Reputation-Einstellungen und aktivieren Sie die Option **Abfragen an Smart Protection Server senden**. Detaillierte Anweisungen dazu finden Sie unter *Einstellungen für Web Reputation konfigurieren auf Seite 7-3*.

Wichtig

Wenn diese Option in Apex Central oder in der Richtlinienverwaltung von Control Manager aktiviert und anschließend einem mit OfficeScan installierten Trend Micro Apex One (Mac) Server bereitgestellt wird, bleibt die Einstellung wirkungslos und die Option deaktiviert.

3. Vergewissern Sie sich, dass die Smart Protection Server verfügbar sind. Wenn keiner der Smart Protection Server verfügbar ist, senden die Agents keine Abfragen an das Smart Protection Network. Das bedeutet, dass die Endpunkte anfällig für Bedrohungen sind.
4. Aktualisieren Sie die Smart Protection Server regelmäßig, damit der Schutz stets aktuell ist.

Smart Protection Network als Quelle für interne Agents

Zum Versand von Abfragen an das Smart Protection Network ist eine Internetverbindung erforderlich.

Um das Smart Protection Network als Quelle für interne Agents festzulegen, aktivieren Sie im Fenster der Web Reputation-Dienste die Web Reputation Richtlinie für interne Agents. Achten Sie darauf, die Option **Abfragen an Smart Protection Server senden** nicht zu aktivieren. Detaillierte Anweisungen dazu finden Sie unter *Einstellungen für Web Reputation konfigurieren auf Seite 7-3*.

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

Kapitel 4

Security Agent installieren

In diesem Kapitel werden die Installationsanforderungen und Verfahren für Trend Micro Apex One (Mac)Security Agent beschrieben.

Informationen zum Aktualisieren des Security Agent finden Sie unter *Aktualisierung des Servers und Security Agents auf Seite 9-5*.

Voraussetzungen für die Installation des Agents

Nachfolgend sind die Systemvoraussetzungen für die Installation des Security Agent auf einem Mac-Endpunkt aufgeführt.

TABELLE 4-1. Voraussetzungen zur Installation des Security Agents

RESSOURCE	VORAUSSETZUNG
Betriebssystem	• macOS™ Tahoe 26 • macOS™ Sequoia 15 • macOS™ Sonoma 14 • macOS™ Ventura 13 • macOS™ Monterey 12

Hardware	• **Processor**:
	  • Intel® Core
	  • Apple® Silicon
	• **RAM**: Mindestens 2GB
	• **Available disk space**: Mindestens 512MB

Ressource	Voraussetzung

Kommunikation zwischen Server und Agents	• SSL-Port (Verwendet von der Endpoint Sensor-Funktion. Die gleiche SSL-Portnummer, die auf dem Apex One-Server konfiguriert ist.)
	• Listening-Port:
	  • Für Security Agent Version 3.5.3xxx oder später: 4343
	  Wichtig
	  Stellen Sie sicher, dass der Abhörport derselbe ist wie auf dem Apex One-Server konfiguriert.
	  Wenn Sie planen, den Abhörport zu aktualisieren, tun Sie dies vor der Installation von Security Agents. Wenn Sie Security Agents installiert haben und dann Änderungen vornehmen, verliert Security Agents die Verbindung zum Server und die einzige Möglichkeit, die Verbindung wiederherzustellen, besteht darin, Security Agents erneut bereitzustellen.
	  Weitere Informationen finden Sie unter *Agent-Server-Kommunikationseinstellungen konfigurieren auf Seite 9-15*.
	  • Für Security Agent Version 3.5.2xxx oder früher: 61617

Andere	• Zugriff auf *.trendmicro.com • Bei Bedarf Proxyserver-Einstellungen für Internetverbindung

Methoden und Setup-Dateien zur Agent-Installation

Sie haben folgende Möglichkeiten, um den Security Agent zu installieren:

- Installation auf einem einzelnen Endpunkt durch Starten des Installationspakets (`tmsminstall.zip`) auf dem Endpunkt

- Installieren Sie auf mehreren Endpunkten, indem Sie ein Betriebssystem-Image bereitstellen, das Security Agent enthält. Nach der Installation registriert sich Security Agent automatisch beim Apex One (Mac) Server.

Wichtig

Fügen Sie das TMMakeGoldenImage-Tool in das Master-Betriebssystem-Image ein, um das Problem der doppelten Security Agent-IDs auf dem Apex One (Mac)-Server zu beheben. Beschaffen Sie das Tool und folgen Sie dem Verfahren auf der folgenden Website:

https://success.trendmicro.com/dcx/s/solution/1107539-deploying-tmsm-client-using-a-cloned-mac-image-in-version-2-0-3-0-or-apex-one-mac?language=en_US

Hinweis

Informationen zum Upgrade von Security Agents finden Sie unter *Aktualisierung des Servers und Security Agents auf Seite 9-5*.

Laden Sie das nötige Agent-Installationspaket vom Trend Micro Apex One (Mac) Server herunter, und kopieren Sie es auf den Endpunkt.

Es gibt verschiedene Möglichkeiten, das Paket zu beziehen:

- Navigieren Sie in der Trend Micro Apex One (Mac) Webkonsole zu **Agents** > **Agent-Installationsdateien** und klicken Sie auf einen Link unter **Agent-Installationsdatei**.

Hinweis

Die Links zu den Security Agent-Deinstallationspaketen sind ebenfalls auf diesem Bildschirm verfügbar. Verwenden Sie diese Pakete, um das Security Agent-Programm von Endpunkten zu entfernen. Wählen Sie das Paket entsprechend der Version des Security Agent-Programms, das Sie entfernen möchten.

Informationen zur Deinstallation des Trend Micro Apex One (Mac)Security Agent finden Sie unter *Agent-Deinstallation auf Seite 4-21*.

- Wechseln Sie zu <*Server-Installationsordner*>`TMSM_HTML\ActiveUpdate\ClientInstall\`.
- Über die Webkonsole von Apex Central

  Weitere Informationen finden Sie im *Trend Micro Apex Central-Administratorhandbuch*.

Auf einem einzelnen Endpunkt installieren

Die Installation des Trend Micro Apex One (Mac)Security Agent auf einem einzelnen Endpunkt ist vergleichbar mit der Installation anderer Mac-Software.

Während der Installation wird der Benutzer möglicherweise aufgefordert, Verbindungen zu **iCoreService** zu erlauben. Diese Komponente wird zur Registrierung des Security Agent am Server verwendet. Weisen Sie die Benutzer an, diese Verbindung zuzulassen.

Prozedur

1. Suchen Sie zunächst sämtliche bereits auf dem Endpunkt installierte Sicherheitssoftware, und deinstallieren Sie diese.
2. Laden Sie das Agent-Installationspaket `tmsminstall.zip` herunter.

   Weitere Informationen zum Erhalt des Pakets finden Sie unter *Methoden und Setup-Dateien zur Agent-Installation auf Seite 4-3*.

3. Kopieren Sie `tmsminstall.zip` auf den Endpunkt, und starten Sie es dann über das integrierte Archivierungsprogramm.

Warnung!

Die Dateien im Paket `tmsminstall.zip` können beschädigt werden, wenn das Paket nicht mit einem integrierten Mac-Archivierungsprogramm geöffnet wird.

Um das Paket `tmsminstall.zip` in einem Terminalfenster zu starten, verwenden Sie folgenden Befehl:

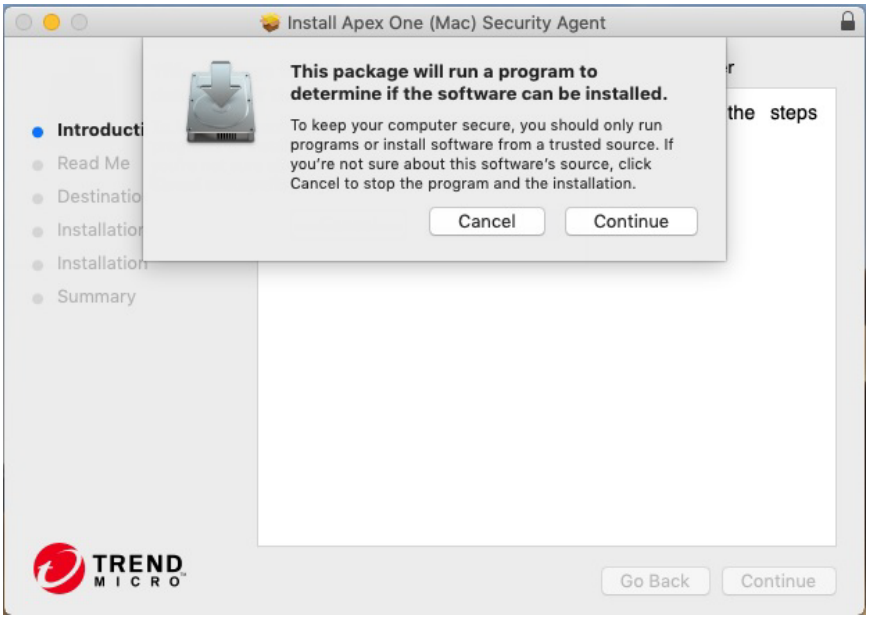
```
ditto -xk <Pfad der Datei tmsminstall.zip> <Zielordner>
```

Zum Beispiel:

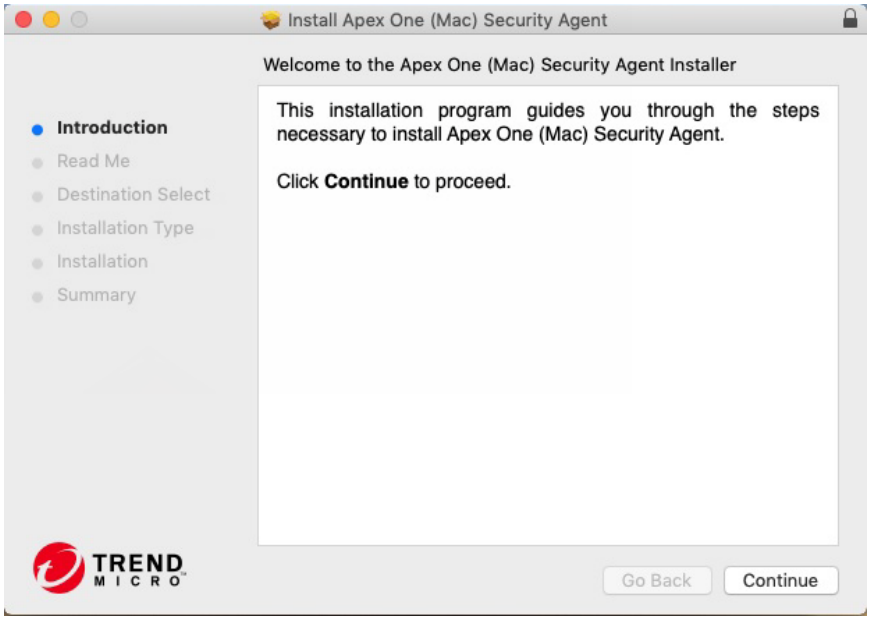
```
ditto -xk users/mac/Desktop/tmsminstall.zip users/mac/
Desktop
```

Durch den Start von `tmsminstall.zip` wird ein neuer Ordner `tmsminstall` erstellt.

4. Öffnen Sie den Ordner `tmsminstall` und starten Sie `tmsminstall.pkg`.
5. Wenn Sie gefragt werden, ob Sie mit der Installation fortfahren möchten, klicken Sie auf **Weiter**.



6. Klicken Sie im Einführungsfenster auf **Weiter**, um fortzufahren.



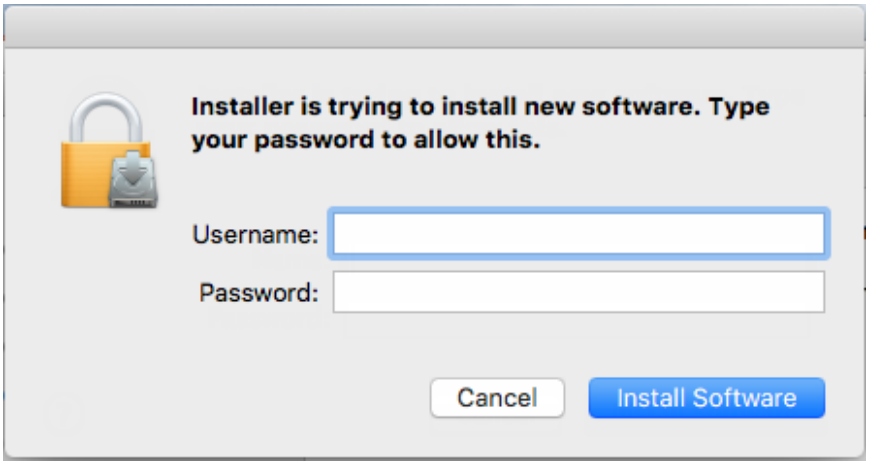
7. Lesen Sie die Erinnerungen und klicken Sie auf **Weiter**.

8. Klicken Sie im Bildschirm mit dem Installationstyp auf **Installation**.

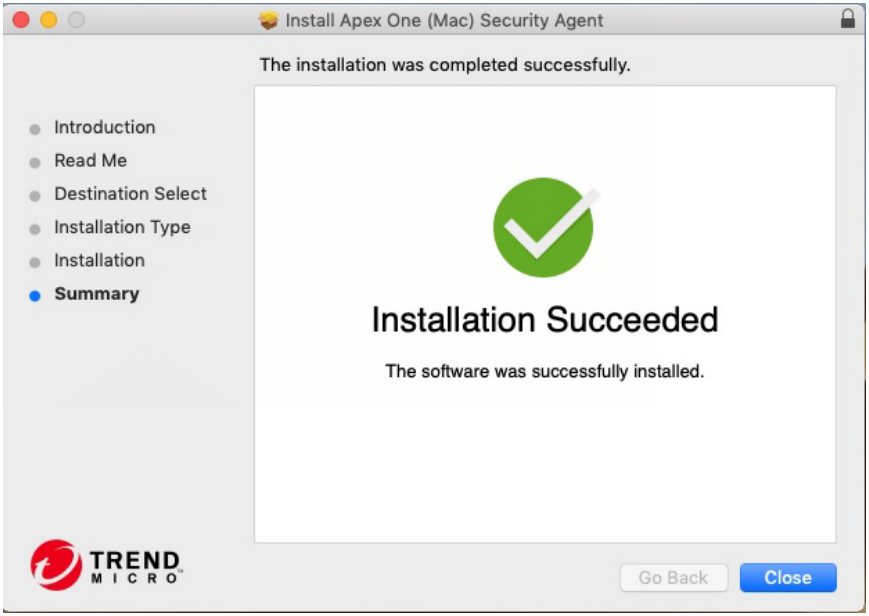
9. Tragen Sie den **Name** und das **Kennwort** in die entsprechenden Felder ein, um die Installation zu starten.

Hinweis

Geben Sie den Namen und das Kennwort für ein Konto mit Administratorrechten auf dem Endpunkt an.



10. Wenn die Installation erfolgreich war, klicken Sie auf **Schließen**, um die Installation abzuschließen.



Das Security Agent registriert sich automatisch bei dem Server, von dem das Agenten-Installationspaket bezogen wurde. Das Security Agent wird auch zum ersten Mal aktualisiert.

Nächste Schritte

Führen Sie für den Agent Tasks nach der Installation durch. Weitere Informationen finden Sie unter *Vorgänge nach der Agent-Installation auf Seite 4-12*.

Vorgänge nach der Agent-Installation

Prozedur

1. Wenn Sie den Security Agent zum ersten Mal auf einem Endpunkt mit einer unterstützten macOS™-Version installieren, zeigt das System den Setup-Assistenten an, der Sie auffordert, die erforderlichen Berechtigungen für die Funktion des Security Agent zu erlauben. Befolgen Sie die Anweisungen auf dem Bildschirm, um die Einstellungen abzuschließen.

   Im Folgenden wird das vollständige Verfahren beschrieben. Der Setup-Assistent überspringt automatisch die Berechtigungseinstellungen, die für Ihre macOS™-Version nicht erforderlich sind.

   Für macOS 26:

   a. Klicken Sie auf **Anmeldeobjekte & Erweiterungen öffnen** oder greifen Sie auf das Apple-Menü zu und gehen Sie zu **System Settings** > **Allgemein** > **Anmeldeelemente & Erweiterungen**.

   b. Scrollen Sie zum Abschnitt **Extensions**.

   c. Klicken Sie auf **By App**.

   d. Suchen Sie **iCore Service** und klicken Sie auf das Informationssymbol **(i)**.

   e. Aktivieren Sie **Network Extension**.

   f. Geben Sie Ihr macOS-Administratorkennwort ein und klicken Sie auf **OK**.

g. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Zulassen**, um dem Security Agent zu erlauben, Netzwerk-Inhalte zu filtern, und klicken Sie auf **Weiter**.

h. Aktivieren Sie **Security Extension**.

i. Geben Sie Ihr macOS-Administratorkennwort ein und klicken Sie auf **OK**.

j. Klicken Sie auf **Fertig**.

k. Klicken Sie auf **Weiter**.

l. Klicken Sie auf **Festplattenvollzugriff öffnen** oder greifen Sie auf das Apple-Menü zu und gehen Sie zu **System Settings** > **Datenschutz & Sicherheit** > **Festplattenvollzugriff**.

m. Ziehen Sie das Symbol für **Dateien** in die Tabelle für Festplattenvollzugriff unter „Festplattenvollzugriff“.

n. Geben Sie Ihr macOS-Administratorkennwort ein und klicken Sie auf **Einstellung verändern**.

o. Falls Sie aufgefordert werden, die App neu zu starten, klicken Sie auf **Später**, um die App später neu zu starten.

p. Klicken Sie auf die Umschaltfläche, um die folgenden Funktionen zu aktivieren:

- iCore-Dienst
- Apex One (Mac) Security Agent
- Trend Micro Erweiterung (falls verfügbar)

q. Klicken Sie auf **Fertig**.

r. Starten Sie den Computer neu, damit die Änderungen wirksam werden.

Für macOS 15:

a. Klicken Sie auf **Anmeldeobjekte & Erweiterungen öffnen** oder greifen Sie auf das Apple-Menü zu und gehen Sie

zu **Systemeinstellungen** > **Allgemein** > **Anmeldeobjekte & Erweiterungen**.

b. Scrollen Sie nach unten zum Abschnitt **Erweiterungen** > **Endpunkt-Sicherheitserweiterungen**.

c. Klicken Sie auf die Schaltfläche **(i)** auf der rechten Seite und aktivieren Sie die **iCore-Dienst**.

d. Geben Sie Ihr macOS-Administrator-Passwort ein und klicken Sie auf **OK**.

e. Klicken Sie auf **Fertig**.

f. Suchen Sie nach **Netzwerkerweiterungen** und wiederholen Sie die Schritte c bis e.

g. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Zulassen**, um dem Security Agent zu erlauben, Netzwerk-Inhalte zu filtern, und klicken Sie auf **Weiter**.

h. Klicken Sie auf **Festplattenvollzugriff öffnen** oder rufen Sie das Apple-Menü auf und gehen Sie zu **Systemeinstellungen** > **Datenschutz & Sicherheit** > **Festplattenvollzugriff**.

i. Klicken Sie auf **Dateispeicherort öffnen** und suchen Sie die Datei `com.trendmicro.icore.es.systemextension`; verschieben Sie sie dann per Drag & Drop in die Tabelle für Festplattenvollzugriff.

j. Klicken Sie auf **Dateispeicherort öffnen** und verschieben Sie `Apex One (Mac) Security Agent` aus dem Anwendungsordner per Drag & Drop in die Tabelle für Festplattenvollzugriff. Klicken Sie auf dem daraufhin angezeigten Bildschirm auf **Später**.

k. Klicken Sie auf **Dateispeicherort öffnen** und suchen Sie die Datei `iCore Service`; ziehen Sie dann die Datei in die Tabelle "Voller Festplattenzugriff".

l. Klicken Sie auf den Kippschalter, um die folgenden Apps zu aktivieren:

- iCore-Dienst

- Apex One (Mac) Security Agent
- Trend Micro Erweiterung (falls verfügbar)

m. Klicken Sie auf **Weiter**.

n. Starten Sie den Computer neu, damit die Änderungen wirksam werden.

Für macOS 13 und 14:

a. Klicken Sie auf **Datenschutz und Sicherheit öffnen** oder rufen Sie das Apple-Menü auf und gehen Sie zu **Systemeinstellungen** > **Datenschutz & Sicherheit**.

b. Scrollen Sie zum Abschnitt **Sicherheit**, und klicken Sie auf **Details**.

c. Geben Sie Ihr macOS-Administratorpasswort ein und klicken Sie auf **Entsperren** oder **Einstellungen ändern**, um Änderungen vorzunehmen.

d. Klicken Sie auf die Umschaltfläche, um alle iCore Service-Einträge zu aktivieren, und klicken Sie auf **OK**.

e. Klicken Sie auf **Zulassen**, um dem Security Agent zu erlauben, Netzwerk-Inhalte zu filtern.

f. Klicken Sie auf **Weiter**.

g. Klicken Sie auf **Festplattenvollzugriff öffnen** oder rufen Sie das Apple-Menü auf und gehen Sie zu **Systemeinstellungen** > **Datenschutz & Sicherheit** > **Festplattenvollzugriff**.

h. Klicken Sie auf **Dateispeicherort öffnen** und suchen Sie die Datei `com.trendmicro.icore.es.systemextension`; verschieben Sie sie dann per Drag & Drop in die Tabelle für Festplattenvollzugriff.

i. Klicken Sie auf **Dateispeicherort öffnen** und verschieben Sie `Apex One (Mac) Security Agent` aus dem Anwendungsordner per Drag & Drop in die Tabelle für Festplattenvollzugriff. Klicken Sie auf dem daraufhin angezeigten Bildschirm auf **Später**.

j. Klicken Sie auf **Dateispeicherort öffnen** und suchen Sie die Datei `iCore Service`; ziehen Sie dann die Datei in die Tabelle "Voller Festplattenzugriff".

k. Klicken Sie auf den Kippschalter, um die folgenden Apps zu aktivieren:

- iCore-Dienst
- Apex One (Mac) Security Agent
- Trend Micro Erweiterung (falls verfügbar)

l. Klicken Sie auf **Weiter**.

m. Starten Sie den Computer neu, damit die Änderungen wirksam werden.

Für macOS 12:

a. Klicken Sie auf **\"Sicherheit & Datenschutz\" öffnen** oder greifen Sie auf das Apple-Menü zu und gehen Sie zu **Systemeinstellungen** > **Sicherheit und Datenschutz** > **Allgemein**.

b. Klicken Sie auf das Schlosssymbol in der unteren linken Ecke und geben Sie Ihr macOS-Administratorkennwort ein, um Änderungen vorzunehmen.

c. Klicken Sie auf **Zulassen**, um das Trend Micro Zertifikat zu installieren.

d. Klicken Sie auf **Weiter**.

e. Klicken Sie im Fenster **Sicherheit und Datenschutz** auf **Zulassen**.

f. Wählen Sie alle **Trend Micro Inc.** Optionen aus und klicken Sie auf **OK**.

g. Klicken Sie auf **Zulassen**, um dem Security Agent zu erlauben, Netzwerk-Inhalte zu filtern.

h. Klicken Sie auf **Weiter**.

i. Wählen Sie auf dem **Sicherheit und Datenschutz**-Bildschirm **Festplattenvollzugriff** aus der Liste der Dienste aus.

j. Klicken Sie auf **Dateispeicherort öffnen** und suchen Sie die Datei `iCore Service`; ziehen Sie dann die Datei in die Tabelle "Voller Festplattenzugriff".

k. Klicken Sie auf **Dateispeicherort öffnen** und verschieben Sie `Apex One (Mac) Security Agent` aus dem Anwendungsordner per Drag & Drop in die Tabelle für Festplattenvollzugriff.

l. Stellen Sie sicher, dass die folgenden Apps ausgewählt sind:

- iCore-Dienst
- Apex One (Mac) Security Agent
- Trend Micro Erweiterung (falls verfügbar)

m. Klicken Sie auf **Weiter**.

n. Starten Sie den Computer neu, damit die Änderungen wirksam werden.

2. Das System zeigt eine Benachrichtigung an, die Sie auffordert, die Trend Micro Toolbar for Mac-Erweiterung zu installieren und zu aktivieren. Führen Sie die folgenden Schritte für Ihren Webbrowser aus:

- Safari 17 und höher:

  a. Klicken Sie im Benachrichtigungsfenster auf **Erweiterung aktivieren**.

     Das Fenster „Konfigurationsüberblick“ wird angezeigt.

  b. Klicken Sie auf **Safari-Erweiterungen öffnen**.

  c. Wählen Sie die Option **Trend Micro Toolbar for Mac**, um die Erweiterung zu aktivieren.

  d. Klicken Sie im Abschnitt „Berechtigungen“ auf **Immer auf jeder Website zulassen...**.

  e. Wenn Sie gefragt werden, ob Sie die Erweiterung auf jeder Website zulassen möchten, klicken Sie auf **Immer auf jeder Website erlauben**.

- Safari 16 und niedriger:
  a. Klicken Sie im Benachrichtigungsfenster auf **Erweiterung aktivieren**.

     Das Fenster „Konfigurationsüberblick“ wird angezeigt.

  b. Klicken Sie auf **Safari-Erweiterungen öffnen**.

  c. Wählen Sie die Option **Trend Micro Toolbar for Mac**, um die Erweiterung zu aktivieren.

- Firefox:
  a. Klicken Sie im Benachrichtigungsfenster auf **Erweiterung aktivieren**.

     Das Fenster „Konfigurationsüberblick“ wird angezeigt.

  b. Klicken Sie auf **Dateispeicherort öffnen**, um die `Trend Micro Toolbar for Mac extension.xpi`-Datei zu finden; ziehen Sie dann die Datei in das Firefox-Fenster, um sie zu installieren.

  c. Klicken Sie auf **Hinzufügen**, um die Trend Micro Toolbar for Mac-Erweiterung zu installieren.

- (Erforderlich für macOS 11.0 und höher) Google Chrome:
  a. Klicken Sie im Benachrichtigungsfenster auf **Erweiterung aktivieren**.

     Das Fenster „Konfigurationsüberblick“ wird angezeigt.

  b. Klicken Sie auf **Dateispeicherort öffnen**, um die Datei `Trend Micro Toolbar For Mac (Chrome).mobileconfig` zu finden und doppelt darauf zu klicken.

  c. Klicken Sie auf **Profile öffnen**.

  d. Wählen Sie auf dem Profilbildschirm `Trend Micro Toolbar for Mac (Chrome)` aus und klicken Sie auf **Installieren ...**.

  e. Klicken Sie auf **Install**.

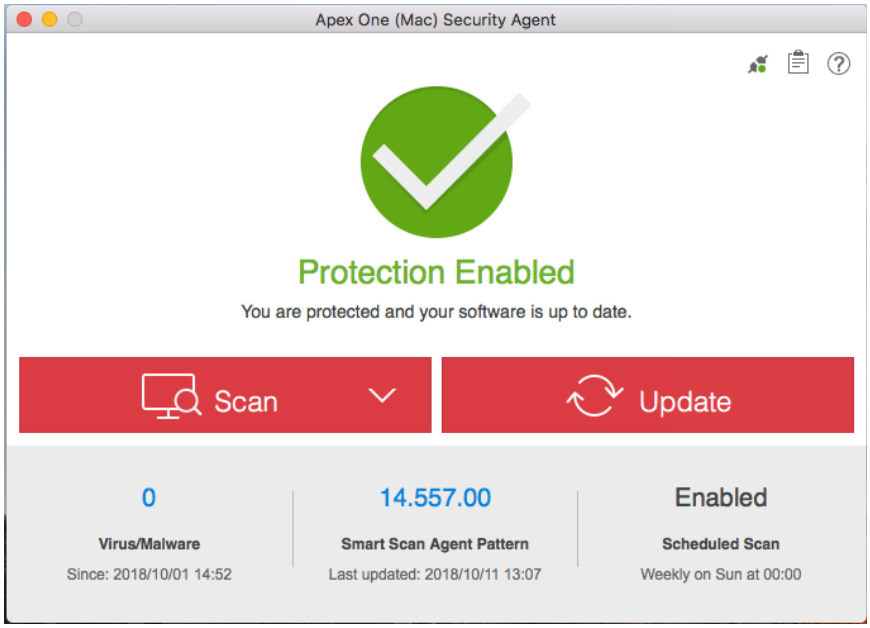
f. Geben Sie, wenn Sie dazu aufgefordert werden, das macOS-Administratorkennwort ein, und klicken Sie auf **OK**.

g. Starten Sie Google Chrome neu, damit die Änderungen wirksam werden.

3. Überprüfen Sie Folgendes:

- Das Symbol für den Security Agent ( ) wird in der Menüleiste des Endpunkts angezeigt.
- Die Trend Micro Apex One (Mac)Security Agent-Dateien befinden sich im <*Agent-Installationsordner*>.
- Der Security Agent erscheint im Agentenbaum der Webkonsole. Um auf den Agentenbaum zuzugreifen, klicken Sie im Hauptmenü auf **Agent-Verwaltung**.

4. Sie können Trend Micro Apex One (Mac) Komponenten aktualisieren, indem Sie in der Agent-Konsole auf **Update** klicken. Der Security Agent lädt Komponenten vom Trend Micro Apex One (Mac) Server herunter. Weitere Informationen finden Sie unter *Agent-Updates auf Seite 5-9*.



Wenn der Security Agent keine Verbindung zum Server herstellen kann, lädt er die Dateien direkt vom Trend Micro ActiveUpdate Server herunter. Für die Verbindung zum ActiveUpdate Server ist eine Internetverbindung notwendig.

5. Um eine manuelle Suche auf dem Endpunkt zu starten, klicken Sie auf **Suche** und wählen Sie eine der folgenden Suchoptionen aus:

   - **Schnellsuche**: Es werden die Bereiche des Endpunkts durchsucht, die üblicherweise Sicherheitsrisiken ausgesetzt sind. Informationen über die Endpunktbereiche, die durchsucht werden sollen, sind in den Pattern-Dateien auf dem Security Agent enthalten.
   - **Benutzerdefinierte Suche**: Durchsucht die angegebenen Dateien oder Ordner. Die benutzerdefinierte Suche empfiehlt sich für Dateien oder Ordner, bei denen Sie eine Vireninfektion vermuten.
   - **Vollständige Suche**: Durchsucht alle Dateien mit Ausnahme von verschlüsselten und kennwortgeschützten Dateien.

Nächste Schritte

Wenn es nach der Installation Probleme mit dem Security Agent gibt, versuchen Sie, das Security Agent zu deinstallieren und dann erneut zu installieren.

Agent-Deinstallation

Deinstallieren Sie das Security Agent Programm nur, wenn Probleme mit dem Programm auftreten. Installieren Sie es umgehend neu, damit Ihr Endpunkt vor Sicherheitsrisiken geschützt bleibt.

Prozedur

1. Laden Sie das Security Agent-Deinstallationspaket (`tmsmuninstall.zip`) vom Apex One (Mac) Server herunter. Navigieren Sie in der Apex One (Mac) Webkonsole zu **Agents** > **Agent-Installationsdateien**, und klicken Sie auf den Link unter **Agent-Deinstallationsdatei**.
2. Kopieren Sie das Paket auf den Endpunkt, und starten Sie es.
3. Tragen Sie den **Namen** und das **Kennwort** in die entsprechenden Felder ein, um die Deinstallation zu starten.

   Hinweis

   Geben Sie den Namen und das Kennwort für ein Konto mit Administratorrechten auf dem Endpunkt an.

4. (Für macOS 11.0 und höher) Klicken Sie auf **Weiter**, um die Systemerweiterungen zu entfernen.
5. Klicken Sie nach erfolgreicher Deinstallation auf **Schließen**, um die Deinstallation abzuschließen.

Nächste Schritte

Melden Sie den Security Agent vom Server ab.

1. Klicken Sie in der Webkonsole auf **Agent-Verwaltung** und wählen Sie das Security Agent aus, das deinstalliert wurde.

2. Klicken Sie auf **Agent-Struktur verwalten** > **Gruppe/Agent entfernen**.

Kapitel 5

Den Schutz auf dem neuesten Stand halten

In diesem Kapitel werden die Trend Micro Apex One (Mac) Komponenten und Update-Verfahren erläutert.

Komponenten

Trend Micro Apex One (Mac) besteht aus mehreren Komponenten, die zusammen Endpunkte vor den aktuellen Sicherheitsrisiken schützen. Halten Sie diese Komponenten mit manuellen oder zeitgesteuerten Updates auf dem neuesten Stand.

Zusätzlich zu den Komponenten erhalten Security Agents auch aktualisierte Konfigurationsdateien vom Trend Micro Apex One (Mac) Server. Security Agents benötigen diese Konfigurationsdateien, um neue Einstellungen zu übernehmen. Bei jeder Änderung der Trend Micro Apex One (Mac) Einstellungen über die Webkonsole ändern sich auch die Konfigurationsdateien.

Komponente	Beschreibung
Agent-Programm	Das Security Agent-Programm dient dem Schutz vor Sicherheitsrisiken.
Fortgeschrittene Bedrohungssuchmaschine (Universell)	Die Fortgeschrittene Bedrohungssuchmaschine schützt vor Viren, Malware und Exploits von Schwachstellen in Software wie Java und Flash. Integriert mit der Trend Micro Virensuch-Engine, verwendet die Fortgeschrittene Bedrohungssuchmaschine signaturbasierte, verhaltensbasierte und aggressive heuristische Erkennung.
Damage Cleanup Engine (Universell)	Die Damage-Cleanup-Engine sucht und entfernt Trojaner und Trojaner-Prozesse.
Damage-Cleanup-Template	Die Damage-Cleanup-Template wird von der Damage-Cleanup-Engine verwendet, um Trojaner-Dateien oder -Prozesse zu erkennen und zu beseitigen.
Heuristisches Pattern für Mac	Das heuristische Pattern für Mac wird von der Smart Scan verwendet, um Malware auf Mac-Plattformen zu identifizieren.
Smart Scan Agent Pattern	Die Pattern-Datei, die der Security Agent zum Identifizieren von Bedrohungen verwendet. Diese Pattern-Datei wird auf dem Agent-Endpunkt gespeichert.

Komponente	Beschreibung
Pattern zur aktiven Spyware-Überwachung	Das Spyware-Aktivmonitor-Pattern enthält Informationen, mit denen Trend Micro Apex One (Mac) Spyware und Grayware erkennt.
Viren-Scan-Engine (Universell)	Die Viren-Scan-Engine bildet den Kern aller Trend Micro-Produkte. Sie wurde ursprünglich als Reaktion auf die ersten dateibasierten Computerviren entwickelt. Heute ist die Scan-Engine technisch so ausgefeilt, dass sie verschiedenste Sicherheitsrisiken einschließlich Spyware erkennt. Die Viren-Scan-Engine erkennt auch kontrollierte Viren, die zu Forschungszwecken entwickelt und verwendet werden. Da die zeitkritischsten Informationen über Sicherheitsrisiken in den Pattern-Dateien gespeichert sind, kann Trend Micro die Anzahl der Scan-Engine-Updates auf ein Mindestmaß reduzieren und gleichzeitig ein hohes Schutzniveau beibehalten. Dennoch stellt Trend Micro in regelmäßigen Abständen neue Versionen der Scan-Engine zur Verfügung, und zwar in den folgenden Fällen: • Neue Technologien zur Suche und Entdeckung von Viren werden in die Software integriert. • Neue, potenziell gefährliche Sicherheitsrisiken wurden entdeckt, auf welche die Scan Engine nicht reagieren kann. • Die Suchleistung wurde verbessert. • Neue Dateiformate, Skriptsprachen, Kodierungen und/oder Komprimierungsformate werden hinzugefügt.
Viren-Pattern	Das Viren-Pattern enthält Informationen, mit denen Trend Micro Apex One (Mac) die neuesten Viren- und Malware-Programme sowie kombinierte Angriffe erkennt. Mehrmals pro Woche und bei jeder Entdeckung besonders schädlicher Viren- oder Malware-Programme erstellt und veröffentlicht Trend Micro ein neues Viren-Pattern.

Update-Übersicht

Alle Komponenten-Updates stammen vom Trend Micro ActiveUpdate Server. Wenn Updates verfügbar sind, lädt der Trend Micro Apex One (Mac) Server die aktualisierten Komponenten herunter.

Der Trend Micro Apex One (Mac) Server kann so konfiguriert werden, dass Updates von einer anderen Adresse als dem Trend Micro ActiveUpdate Server bezogen werden. Dafür müssen Sie eine benutzerdefinierte Update-Adresse einrichten. Wenden Sie sich an Ihren Support-Anbieter, um Unterstützung beim Einrichten dieser Update-Adresse zu erhalten.

In der folgenden Tabelle sind die verschiedenen Optionen für das Komponenten-Update bei Trend Micro Apex One (Mac) Servern und Security Agents aufgeführt:

TABELLE 5-1. Server-/Agent-Update-Optionen

UPDATE-OPTION	BESCHREIBUNG
ActiveUpdate Server ↓ Trend Micro Apex One (Mac) Server ↓ Security Agents	Der Trend Micro Apex One (Mac) Server empfängt aktualisierte Komponenten vom Trend Micro ActiveUpdate Server (oder einer anderen Update-Adresse, wenn eine solche eingerichtet wurde) und verteilt diese dann an Security Agents.
ActiveUpdate Server ↓ Security Agents	Security Agents erhalten die aktualisierten Komponenten direkt vom ActiveUpdate Server, wenn sie keine Verbindung zum Trend Micro Apex One (Mac) Server herstellen können.

Server-Update

Der Trend Micro Apex One (Mac) Server lädt die folgenden Komponenten herunter und verteilt sie an die Security Agents:

- Viren-Pattern
- Pattern zur aktiven Spyware-Überwachung
- Viren-Scan-Engine (32 Bit/64 Bit)
- Damage Cleanup Engine (64 Bit)
- Damage-Cleanup-Template
- Smart Scan Agent Pattern
- Trend Micro Apex One (Mac)Security Agent
- Heuristisches Pattern für Mac
- Fortgeschrittene Bedrohungssuchmaschine (64 Bit)

Sie können die aktuellen Versionen der Komponenten in der Webkonsole im Übersichtsfenster anzeigen und die Anzahl der Security Agents mit oder ohne aktuelle Komponenten bestimmen.

Wenn die Verbindung zum Internet über einen Proxy-Server hergestellt wird, müssen Sie für den Download der Updates die korrekten Proxy-Einstellungen verwenden.

Update-Adresse des Servers konfigurieren

Sie können den Trend Micro Apex One (Mac) Server so konfigurieren, dass die Komponenten vom Trend Micro ActiveUpdate Server oder einer anderen Adresse heruntergeladen werden.

Hinweis

Wenn der Server ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Server-Updates in *Einschränkungen eines reinen IPv6-Servers auf Seite A-2*.

Nachdem der Server alle verfügbaren Updates heruntergeladen hat, benachrichtigt er automatisch Security Agents, um ihre Komponenten zu aktualisieren. Wenn das Komponenten-Update kritisch ist, lassen Sie den Server Security Agents sofort benachrichtigen, indem Sie zu **Agents** > **Agent-Verwaltung** > **Tasks** > **Update** navigieren.

Prozedur

1. Navigieren Sie zu **Updates** > **Update-Adresse**.
2. Wählen Sie den Ort aus, von dem das Update heruntergeladen werden soll.
   - Bei Auswahl von ActiveUpdate Server:
     - Stellen Sie sicher, dass der Trend Micro Apex One (Mac) Server mit dem Internet verbunden ist.
     - Wenn Sie einen Proxy-Server verwenden, testen Sie die Internetverbindung mit den betreffenden Proxy-Einstellungen.

       Weitere Informationen finden Sie unter *Proxy-Einstellungen für Server-Updates konfigurieren auf Seite 5-6*.
   - Bei Auswahl einer benutzerdefinierten Update-Adresse:
     - Richten Sie die betreffende Umgebung und die erforderlichen Update-Ressourcen ein.
     - Stellen Sie sicher, dass der Servercomputer mit dieser Update-Adresse verbunden ist. Wenden Sie sich an Ihren Support-Anbieter, um Unterstützung beim Einrichten einer Update-Adresse zu erhalten.
     - Sie können Updates von Trend Micro Apex Central erhalten, indem Sie die Trend Micro Apex Central-Serveradresse eingeben.
3. Klicken Sie auf **Save**.

Proxy-Einstellungen für Server-Updates konfigurieren

Sie können den Trend Micro Apex One (Mac) Server so konfigurieren, dass für den Download der Updates vom Trend Micro ActiveUpdate Server die Proxy-Einstellungen verwendet werden.

Hinweis

Wenn der Server ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Proxy-Einstellungen in *Einschränkungen eines reinen IPv6-Servers auf Seite A-2*.

Prozedur

1. Navigieren Sie zu **Administration** > **Externe Proxy-Einstellungen**.
2. Aktivieren Sie das Kontrollkästchen für die Verwendung eines Proxy-Servers.
3. Geben Sie den Namen oder die IPv4- bzw. IPv6-Adresse des Proxy-Servers und seine Portnummer an.
4. Falls der Proxy-Server einen Benutzernamen und ein Kennwort erfordert, geben Sie diese in die dafür vorgesehenen Textfelder ein.
5. Klicken Sie auf **Save**.

Server-Update-Methoden

Sie können das Update der Komponenten von Trend Micro Apex One (Mac) Server manuell oder zeitgesteuert durchführen.

- **Manuelles Update**: Führen Sie ein manuelles Update durch, wenn ein Update kritisch ist, damit der Server die Updates umgehend beziehen kann. Weitere Informationen finden Sie unter *Server manuell aktualisieren auf Seite 5-8*.
- **Zeitgesteuertes Update**: Der Trend Micro Apex One (Mac) Server stellt am geplanten Tag und zur geplanten Uhrzeit eine Verbindung zur Update-Adresse her, um die aktuellsten Komponenten herunterzuladen. Weitere Informationen finden Sie unter *Server-Updates zeitlich planen auf Seite 5-8*.

Nachdem ein Server-Update abgeschlossen ist, wird der Agent umgehend zum Update aufgefordert.

Server-Updates zeitlich planen

Sie können den Trend Micro Apex One (Mac) Server so konfigurieren, dass er seine Update-Adresse regelmäßig überprüft und verfügbare Updates automatisch herunterlädt. Durch das zeitgesteuerte Server-Update können Sie einfach und wirksam sicherstellen, dass Ihr Schutz vor Sicherheitsrisiken immer auf dem neuesten Stand ist.

Nachdem ein Server-Update abgeschlossen ist, wird der Agent zum Update aufgefordert.

Prozedur

1. Navigieren Sie zu **Updates** > **Zeitgesteuertes Update**.
2. Wählen Sie die zu aktualisierenden Komponenten aus.
3. Geben Sie den Update-Zeitplan an.

   Bei täglichen, wöchentlichen und monatlichen Updates gibt der Zeitraum die Anzahl der Stunden an, in denen Trend Micro Apex One (Mac) das Update durchführt. Trend Micro Apex One (Mac) führt das Update zu einem beliebigen Zeitpunkt innerhalb dieses Zeitraums durch.

   Wenn Sie für die monatlichen Updates den 29., 30. oder 31. Tag des Monats ausgewählt haben, dieser Tag im betreffenden Monat jedoch nicht vorkommt, führt Trend Micro Apex One (Mac) das Update am letzten Tag des Monats durch.
4. Klicken Sie auf **Save**.

Server manuell aktualisieren

Führen Sie nach der Installation oder einem Upgrade von Trend Micro Apex One (Mac) Server sowie bei einem Ausbruch ein manuelles Update der Komponenten auf dem Server durch.

Prozedur

1. Navigieren Sie zu **Updates** > **Manuelles Update**.
2. Wählen Sie die zu aktualisierenden Komponenten aus.
3. Klicken Sie auf **Update**.

   Der Server lädt die aktualisierten Komponenten herunter.

   Nachdem ein Server-Update abgeschlossen ist, wird der Agent umgehend zum Update aufgefordert.

Agent-Updates

Um sicherzustellen, dass Security Agents vor den neuesten Sicherheitsrisiken geschützt bleibt, aktualisieren Sie die Update-Agent-Komponenten regelmäßig. Aktualisieren Sie außerdem Security Agents mit stark veralteten Komponenten und bei einem Ausbruch. Komponenten veralten stark, wenn der Security Agent über einen längeren Zeitraum nicht vom Apex One (Mac)-Server oder dem ActiveUpdate-Server aktualisieren kann.

Agent-Update-Methoden

Es gibt mehrere Möglichkeiten, Security Agents zu aktualisieren.

Update-Methode	Beschreibung
Vom Administrator eingeleitetes manuelles Update	Updates können in den folgenden Webkonsolen-Fenstern gestartet werden: • Agent-Verwaltung: Weitere Informationen finden Sie unter *Agent-Updates aus dem Agent-Verwaltung-Fenster starten auf Seite 5-15*. • Übersicht: Weitere Informationen finden Sie unter *Agent-Updates aus dem Übersichtsfenster starten auf Seite 5-14*.

Update-Methode	Beschreibung
Automatisches Update	• Nachdem der Server ein Update abgeschlossen hat, benachrichtigt er Security Agents sofort, um zu aktualisieren. Weitere Informationen finden Sie unter *Automatisches Update des Agents konfigurieren auf Seite 5-11*. • Updates können gemäß dem von Ihnen konfigurierten Zeitplan ausgeführt werden. Sie können einen Zeitplan konfigurieren, der für ein oder mehrere Security Agents und Domänen gilt, oder für alle Security Agents, die der Server verwaltet. Weitere Informationen finden Sie unter *Agent-Update-Einstellungen konfigurieren auf Seite 5-12*.
Vom Benutzer eingeleitete manuelle Aktualisierung	Benutzer starten das Update von ihrem Endpunkt aus.

Agent-Update-Adresse

Standardmäßig laden Security Agents Komponenten vom Apex One (Mac) Server herunter. Zusätzlich zu den Komponenten erhalten Security Agents auch aktualisierte Konfigurationsdateien, wenn sie vom Apex One (Mac) Server aktualisieren. Security Agents benötigen diese Konfigurationsdateien, um neue Einstellungen zu übernehmen. Bei jeder Änderung der Apex One (Mac) Einstellungen über die Webkonsole ändern sich auch die Konfigurationsdateien.

Bevor Sie das Security Agents aktualisieren, überprüfen Sie, ob der Apex One (Mac) Server die neuesten Komponenten hat.

Informationen dazu, wie Sie den Trend Micro Apex One (Mac) Server aktualisieren, finden Sie unter *Server-Update auf Seite 5-4*.

Konfigurieren Sie einen, mehrere oder alle Security Agents, um vom Trend Micro ActiveUpdate Server herunterzuladen, falls der Apex One (Mac) Server nicht verfügbar ist.

Weitere Informationen finden Sie unter *Agent-Update-Einstellungen konfigurieren auf Seite 5-12*.

Hinweis

Wenn ein Security Agent ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Agent-Updates in *Einschränkungen bei reinen IPv6-Agents auf Seite A-3*.

Hinweise und Erinnerungen für Agent-Updates

- Security Agents können Proxy-Einstellungen während eines Updates verwenden. Proxy-Einstellungen werden in der Agentenkonsole konfiguriert.
- Während eines Updates zeigt das Symbol für Security Agent in der Menüleiste des Endpunkts den laufenden Aktualisierungsvorgang an. Ist ein Upgrade für das Security Agent-Programm verfügbar, führen Security Agents zunächst das Update und dann das Upgrade auf die neueste Programmversion oder den neuesten Build durch. Bis zum Abschluss des Updates können keine Tasks über die Konsole gestartet werden.
- Greifen Sie auf den Übersichtsbildschirm zu, um zu überprüfen, ob alle Security Agents aktualisiert wurden.

Automatisches Update des Agents konfigurieren

Das automatische Update befreit Sie von lästigen Update-Benachrichtigungen an alle Security Agents und verringert so das Risiko veralteter Komponenten auf den Endpunkten.

Zusätzlich zu den Komponenten erhalten Trend Micro Apex One (Mac)Security Agents während des automatischen Updates aktualisierte Konfigurationsdateien. Security Agents benötigen diese Konfigurationsdateien, um neue Einstellungen zu übernehmen. Bei jeder Änderung der Trend Micro Apex One (Mac) Einstellungen über die Webkonsole ändern sich auch die Konfigurationsdateien.

Der Trend Micro Apex One (Mac) Server kann Online-Security Agents per Benachrichtigung auffordern, Komponenten zu aktualisieren, wenn er die neuesten Komponenten heruntergeladen hat. Offline-Security Agents werden benachrichtigt, sobald sie neu gestartet wurden und sich wieder

mit dem Server verbinden. Sie können nach dem Update optional die Funktion **Jetzt durchsuchen** (manuelle Suche) auf Trend Micro Apex One (Mac)Security Agent Endpunkten durchführen.

1. Klicken Sie auf **Updates** > **Automatisches Update für Agent**.
2. Wählen Sie die Optionen aus.

TABELLE 5-2. Ereignisbedingtes Update

OPTIONEN	BESCHREIBUNG
Komponenten-Update auf Agents direkt initiieren, nachdem der Server eine neue Komponente heruntergeladen hat	Der Trend Micro Apex One (Mac)-Server benachrichtigt Security Agents, sobald ein Update abgeschlossen ist.
Komponenten-Update von Agents nach dem Neustarten und Verbinden mit dem Server initiieren lassen	Verpasst ein Security Agent ein Update, lädt dieser die Komponenten herunter, sobald eine Verbindung mit dem Server hergestellt wurde. Der Security Agent kann ein Update verpassen, wenn er offline ist, oder wenn der Endpunkt, auf dem er installiert ist, nicht hochgefahren ist.

Hinweis

Standardmäßig werden Update-Benachrichtigungen bis zu sieben Tage auf dem Trend Micro Apex One (Mac) Server aufbewahrt. Offline Security Agents erhalten Update-Benachrichtigungen, wenn die Security Agents während des 7-tägigen Zeitraums online sind.

3. Klicken Sie auf **Save**.

Agent-Update-Einstellungen konfigurieren

Detaillierte Erklärungen zu Agent-Updates erhalten Sie unter *Agent-Updates auf Seite 5-9*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.

2. Klicken Sie in der Agent-Struktur auf das Stammsymbol (), um alle Security Agents oder nur bestimmte Gruppen oder Security Agents einzubeziehen.

3. Klicken Sie auf **Einstellungen** > **Einstellungen für Updates**.

4. Wählen Sie **Agents laden Updates vom Trend Micro ActiveUpdate Server herunter, wenn keine Verbindung zum Trend Apex One (Mac) server möglich ist**, um externen Security Agents das Herunterladen von Updates vom Trend Micro ActiveUpdate Server zu erlauben.

Hinweis

Wenn ein Security Agent ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Agent-Updates in *Einschränkungen bei reinen IPv6-Agents auf Seite A-3*.

5. Wählen Sie **Agents können die Komponenten aktualisieren, nicht jedoch das Agent-Programm upgraden oder Hot Fixes installieren**, um Komponenten-Updates zuzulassen, aber das Upgrade von Trend Micro Apex One (Mac)Security Agent zu verhindern.

6. Führen Sie die folgenden Schritte aus, um geplante Updates einzurichten:

   a. Wählen Sie **Zeitgesteuertes Update aktivieren**.

   b. Konfigurieren Sie den Zeitplan.

   c. Geben Sie bei Auswahl von **Täglich** oder **Wöchentlich** die Uhrzeit des Updates und den Zeitraum an, in dem der Apex One (Mac) Server Security Agents zum Update der Komponenten auffordert. Wenn Sie die Startzeit beispielsweise für 12 Uhr und den Zeitraum mit 2 Stunden festlegen, fordert der Server zwischen 12 und 14 Uhr in zufälligen Abständen alle online geschalteten Security Agents zum Update auf. Mit dieser Einstellung wird verhindert, dass sich alle Security Agents gleichzeitig zum festgelegten Zeitpunkt mit dem Server verbinden, damit es zu keiner Überlastung des Servers kommt.

7. Wenn Sie eine oder mehrere Gruppen oder Security Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die Gruppen oder Security Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:
   - **Für alle Agenten übernehmen**: Wendet die Einstellungen auf alle vorhandenen Security Agents und auf neu zu einer vorhandenen/zukünftigen Gruppe hinzukommende Agents an. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Gruppen anwenden**: Wendet die Einstellungen nur auf Security Agents an, die zukünftigen Gruppen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf Security Agents angewendet, die einer vorhandenen Gruppe hinzugefügt werden.

Agent-Updates aus dem Übersichtsfenster starten

Informationen zu anderen Agent-Update-Methoden finden Sie unter *Agent-Updates auf Seite 5-9*.

Prozedur

1. Klicken Sie im Hauptmenü auf **Übersicht**.
2. Gehen Sie zum Abschnitt **Update-Status** und klicken Sie auf den Link unter der Spalte **Nicht aktuell**.

   Die Agent-Struktur öffnet sich und zeigt alle Security Agents, die ein Update benötigen.
3. Wählen Sie die Security Agents aus, die Sie aktualisieren möchten.
4. Klicken Sie auf **Tasks** > **Update**.

   Security Agents, die die Benachrichtigung erhalten, beginnen mit der Aktualisierung. Auf Endpunkten zeigt das Trend Micro Apex One (Mac)-Symbol in der Menüleiste an, dass das Produkt aktualisiert wird.

Benutzer können keine Aufgaben von der Konsole ausführen, bis die Aktualisierung abgeschlossen ist.

Agent-Updates aus dem Agent-Verwaltung-Fenster starten

Informationen zu anderen Agent-Update-Methoden finden Sie unter *Agent-Updates auf Seite 5-9*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stammdomänensymbol ( ) um alle Security Agents einzuschließen oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Tasks** > **Update**.

   Security Agents, die die Benachrichtigung erhalten, beginnen mit dem Update. Auf Endpunkten zeigt das Trend Micro Apex One (Mac)-Symbol in der Menüleiste an, dass das Produkt aktualisiert wird. Benutzer können keine Aufgaben von der Konsole ausführen, bis das Update abgeschlossen ist.

Kapitel 6

Endpunkte vor Sicherheitsrisiken schützen

In diesem Kapitel wird beschrieben, wie Sie Endpunkte durch dateibasierte Suchvorgänge vor Sicherheitsrisiken schützen können.

Info über Sicherheitsrisiken

Sicherheitsrisiken umfassen Viren, Malware, Spyware und Grayware. Trend Micro Apex One (Mac) schützt Endpunkte vor Sicherheitsrisiken, indem Dateien durchsucht werden und dann eine spezifische Aktion für jedes entdeckte Sicherheitsrisiko durchgeführt wird. Eine große Anzahl entdeckter Sicherheitsrisiken innerhalb kurzer Zeit deutet auf einen Virenausbruch hin. Durch Anwendung von Ausbruchspräventionsrichtlinien und die Isolierung infizierter Endpunkte, bis keine Bedrohung mehr von ihnen ausgeht, kann Trend Micro Apex One (Mac) helfen, die schädlichen Auswirkungen zu begrenzen. Mittels Benachrichtigungen und Protokollen werden Sie ständig über den Verlauf der Sicherheitsrisiken informiert und alarmiert, wenn Sofortmaßnahmen erforderlich sind.

Viren und Malware

Zehntausende von Viren und Malware-Typen sind bereits bekannt, und täglich kommen neue hinzu. Durch Ausnutzen von Schwachstellen in Unternehmensnetzwerken, E-Mail-Systemen und Websites können Endpunktviren heutzutage verheerende Schäden anrichten.

Trend Micro Apex One (Mac) schützt Endpunkte vor folgenden Viren- und Malware-Typen:

Viren-/Malware-Typen	Beschreibung
Scherzprogramm	Ein Scherzprogramm ist ein virenähnliches Programm, das meist die Anzeige auf dem Bildschirm des Endpunkts verändert.
Trojaner	Ein Trojaner ist ein ausführbares Programm, das sich nicht selbst repliziert, sondern auf einem Endpunkt einnistet und unerwünschte Aktionen auslöst (z. B. Ports für Hacker zugänglich macht). Dieses Programm verschafft sich oft über Trojanerports Zugang zu Endpunkten. Ein bekanntes Beispiel für einen Trojaner ist eine Anwendung, die vorgibt, den betreffenden Endpunkt von Viren zu befreien, obwohl sie in Wirklichkeit den Endpunkt mit Viren infiziert.

Viren-/Malware-Typen	Beschreibung
Virus	Ein Virus ist ein Programm, das sich selbst vervielfältigt. Der Virus muss sich dazu an andere Programmdateien anhängen und wird ausgeführt, sobald das Host-Programm ausgeführt wird. • **Bootvirus**: Diese Virenart infiziert den Bootsektor von Partitionen oder Festplatten. • **Bösartiger Java-Code**: Virencode, der in Java geschrieben oder eingebettet wurde und auf einem beliebigen Betriebssystem ausgeführt werden kann • **Makrovirus**: Diese Virenart ist wie das Makro einer Anwender-Software aufgebaut und verbirgt sich häufig in Dokumenten. • **VBScript-, JavaScript- oder HTML-Virus**: Ein Virus, der sich auf Websites verbirgt und über den Browser heruntergeladen wird • **Wurm**: Ein eigenständig oder in Gruppen auftretendes Programm, das funktionsfähige Kopien von sich selbst oder seinen Segmenten an andere Endpunkte (meist per E-Mail) verteilen kann.
Testvirus:	Ein Testvirus ist eine inaktive Datei, die von Antiviren-Software erkannt wird. Mit Testviren wie dem EICAR-Testskript können Sie die Funktion Ihrer Antiviren-Software überprüfen.
Packer	Packer sind komprimierte und/oder verschlüsselte ausführbare Programme für Windows oder Linux™; häufig handelt es sich dabei um Trojaner. In komprimierter Form ist ein Packer für ein Antiviren-Programm schwieriger zu erkennen.
Wahrscheinlich Virus/ Malware	Verdächtige Dateien, die einige Eigenschaften von Viren/Malware aufweisen, werden als dieser Viren-/Malware-Typ kategorisiert. Weitere Informationen über wahrscheinliche Viren/Malware finden Sie in der Trend Micro Online-Viren-Enzyklopädie: http://www.trendmicro.de/vinfo/de/threat-encyclopedia/
Andere	„Andere“ bezieht sich auf die Viren/Malware, die unter keinem der Viren-/Malware-Typen eingestuft wurden.

Spyware und Grayware

Die Begriffe Spyware und Grayware beziehen sich auf Anwendungen oder Dateien, die nicht als Viren oder Malware eingestuft werden, sich aber dennoch negativ auf die Leistung von Endpunkten im Netzwerk auswirken können. Spyware stellt ebenso wie Grayware ein signifikantes Sicherheits-, Vertraulichkeits- und rechtliches Risiko für eine Organisation dar. Häufig führt Spyware/Grayware eine Vielzahl unerwünschter und bedrohlicher Aktionen durch. Dazu zählen das Öffnen lästiger Popup-Fenster, das Aufzeichnen von Tastatureingaben und das Offenlegen von Sicherheitslücken, durch die der Endpunkt angegriffen werden kann.

Trend Micro Apex One (Mac) schützt Endpunkte vor folgenden Spyware- und Grayware-Typen:

Spyware-/ Grayware-Typen	Beschreibung
Spyware	Spyware sammelt Daten wie Benutzernamen, Kennwörter, Kreditkartennummern und andere vertrauliche Informationen, um sie an Dritte weiterzuleiten.
Adware	Adware zeigt Werbeschaltungen an und protokolliert Benutzerdaten, beispielsweise das Surfverhalten im Internet, die wiederum zu Werbezwecken genutzt werden.
Dialer	Ein Dialer ändert die Internet-Einstellungen des Clients und erzwingt auf dem Endpunkt das Wählen von voreingestellten Telefonnummern über ein Modem. Oft handelt es sich um Pay-per-Call oder internationale Rufnummern, die einem Unternehmen beträchtliche Kosten verursachen können.
Hacker-Tools	Ein Hacker-Tool hilft Hackern, sich Zugriff auf eine Endpunkt zu verschaffen.
Tools für den Remote-Zugriff	Mit einem Tool für den Remote-Zugriff können Hacker per Fernzugriff in Endpunkte eindringen und diese steuern.
Anwendungen zum Entschlüsseln von Kennwörtern	Mit Hilfe solcher Anwendungen versuchen Hacker, Benutzernamen und Kennwörter zu entschlüsseln.

Spyware-/ Grayware-Typen	Beschreibung
Andere	„Andere“ bezieht sich auf die potenziell bösartige Programme, die unter keinem der Spyware-/Grayware-Typen eingestuft wurden.

Suchmethodentypen

Trend Micro Apex One (Mac)Security Agents können eine von zwei Suchmethoden anwenden, wenn sie nach Sicherheitsrisiken suchen. Die Suchmethoden sind intelligente Suche und herkömmliche Suche.

- **Intelligente Suche**

  Security Agents, die die intelligente Suche anwenden, werden in diesem Dokument als „Smart Scan Agents“ bezeichnet. Smart Scan Agents nutzen die lokale Suche und webbasierte Abfragen, die von File Reputation-Diensten bereitgestellt werden.

- **Herkömmliche Suche**

  Security Agents, die Smart Scan nicht anwenden, werden als „Herkömmliche Suchagenten“ bezeichnet. Ein Agent zur herkömmlichen Suche speichert alle Trend Micro Apex One (Mac)-Komponenten auf dem Agent-Endpunkt und durchsucht alle Dateien lokal.

Standard-Suchmethode

Die standardmäßige Suchmethode für neue Trend Micro Apex One (Mac)-Serverinstallationen ist die intelligente Suche.

Suchmethoden im Vergleich

Die folgende Tabelle beinhaltet einen Vergleich zwischen den beiden Suchmethoden.

Tabelle 6-1. Vergleich zwischen herkömmlicher Suche und intelligenter Suche

Vergleichsgrundlage	Herkömmliche Suche	Intelligente Suche
Verfügbarkeit	Verfügbar in dieser Trend Micro Apex One (Mac) Version.	Verfügbar in dieser Trend Micro Apex One (Mac) Version.
Suchverhalten	Der Agent zur herkömmlichen Suche durchsucht den lokalen Endpunkt.	• Der intelligente Suchagent durchsucht den lokalen Endpunkt. • Wenn der Security Agent das Risiko der Datei während der Suche nicht ermitteln kann, überprüft Security Agent dies, indem er eine Suchabfrage an eine Smart Protection-Quelle sendet. • Der Security Agent legt die Ergebnisse der Suchabfrage zur Verbesserung der Suchleistung in einem Zwischenspeicher ab.
Verwendete und aktualisierte Komponenten	Alle unter der Update-Adresse verfügbaren Komponenten, außer dem Mac-Heuristik-Pattern und dem Agent-Pattern der intelligenten Suche.	Alle unter der Update-Adresse verfügbaren Komponenten, außer dem Viren-Pattern und dem Spyware-Aktivmonitor-Pattern.
Typische Update-Adresse	Trend Micro Apex One (Mac) Server	Trend Micro Apex One (Mac) Server

Suchmethode ändern

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol (), um alle Security Agents oder nur bestimmte Gruppen oder Security Agents einzubeziehen.

3. Klicken Sie auf **Einstellungen** > **Suchmethoden**.
4. Wählen Sie **Herkömmliche Suche** oder **Intelligente Suche**.
5. Wenn Sie eine oder mehrere Gruppen oder Security Agent in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**. Wenn Sie auf das Stammsymbol geklickt haben, stehen Ihnen die folgenden Optionen zur Verfügung:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Security Agents und auf alle neuen Security Agent an, die einer vorhandenen/zukünftigen Gruppe hinzugefügt werden. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Gruppen anwenden**: Wendet die Einstellungen nur auf Security Agents an, die zukünftigen Gruppen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf Security Agent angewendet, die einer vorhandenen Gruppe hinzugefügt werden.

Wechsel von der intelligenten Suche zur herkömmlichen Suche

Die folgende Tabelle bietet weitere Überlegungen beim Wechsel von Security Agents zur herkömmlichen Suche.

Tabelle 6-2. Überlegungen bei der Umstellung auf die herkömmliche Suche

Überlegung	Details
Anzahl der umzuschaltenden Security Agents	Wenn Sie eine relativ kleine Anzahl von Security Agents gleichzeitig umschalten, werden die Ressourcen von Trend Micro Apex One (Mac) Server und Smart Protection Server effizient genutzt. Diese Server können andere wichtige Aufgaben ausführen, während Security Agents ihre Suchmethoden ändern.

ÜBERLEGUNG	DETAILS
Timing	Wenn Sie wieder auf die herkömmliche Suche umschalten, wird Security Agents wahrscheinlich die vollständige Version des Viren-Patterns und des Spyware-Aktivmonitor-Patterns vom Trend Micro Apex One (Mac) Server herunterladen. Diese Pattern-Dateien werden nur von den Agents der herkömmlichen Suche verwendet. Die Umschaltung sollte bei geringem Netzaufkommen durchgeführt werden, um sicherzustellen, dass der Download-Prozess in kurzer Zeit beendet wird. Außerdem sollten Sie dann umschalten, wenn keine Aktualisierung eines Security Agent über den Server geplant ist.
Einstellungen der Agent-Hierarchie	Die Suchmethode ist eine granulare Einstellung, die auf Root- oder Domänenebene oder für einen einzelnen Security Agent festgelegt werden kann. Wenn Sie zur herkömmlichen Suche wechseln, können Sie: • Erstellen Sie eine neue Gruppe und ordnen Sie die herkömmliche Suche als Suchmethode zu. Alle Security Agent, die Sie in diese Gruppe verschieben, werden die herkömmliche Suche verwenden. Wenn Sie den Security Agent verschieben, aktivieren Sie die Einstellung **Einstellungen der neuen Gruppe für ausgewählte Agents übernehmen**. • Wählen Sie eine Gruppe aus, und konfigurieren Sie diese zur Verwendung der herkömmlichen Suche. Agents der intelligenten Suche, die der Gruppe angehören, werden auf die herkömmliche Suche umgestellt. • Wählen Sie einen oder mehrere Agents der herkömmlichen Suche aus einer Gruppe aus, und stellen Sie diese dann auf die intelligente Suche um. **Hinweis** Alle Änderungen an der Suchmethode der Gruppe überschreiben die Suchmethode, die Sie für individuelle Security Agents konfiguriert haben.

Wechsel von der herkömmlichen Suche zur intelligenten Suche

Wenn Sie Security Agents von der herkömmlichen Suche auf die intelligente Suche umstellen, stellen Sie sicher, dass Smart Protection-Dienste auf dem Apex One-Server eingerichtet sind. Weitere Informationen finden Sie in der Apex One-Dokumentation.

Die folgende Tabelle bietet weitere Überlegungen beim Wechsel von Security Agent zur intelligenten Suche.

TABELLE 6-3. Überlegungen bei der Umstellung auf die intelligente Suche

ÜBERLEGUNG	DETAILS
Produktlizenz	Um die intelligente Suche zu verwenden, vergewissern Sie sich, dass Sie die Lizenzen für die folgenden Dienste auf dem Apex One Server aktiviert haben und die Lizenzen nicht abgelaufen sind: • Virenschutz • Web Reputation und Anti-Spyware
Apex One (Mac) Server	Stellen Sie sicher, dass Security Agents eine Verbindung zum Apex One (Mac)-Server herstellen kann. Nur online Security Agents werden benachrichtigt, um auf intelligente Suche umzuschalten. Offline Security Agents werden benachrichtigt, wenn sie online gehen. Roaming Security Agents werden benachrichtigt, wenn sie online gehen oder, falls der Security Agent Berechtigungen für zeitgesteuerte Updates hat, wenn das zeitgesteuerte Update ausgeführt wird. Überprüfen Sie auch, ob der Trend Micro Apex One (Mac)-Server die neuesten Komponenten hat, da Smart Scan Agents das Mac Heuristic Pattern und das Smart Scan Agent Pattern vom Server herunterladen müssen. Um Komponenten zu aktualisieren, siehe *Server-Update auf Seite 5-4*.
Anzahl der umzuschaltenden Security Agents	Wenn Sie eine relativ kleine Anzahl von Security Agents gleichzeitig umschalten, werden die Ressourcen des Apex One (Mac) Servers effizient genutzt. Der Apex One (Mac) Server kann andere wichtige Aufgaben ausführen, während Security Agents ihre Suchmethoden ändern.

ÜBERLEGUNG	DETAILS
Timing	Wenn Sie zum ersten Mal zu Smart Scan wechseln, müssen Security Agents die Vollversion des Mac Heuristic Pattern und des Smart Scan Agent Pattern vom Server mit Apex One (Mac) herunterladen. Das Smart Scan Pattern wird nur von Smart Scan-Agents verwendet. Die Umschaltung sollte bei geringem Netzaufkommen durchgeführt werden, um sicherzustellen, dass der Download-Prozess in kurzer Zeit beendet wird. Außerdem sollten Sie dann umschalten, wenn keine Aktualisierung eines Security Agent über den Server geplant ist.
Einstellungen der Agent-Hierarchie	Die Suchmethode ist eine granuläre Einstellung, die auf Stamm- oder Gruppenebene oder für einzelne Agents festgelegt werden kann. Bei der Umschaltung zur intelligenten Suche können Sie Folgendes tun: • Erstellen Sie eine neue Gruppe und ordnen Sie die intelligente Suche als Suchmethode zu. Alle Security Agent, die Sie in diese Gruppe verschieben, werden die intelligente Suche verwenden. Wenn Sie den Security Agent verschieben, aktivieren Sie die Einstellung **Einstellungen der neuen Gruppe auf ausgewählte Agenten anwenden**. • Wählen Sie eine Gruppe aus, und konfigurieren Sie diese zur Verwendung der intelligenten Suche. Agents der herkömmlichen Suche, die der Gruppe angehören, werden auf die intelligente Suche umgestellt. • Wählen Sie einen oder mehrere Agents der herkömmlichen Suche aus einer Gruppe aus, und stellen Sie diese dann auf die intelligente Suche um. **Hinweis** Alle Änderungen an der Suchmethode der Gruppe überschreiben die Suchmethode, die Sie für individuelle Security Agents konfiguriert haben.

Überlegung	Details
IPv6-Unterstützung	Die Agents der intelligenten Suche senden Suchabfragen an Smart Protection Quellen. Ein reiner IPv6-Agent der intelligenten Suche kann Abfragen nicht direkt an IPv4-Quellen senden wie zum Beispiel: • Smart Protection Server 3.0 (integriert oder eigenständig) **Hinweis** IPv6-Unterstützung für Smart Protection Server ist ab Version 2.5 verfügbar. • Trend Micro Smart Protection Network Entsprechend kann ein reiner IPv4-Agent der intelligenten Suche ebenfalls keine Abfragen an reine IPv6 Smart Protection Server senden. Ein Dual-Stack-Proxy-Server wie beispielsweise DeleGate, der IP-Adressen konvertieren kann, muss ermöglichen, dass Agents der intelligenten Suche eine Verbindung zu den Quellen herstellen können.

Suchtypen

Apex One (Mac) stellt die folgenden Suchtypen bereit, um Endpunkte vor Sicherheitsrisiken zu schützen:

Suchtyp	Beschreibung
Echtzeitsuche	Beim Empfangen, Öffnen, Herunterladen, Kopieren oder Ändern einer Datei wird diese automatisch durchsucht. Weitere Informationen finden Sie unter *Echtzeitsuche auf Seite 6-12*.
Manuelle Suche	Eine vom Benutzer eingeleitete Suche, bei der eine vom Benutzer angeforderte Datei oder ein Dateisatz durchsucht wird. Weitere Informationen finden Sie unter *Manuelle Suche auf Seite 6-15*.

Suchtyp	Beschreibung
Zeitgesteuerte Suche	Dateien auf dem Endpunkt werden automatisch gemäß dem vom Administrator festgelegten Zeitplan durchsucht. Weitere Informationen finden Sie unter *Zeitgesteuerte Suche auf Seite 6-19*.
Jetzt durchsuchen	Eine vom Administrator gestartete Suche, bei der Dateien auf einem oder mehreren Zielendpunkten durchsucht werden. Weitere Informationen finden Sie unter *Jetzt durchsuchen auf Seite 6-25*.

Echtzeitsuche

Die Echtzeitsuche wird kontinuierlich und dauerhaft ausgeführt. Bei jedem Empfang, Öffnen, Herunterladen, Kopieren oder Ändern einer Datei wird diese durch die Echtzeitsuche nach Sicherheitsrisiken durchsucht. Wenn Trend Micro Apex One (Mac) kein Sicherheitsrisiko erkennt, verbleibt die Datei an ihrem Speicherort und Benutzer können darauf zugreifen. Wenn Trend Micro Apex One (Mac) ein Sicherheitsrisiko entdeckt, wird eine Nachricht mit dem Namen der infizierten Datei und dem jeweiligen Sicherheitsrisiko angezeigt.

Konfigurieren und Anwenden der Echtzeitsuche-Einstellungen für einen oder mehrere Security Agents und Gruppen bzw. für alle Security Agents, die vom Server verwaltet werden.

Einstellungen der Echtzeitsuche konfigurieren

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon ( ), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für Echtzeitsuche**.
4. Aktivieren Sie das Kontrollkästchen, um die Echtzeitsuche zu aktivieren.

5. Klicken Sie auf die Registerkarte **Ziel**, um die Dateiaktivitäten und die Sucheinstellungen zu konfigurieren.

   Weitere Informationen finden Sie unter *Echtzeitsuche: Registerkarte "Ziel" auf Seite 6-13*.

6. Klicken Sie auf die Registerkarte **Aktion**, um die Suchaktionen zu konfigurieren, die Apex One (Mac) bei entdeckten Sicherheitsbedrohungen durchführen soll.

   Weitere Informationen finden Sie unter *Echtzeitsuche: Registerkarte "Aktion" auf Seite 6-14*.

7. Wenn Sie eine oder mehrere Gruppen oder Security Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die Gruppen oder Security Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:

   - **Für alle Agenten übernehmen**: Wendet die Einstellungen auf alle vorhandenen Security Agents und auf alle neuen Security Agent an, die einer vorhandenen/zukünftigen Gruppe hinzugefügt werden. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden sind.
   - **Nur auf zukünftige Gruppen anwenden**: Wendet die Einstellungen nur auf Security Agents an, die zukünftigen Gruppen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf Security Agents angewendet, die einer vorhandenen Gruppe hinzugefügt werden.

Echtzeitsuche: Registerkarte "Ziel"

Prozedur

1. Unter **Benutzerdefinierte Aktionen für Dateien** wählen Sie Aktivitäten für Dateien aus, die die Echtzeitsuche auslösen. Wählen Sie unter folgenden Optionen:

- **Dateien beim Erstellen/Ändern DURCHSUCHEN**: Durchsucht Dateien, die dem Endpunkt neu hinzugefügt werden (z. B. nach dem Herunterladen einer Datei) oder gerade verändert werden
- **Dateien beim Abrufen/Ausführen DURCHSUCHEN**: Durchsucht Dateien, wenn sie geöffnet werden
- **Dateien durchsuchen, die erstellt/bearbeitet und abgefragt/ausgeführt werden**
- **Dateien durchsuchen, die erstellt/bearbeitet/ausgeführt werden**

Angenommen, die dritte Option wird aktiviert: Wird eine neue Datei auf den Endpunkt heruntergeladen, wird sie durchsucht und bleibt an ihrem aktuellen Speicherort, wenn kein Sicherheitsrisiko entdeckt wird. Dieselbe Datei wird erneut durchsucht, wenn sie geöffnet wird und bevor etwaige Änderungen daran gespeichert werden.

2. Wählen Sie unter **Sucheinstellungen** eine oder mehrere der folgenden Optionen aus:
   - **Komprimierte Dateien durchsuchen**: Einzelne Dateien innerhalb einer Archivdatei durchsuchen

     Weitere Informationen finden Sie unter *Unterstützte komprimierte Dateitypen auf Seite 6-26*.
   - **Scan network drive**: Durchsucht Verzeichnisse, die sich physisch auf anderen Endpunkten befinden, aber dem lokalen Endpunkt zugeordnet sind

---

Echtzeitsuche: Registerkarte "Aktion"

Auf der Registerkarte **Aktionen** konfigurieren Sie die Suchaktionen, die Apex One (Mac) bei entdeckten Sicherheitsbedrohungen durchführen soll.

Prozedur

1. Geben Sie unter **Aktion** die Suchaktionen an.

Optionen	Beschreibung
ActiveAction verwenden	In ActiveAction sind mehrere vorkonfigurierte Aktionen für die Suche nach unterschiedlichen Arten von Sicherheitsrisiken zusammengefasst. Trend Micro empfiehlt die Verwendung von ActiveAction, wenn Sie nicht genau wissen, welche Suchaktion sich für einen bestimmten Typ von Sicherheitsrisiko am besten eignet. Die ActiveAction-Einstellungen werden in den Pattern-Dateien ständig aktualisiert, um Endpunkte gegen die neuesten Sicherheitsrisiken und Angriffsmethoden zu schützen.
Die gleiche Aktion für alle Typen von Sicherheitsrisiken verwenden	Wählen Sie diese Option, wenn dieselbe Aktion für alle Typen von Sicherheitsrisiken außer für wahrscheinliche Viren/Malware durchgeführt werden soll. Beim Typ „Wahrscheinlich Virus/ Malware“ erfolgt stets die Aktion „Übergehen“. Wenn Sie „Säubern“ als erste Aktion auswählen, geben Sie eine Ersatzaktion an, die Apex One (Mac) durchführt, falls das Säubern fehlschlägt. Nur wenn die erste Aktion „Säubern“ ist, ist eine zweite Aktion einstellbar. Details zu den Suchoptionen finden Sie unter *Suchaktionen auf Seite 6-27*.

2. Wählen Sie **Eine Benachrichtigung auf dem Agent anzeigen, wenn Viren-/Malware erkannt wird**, um eine Benachrichtigung anzuzeigen, wenn Apex One (Mac) während der Echtzeitsuche ein Sicherheitsrisiko erkennt.

Manuelle Suche

Die manuelle Suche wird bei Bedarf gestartet, wenn der Benutzer sie in der Agent-Konsole aktiviert. Die Dauer der Suche hängt von der Anzahl der zu durchsuchenden Dateien und den Hardware-Ressourcen des Endpunkts ab.

Sie können die Einstellungen für die manuelle Suche für einen oder mehrere Security Agents und Gruppen bzw. für alle Security Agents, die vom Server verwaltet werden, konfigurieren und anwenden.

Einstellungen für manuelle Suche konfigurieren

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon ( ), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für manuelle Suche**.
4. Klicken Sie auf die Registerkarte **Ziel**, um die Einstellungen für die allgemeine Suche und die CPU-Nutzung zu konfigurieren.

   Weitere Informationen finden Sie unter *Manuelle Suche: Registerkarte "Ziel" auf Seite 6-17*.
5. Klicken Sie auf die Registerkarte **Aktion**, um die Suchaktionen zu konfigurieren, die Apex One (Mac) bei entdeckten Sicherheitsbedrohungen durchführen soll.

   Weitere Informationen finden Sie unter *Manuelle Suche: Registerkarte "Aktion" auf Seite 6-18*.
6. Wenn Sie eine oder mehrere Gruppen oder Security Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die Gruppen oder Security Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:
   - **Für alle Agenten übernehmen**: Wendet die Einstellungen auf alle vorhandenen Security Agents und auf alle neuen Security Agent an, die einer vorhandenen/zukünftigen Gruppe hinzugefügt werden. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden sind.

- **Nur auf zukünftige Gruppen anwenden**: Wendet die Einstellungen nur auf Security Agents an, die zukünftigen Gruppen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf Security Agents angewendet, die einer vorhandenen Gruppe hinzugefügt werden.

Manuelle Suche: Registerkarte "Ziel"

Prozedur

1. Wählen Sie im Abschnitt **Zu durchsuchende Dateien** eine der folgenden Optionen aus:

   - **Alle durchsuchbaren Dateien**: alle durchsuchbaren Dateien werden berücksichtigt. Zu den nicht durchsuchbaren Dateien gehören kennwortgeschützte und verschlüsselte Dateien sowie Dateien, die die vom Benutzer festgelegten Suchkriterien nicht erfüllen.

     Hinweis

     Das Durchsuchen jeder Datei erfordert viel Zeit und viele Ressourcen und ist möglicherweise in manchen Fällen gar nicht notwendig. Deshalb können Sie bei Bedarf die Anzahl der Dateien begrenzen, die der Security Agent durchsucht.

   - **Nur Mach-O-Dateien durchsuchen**: Nur Mach-O-Dateien auf Endpunkten durchsuchen. Apex One (Mac) Security Agents durchsucht keine anderen Dateitypen auf Malware.

     Hinweis

     Wenn Sie diese Option auswählen, müssen Sie die Funktion für intelligente Suche aktivieren, um Schutz vor den neuesten Malware-Angriffen auf OS X- und macOS-Plattformen zu gewährleisten.

2. Wählen Sie unter **Sucheinstellungen** eine oder mehrere der folgenden Optionen aus:

- **Komprimierte Dateien durchsuchen**: Einzelne Dateien innerhalb einer Archivdatei durchsuchen

  Weitere Informationen finden Sie unter *Unterstützte komprimierte Dateitypen auf Seite 6-26*.

- **Scan network drive**: Durchsucht Verzeichnisse, die sich physisch auf anderen Endpunkten befinden, aber dem lokalen Endpunkt zugeordnet sind
- **Zeitmaschine durchsuchen**: Nur Dateien auf Time Machine-Laufwerken durchsuchen

Hinweis

Nach dem Aktivieren der Option **Zeitmaschine durchsuchen** für die manuelle und zeitgesteuerte Suche kann Apex One (Mac) Malware-Bedrohungen nur erkennen. Aufgrund von Berechtigungseinschränkungen im Mac-Betriebssystem können keine entsprechenden Aktionen (Bereinigen, Quarantäne oder Löschen) ergriffen werden. Konfigurierte Suchaktionen werden in den Produktprotokollen als nicht erfolgreich angezeigt.

3. Konfigurieren Sie im Abschnitt **CPU-Auslastung** die erforderlichen Einstellungen.
   - **Hoch**: Ohne Pause zwischen den Suchläufen
   - **Niedrig**: Pause zwischen den Suchläufen, wenn die CPU-Auslastung über 20 % liegt, sonst keine Pause

Manuelle Suche: Registerkarte "Aktion"

Auf der Registerkarte **Aktionen** konfigurieren Sie die Suchaktionen, die Apex One (Mac) bei entdeckten Sicherheitsbedrohungen durchführen soll.

Optionen	Beschreibung
ActiveAction verwenden	In ActiveAction sind mehrere vorkonfigurierte Aktionen für die Suche nach unterschiedlichen Arten von Sicherheitsrisiken zusammengefasst. Trend Micro empfiehlt die Verwendung von ActiveAction, wenn Sie nicht genau wissen, welche Suchaktion sich für einen bestimmten Typ von Sicherheitsrisiko am besten eignet. Die ActiveAction-Einstellungen werden in den Pattern-Dateien ständig aktualisiert, um Endpunkte gegen die neuesten Sicherheitsrisiken und Angriffsmethoden zu schützen.
Die gleiche Aktion für alle Typen von Sicherheitsrisiken verwenden	Wählen Sie diese Option, wenn dieselbe Aktion für alle Typen von Sicherheitsrisiken außer für wahrscheinliche Viren/Malware durchgeführt werden soll. Beim Typ „Wahrscheinlich Virus/Malware“ erfolgt stets die Aktion „Übergehen“. Wenn Sie „Säubern“ als erste Aktion auswählen, geben Sie eine Ersatzaktion an, die Apex One (Mac) durchführt, falls das Säubern fehlschlägt. Nur wenn die erste Aktion „Säubern“ ist, ist eine zweite Aktion einstellbar. Details zu den Suchoptionen finden Sie unter *Suchaktionen auf Seite 6-27*.

Zeitgesteuerte Suche

Die zeitgesteuerte Suche wird automatisch zur angegebenen Uhrzeit am angegebenen Datum ausgeführt. Verwenden Sie die zeitgesteuerte Suche, um die routinemäßige Suche auf dem Security Agent zu automatisieren und die Verwaltung der Virensuche zu optimieren.

Konfigurieren und Anwenden der Einstellungen für die Zeitgesteuerte Suche für einen oder mehrere Security Agents und Gruppen bzw. für alle Security Agents, die vom Server verwaltet werden.

Einstellungen für zeitgesteuerte Suche konfigurieren

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon (), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für die zeitgesteuerte Suche**.
4. Aktivieren Sie das Kontrollkästchen, um die zeitgesteuerte Suche zu aktivieren.
5. Klicken Sie auf der Registerkarte **Ziel** die Einstellungen für die allgemeine Suche und die CPU-Nutzung sowie die Einstellungen für die zeitgesteuerte Suche.

   Weitere Informationen finden Sie unter *Zeitgesteuerte Suche: Registerkarte "Ziel" auf Seite 6-21*.
6. Klicken Sie auf die Registerkarte **Aktion**, um die Suchaktionen zu konfigurieren, die Apex One (Mac) bei entdeckten Sicherheitsbedrohungen durchführen soll.

   Weitere Informationen finden Sie unter *Zeitgesteuerte Suche: Registerkarte "Aktion" auf Seite 6-22*.
7. Wenn Sie eine oder mehrere Gruppen oder Security Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die Gruppen oder Security Agents anzuwenden. Wenn Sie auf das Stammsymbol () geklickt haben, haben Sie folgende Optionen:
   - **Für alle Agenten übernehmen**: Wendet die Einstellungen auf alle vorhandenen Security Agents und auf alle neuen Security Agent an, die einer vorhandenen/zukünftigen Gruppe hinzugefügt werden. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden sind.

- **Nur auf zukünftige Gruppen anwenden**: Wendet die Einstellungen nur auf Security Agents an, die zukünftigen Gruppen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf Security Agents angewendet, die einer vorhandenen Gruppe hinzugefügt werden.

Zeitgesteuerte Suche: Registerkarte "Ziel"

Prozedur

1. Unter **Zeitplan** stellen Sie ein, wie oft (täglich, wöchentlich oder monatlich) und wann die zeitgesteuerte Suche durchgeführt werden soll.

   Für die monatliche zeitgesteuerte Suche, wenn Sie den 29., 30. oder 31. Tag ausgewählt haben und ein Monat diesen Tag nicht hat, führt Apex One (Mac) die zeitgesteuerte Suche am letzten Tag des Monats durch.

2. Wählen Sie im Abschnitt **Zu durchsuchende Dateien** eine der folgenden Optionen aus:

   - **Alle durchsuchbaren Dateien**: alle durchsuchbaren Dateien werden berücksichtigt. Zu den nicht durchsuchbaren Dateien gehören kennwortgeschützte und verschlüsselte Dateien sowie Dateien, die die vom Benutzer festgelegten Suchkriterien nicht erfüllen.

     Hinweis

     Das Durchsuchen jeder Datei erfordert viel Zeit und viele Ressourcen und ist möglicherweise in manchen Fällen gar nicht notwendig. Deshalb können Sie bei Bedarf die Anzahl der Dateien begrenzen, die der Security Agent durchsucht.

   - **Dateitypen gescannt von IntelliScan**: Durchsucht nur Dateien, die potenziell bösartigen Code enthalten, selbst wenn dieser sich hinter einer scheinbar harmlosen Erweiterung verbirgt.
   - **Geben Sie den Pfad oder den vollständigen Pfad an**: Geben Sie manuell die Dateien oder Verzeichnisse an, die durchsucht werden

sollen. Zum Beispiel `/Shared/Files/mytext.txt` oder `/Shared/Files`.

3. Wählen Sie unter **Sucheinstellungen** eine oder mehrere der folgenden Optionen aus:

   - **Komprimierte Dateien durchsuchen**: Einzelne Dateien innerhalb einer Archivdatei durchsuchen

     Weitere Informationen finden Sie unter *Unterstützte komprimierte Dateitypen auf Seite 6-26*.

   - **Zeitmaschine durchsuchen**: Nur Dateien auf Time Machine-Laufwerken durchsuchen

     Hinweis

     Nach dem Aktivieren der Option **Zeitmaschine durchsuchen** für die manuelle und zeitgesteuerte Suche kann Apex One (Mac) Malware-Bedrohungen nur erkennen. Aufgrund von Berechtigungseinschränkungen im Mac-Betriebssystem können keine entsprechenden Aktionen (Bereinigen, Quarantäne oder Löschen) ergriffen werden. Konfigurierte Suchaktionen werden in den Produktprotokollen als nicht erfolgreich angezeigt.

4. Konfigurieren Sie im Abschnitt **CPU-Auslastung** die erforderlichen Einstellungen.

   - **Hoch**: Ohne Pause zwischen den Suchläufen
   - **Niedrig**: Pause zwischen den Suchläufen, wenn die CPU-Auslastung über 20 % liegt, sonst keine Pause

Zeitgesteuerte Suche: Registerkarte "Aktion"

Auf der Registerkarte **Aktionen** konfigurieren Sie die Suchaktionen, die Apex One (Mac) bei entdeckten Sicherheitsbedrohungen durchführen soll.

Prozedur

1. Geben Sie unter **Aktion** die Suchaktionen an.

Optionen	Beschreibung
ActiveAction verwenden	In ActiveAction sind mehrere vorkonfigurierte Aktionen für die Suche nach unterschiedlichen Arten von Sicherheitsrisiken zusammengefasst. Trend Micro empfiehlt die Verwendung von ActiveAction, wenn Sie nicht genau wissen, welche Suchaktion sich für einen bestimmten Typ von Sicherheitsrisiko am besten eignet. Die ActiveAction-Einstellungen werden in den Pattern-Dateien ständig aktualisiert, um Endpunkte gegen die neuesten Sicherheitsrisiken und Angriffsmethoden zu schützen.
Die gleiche Aktion für alle Typen von Sicherheitsrisiken verwenden	Wählen Sie diese Option, wenn dieselbe Aktion für alle Typen von Sicherheitsrisiken außer für wahrscheinliche Viren/Malware durchgeführt werden soll. Beim Typ „Wahrscheinlich Virus/ Malware“ erfolgt stets die Aktion „Übergehen“. Wenn Sie „Säubern“ als erste Aktion auswählen, geben Sie eine Ersatzaktion an, die Apex One (Mac) durchführt, falls das Säubern fehlschlägt. Nur wenn die erste Aktion „Säubern“ ist, ist eine zweite Aktion einstellbar. Details zu den Suchoptionen finden Sie unter *Suchaktionen auf Seite 6-27*.

2. Unter **Zeitgesteuerte Suche – Berechtigungen** angeben, ob Benutzer eine zeitgesteuerte Suche verschieben oder überspringen können.

Berechtigung	Beschreibung
Zeitgesteuerte Suche verschieben	Benutzer mit der Berechtigung "Zeitgesteuerte Suche verschieben" können die folgenden Aktionen durchführen: • Zeitgesteuerte Suche verschieben, bevor diese durchgeführt wird, und anschließend die Dauer der Verschiebung festlegen. Die zeitgesteuerte Suche kann nur einmal verschoben werden. • Wenn die zeitgesteuerte Suche gerade durchgeführt wird, können Benutzer die Suche beenden und später neu starten. Der Benutzer legt anschließend fest, nach wie viel Minuten die Suche erneut durchgeführt werden soll. Wenn die Suche erneut durchgeführt wird, werden alle bereits durchsuchten Dateien nochmal durchsucht. Die zeitgesteuerte Suche kann nur einmal beendet und neu gestartet werden. Der Benutzer kann die Anzahl der Stunden und Minuten für folgende Einstellungen angeben: • die maximale Dauer der Verschiebung • die maximalen Zeit, die bis zum Neustart der Suche verstreichen soll
Zeitgesteuerte Suche überspringen und beenden	Mit dieser Berechtigung darf ein Benutzer folgende Aktionen durchführen: • Zeitgesteuerte Suche überspringen, bevor diese durchgeführt wird • Zeitgesteuerte Suche beenden, wenn diese gerade durchgeführt wird

3. Unter **Einstellungen für die zeitgesteuerte Suche** die Benachrichtigungs- und Akkuleistungseinstellungen festlegen.

Einstellung	Beschreibung
Vor Beginn der zeitgesteuerten Suche Benachrichtigung anzeigen	Wenn Sie diese Option aktivieren, wird einige Minuten vor Beginn der zeitgesteuerten Suche eine Benachrichtigung auf dem betreffenden Endpunkt angezeigt. Darin erhalten die Benutzer Auskunft über den Zeitplan (Datum und Uhrzeit) und ihre Berechtigungen im Zusammenhang mit der zeitgesteuerten Suche, etwa ob sie das Recht haben, sie zu verschieben, zu überspringen oder anzuhalten. Sie können die Dauer der Anzeige der Benachrichtigung in Minuten festlegen.
Zeitgesteuerte Suche automatisch anhalten, wenn Suche länger als __ Stunden und __ Minuten dauert	Der Security Agent beendet die Suche automatisch, wenn die festgelegte Zeit überschritten wurde und die Suche noch nicht abgeschlossen ist. Bei der Suche benachrichtigt der Security Agent die Benutzer sofort über die entdeckten Sicherheitsrisiken.
Zeitgesteuerte Suche überspringen, wenn die Akkulaufzeit eines Wireless-Endpunkts weniger als __ % beträgt und der AC-Adapter nicht angeschlossen ist	Apex One (Mac) überspringt eine zeitgesteuerte Suche, wenn festgestellt wird, dass die Akkulebensdauer eines drahtlosen Endpunkts niedrig und das Netzteil nicht angeschlossen ist. Wenn die Akkulebensdauer niedrig ist, aber das Netzteil angeschlossen ist, wird die Suche fortgesetzt. Wenn eine Suche ausgeführt wird und die Akkulebensdauer niedrig ist, wird die Suche nicht beendet.

Jetzt durchsuchen

"Jetzt durchsuchen" wird per Fernzugriff durch einen Administrator für Trend Micro Apex One (Mac) über die Webkonsole gestartet und kann auf einem oder mehreren Endpunkten ausgeführt werden.

Starten Sie "Jetzt durchsuchen" auf Endpunkten, bei denen Sie eine Vireninfektion vermuten.

Jetzt durchsuchen starten

Vorbereitungen

Alle Einstellungen der Zeitgesteuerten Suche, mit Ausnahme des tatsächlichen Zeitplans, werden während DURCHSUCHEN Jetzt verwendet.

Um die Einstellungen vor dem Start von DURCHSUCHEN Jetzt zu konfigurieren, folgen Sie den Schritten in *Einstellungen für zeitgesteuerte Suche konfigurieren auf Seite 6-20*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon (), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Aufgaben** > **Jetzt durchsuchen**.

Unterstützte komprimierte Dateitypen

Apex One (Mac) unterstützt die folgenden Komprimierungstypen.

Erweiterung	Typ
.zip	Mit Pkzip erstelltes Archiv
.rar	Mit RAR erstelltes Archiv
.tar	Mit Tar erstelltes Archiv
.arj	ARJ-komprimiertes Archiv
.hqx	BINHEX
.gz; .gzip	Gnu ZIP
.Z	LZW/16-Bit-komprimiert
.bin	MacBinary
.cab	Microsoft Kabinettdatei
Microsoft-komprimiert/MSCOMP	
.eml; .mht	MIME
.td0	Teledisk Format

Erweiterung	Typ
.bz2	Mit Unix BZ2 Bzip komprimierte Datei
.uu	UUEncode
.ace	WinAce

Suchaktionen

Geben Sie die Aktionen an, die Apex One (Mac) durchführt, wenn ein bestimmter Suchtyp ein Sicherheitsrisiko erkennt.

Die Aktion, die von Apex One (Mac) ausgeführt wird, ist abhängig vom Suchtyp, der das Sicherheitsrisiko erkannt hat. Wenn beispielsweise bei der manuellen Suche (Suchtyp) ein Sicherheitsrisiko von Apex One (Mac) erkannt wird, wird die infizierte Datei gesäubert (Aktion).

Apex One (Mac) kann die folgenden Aktionen bei Sicherheitsrisiken durchführen:

Suchaktion	Details
Löschen	Apex One (Mac) entfernt die infizierte Datei vom Endpunkt.
Quarantäne	Die infizierte Datei wird von Apex One (Mac) umbenannt und in das Quarantäneverzeichnis des Endpunkts `<Agent installation folder>/common/lib/vsapi/quarantine` verschoben. Nachdem die Datei in das Quarantäneverzeichnis verschoben wurde, kann Apex One (Mac) weitere Aktionen für diese Datei durchführen, je nachdem, welche Aktion vom Benutzer angegeben wurde. Apex One (Mac) kann die Datei säubern, löschen oder wiederherstellen. Die Datei wiederherzustellen bedeutet, dass sie an ihren ursprünglichen Speicherort zurückverschoben wird, ohne dass irgendeine Aktion ausgeführt wird. Benutzer können eine Datei wiederherstellen, wenn sie sich als unbedenklich herausstellt. Eine Datei zu säubern bedeutet, dass das Sicherheitsrisiko von der Datei in der Quarantäne entfernt wird und sie nach erfolgreicher Säuberung an ihren ursprünglichen Speicherort zurückverschoben wird.

Suchaktion	Details
Säubern	Apex One (Mac) entfernt das Sicherheitsrisiko aus einer infizierten Datei und ermöglicht dann erst den Zugriff darauf. Lässt sich die Datei nicht säubern, führt Apex One (Mac) zusätzlich eine der folgenden Aktionen aus: Quarantäne, Löschen oder Übergehen. Zum Konfigurieren der zweiten Aktion navigieren Sie zu **Agent-Verwaltung** > **Einstellungen** > **{Suchtyp}**, und klicken Sie auf die Registerkarte **Aktion**.
Übergehen	Apex One (Mac) führt keine Aktion für die infizierte Datei aus. Das erkannte Sicherheitsrisiko wird jedoch in den Protokolldateien verzeichnet. Die Datei wird nicht verschoben. Apex One (Mac) führt bei Dateien mit Infektionen des Typs „Wahrscheinlich Virus/Malware“ stets die Aktion „Übergehen“ aus, um das Risiko von Fehlalarmen zu verringern. Wenn weitere Analysen bestätigen, dass Viren/Malware wahrscheinlich tatsächlich ein Sicherheitsrisiko darstellen, wird ein neues Pattern veröffentlicht, damit Apex One (Mac) die entsprechende Suchaktion durchführen kann. Wenn sich wahrscheinliche Viren/Malware als unbedenklich herausstellen, werden diese nicht mehr entdeckt. Beispiel: Apex One (Mac) entdeckt „x_wahrscheinlicher_Virus“ in einer Datei „123.pdf“ und führt bei Fund keine Aktion durch. Trend Micro bestätigt anschließend, dass „x_wahrscheinlicher_Virus“ ein Trojaner ist und veröffentlicht eine neue Version des Viren-Patterns. Nach dem Laden der neuen Pattern-Version erkennt Apex One (Mac) „x_wahrscheinlicher_Virus“ als Trojaner und löscht „123.pdf“, wenn für diese Dateien die Aktion „Löschen“ festgelegt wurde. **Hinweis** Diese Aktion ist für die Echtzeitsuche nicht verfügbar.
Zugriff verweigern	Beim Versuch, eine Infizierte Datei zu öffnen oder auszuführen, wird dieser Vorgang durch Apex One (Mac) sofort gesperrt. Die infizierte Datei kann manuell gelöscht werden.

Suchausschlüsse

Konfigurieren Sie die Suchausschlüsse, um die Suchleistung zu verbessern und bekannte Dateien zu überspringen, die keinen Schaden anrichten können. Während ein bestimmter Suchtyp ausgeführt wird, überprüft Apex

One (Mac) die Ausschlussliste, um die Dateien auf dem Endpunkt zu bestimmen, die von der Suche ausgeschlossen werden.

Ausschlussliste	Details
Dateien	Apex One (Mac) durchsucht in folgenden Fällen keine Datei: • die Datei sich im Verzeichnispfad befindet, der in der Ausschlussliste angegeben ist • die Datei dem vollständigen Dateipfad (Verzeichnispfad und Dateiname) entspricht, der in der Ausschlussliste angegeben ist
Dateierweiterungen	Apex One (Mac) durchsucht eine Datei nicht, wenn ihre Erweiterung einer der Erweiterungen in der Ausschlussliste entspricht.

Ausschlusslisten für die Suche konfigurieren

Weitere Informationen zu Suchausschlusslisten finden Sie unter *Suchausschlüsse auf Seite 6-28*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon (), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für den Suchausschluss**.
4. Aktivieren Sie das Kontrollkästchen, um den Suchausschluss zu aktivieren.
5. Um die **Ausschlussliste für Virensuche (Dateien)** zu konfigurieren:
   a. Geben Sie einen vollständigen Dateipfad oder einen Verzeichnispfad ein und klicken Sie auf **Hinzufügen**.

      Erinnerung:

      - Die Eingabe nur eines Dateinamens ist nicht zulässig.
      - Es können maximal 64 Pfade angegeben werden. Beispiele erhalten Sie in der folgenden Tabelle.

Pfad	Details	Beispiele

Vollständiger Dateipfad	Schließt eine bestimmte Datei auf dem Endpunkt aus.	• Beispiel 1:
		`/file.log`
		• Beispiel 2:
		`/System/file.log`

Verzeichnispfad	Schließt alle Dateien in einem bestimmten Ordner und dessen Unterordnern aus.	• Beispiel 1:
		`/System/`
		Beispiele für aus Suchvorgängen ausgeschlossene Dateien:
		• `/System/file.log`
		• `/System/Library/file.log`
		Beispiele für Dateien, die durchsucht werden:
		• `/Applications/file.log`
		• Beispiel 2:
		`/System/Library`
		Beispiele für aus Suchvorgängen ausgeschlossene Dateien:
		• `/System/Library/file.log`
		• `/System/Library/Filters/file.log`
		Beispiele für Dateien, die durchsucht werden:
		• `/System/file.log`

- Sie können statt Ordnernamen auch ein Sternchen (*) als Platzhalterzeichen verwenden.

  Beispiele erhalten Sie in der folgenden Tabelle.

Pfad	Beispiele für die Verwendung von Platzhalterzeichen
Vollständiger Dateipfad	`/Users/Mac/*/file.log` Beispiele für aus Suchvorgängen ausgeschlossene Dateien: • `/Users/Mac/Desktop/file.log` • `/Users/Mac/Movies/file.log` Beispiele für Dateien, die durchsucht werden: • `/Users/file.log` • `/Users/Mac/file.log`

Verzeichnispfad	• Beispiel 1:
	`/Users/Mac/*`
	Beispiele für aus Suchvorgängen ausgeschlossene Dateien:
	• `/Users/Mac/doc.html`
	• `/Users/Mac/Documents/doc.html`
	• `/Users/Mac/Documents/Pics/pic.jpg`
	Beispiele für Dateien, die durchsucht werden:
	• `/Users/doc.html`
	• Beispiel 2:
	`/*/Components`
	Beispiele für aus Suchvorgängen ausgeschlossene Dateien:
	• `/Users/Components/file.log`
	• `/System/Components/file.log`
	Beispiele für Dateien, die durchsucht werden:
	• `/file.log`
	• `/Users/file.log`
	• `/System/Files/file.log`

- Teilweise Übereinstimmungen mit Ordnernamen sind nicht zulässig. So ist es beispielsweise nicht möglich, durch Eingabe von `/Users/*user/temp` auch Dateien in Ordnern auszuschließen, deren Namen auf „Benutzer“ enden, etwa „Endbenutzer“ oder „neuer_benutzer“.

b. Wählen Sie zum Löschen eines Pfads den Pfad aus, und klicken Sie auf **Entfernen**.

6. Um die **Ausschlussliste für Virensuche (Dateierweiterungen)** zu konfigurieren:

a. Geben Sie eine Dateierweiterung ohne Punkt (.) ein und klicken Sie auf **Hinzufügen**. Geben Sie z. B. `pdf` ein. Es können maximal 64 Dateierweiterungen angegeben werden.

b. Um eine Erweiterung zu löschen, wählen Sie sie aus und klicken auf **Entfernen**.

7. Wenn Sie eine oder mehrere Gruppen oder Security Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die Gruppen oder Security Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:

- **Für alle Agenten übernehmen**: Wendet die Einstellungen auf alle vorhandenen Security Agents und auf alle neuen Security Agent an, die einer vorhandenen/zukünftigen Gruppe hinzugefügt werden. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden sind.
- **Nur auf zukünftige Gruppen anwenden**: Wendet die Einstellungen nur auf Security Agents an, die zukünftigen Gruppen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf Security Agents angewendet, die einer vorhandenen Gruppe hinzugefügt werden.

Cache-Einstellungen für die Suche

Bei jeder Suche prüft der Security Agent den Zwischenspeicher für geänderte Dateien, um zu ermitteln, ob eine Datei seit dem letzten Start des Agent geändert wurde.

- Wenn eine Datei geändert wurde, durchsucht das Security Agent die Datei und fügt sie dem Cache der durchsuchten Dateien hinzu.
- Wenn eine Datei nicht geändert wurde, überprüft Security Agent, ob die Datei im Cache der gescannten Dateien ist.
  - Wenn die Datei im Cache der gescannten Dateien ist, überspringt der Security Agent das Scannen der Datei.
  - Wenn die Datei nicht im Cache der gescannten Dateien ist, überprüft der Security Agent den Cache der genehmigten Dateien.

Hinweis

Der Zwischenspeicher für genehmigte Dateien enthält alle Dateien, die von Trend Micro Apex One (Mac) für vertrauenswürdig befunden werden. Vertrauenswürdige Dateien sind entweder Dateien, die von aufeinanderfolgenden Versionen des Pattern durchsucht und jedes Mal für frei von Bedrohungen befunden wurden, oder bedrohungsfreie Dateien, die seit längerem nicht mehr geändert wurden.

  - Wenn sich die Datei im Cache der genehmigten Dateien befindet, überspringt Security Agent das Scannen der Datei.
  - Ist dies nicht der Fall, durchsucht der Security Agent die Datei und fügt Sie dem Zwischenspeicher für durchsuchte Dateien hinzu.

Bei jeder Aktualisierung der Such-Engine bzw. des Such-Pattern werden alle oder zumindest einige der Zwischenspeicher geleert.

Wenn Suchvorgänge häufig ausgeführt werden und sich bereits viele Dateien in den Zwischenspeichern befinden, reduziert sich die Suchzeit erheblich.

Wenn Sie die Suche nur selten ausführen, deaktivieren Sie die Zwischenspeicher, so dass bei jeder Suche alle Dateien auf Bedrohungen durchsucht werden können.

Zwischenspeicher-Einstellungen für Suchen konfigurieren

Details zum Zwischenspeicher der On-Demand-Suche finden Sie unter *Cache-Einstellungen für die Suche auf Seite 6-33*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon ( ), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Einstellungen** > **Zwischenspeicher-Einstellungen für Suchen**.
4. Wählen Sie **Cache für die bedarfsgesteuerte Suche aktivieren**.
5. Wenn Sie eine oder mehrere Gruppen oder Security Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die Gruppen oder Security Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:
   - **Für alle Agenten übernehmen**: Wendet die Einstellungen auf alle vorhandenen Security Agents und auf alle neuen Security Agent an, die einer vorhandenen/zukünftigen Gruppe hinzugefügt werden. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden sind.
   - **Nur auf zukünftige Gruppen anwenden**: Wendet die Einstellungen nur auf Security Agents an, die zukünftigen Gruppen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf Security Agents angewendet, die einer vorhandenen Gruppe hinzugefügt werden.

Ausnahmelisten

Sie können den Bildschirm Ausnahmelisten verwenden, um Security Agents so zu konfigurieren, dass die Suche überspringen von vertrauenswürdigen Prozessen erfolgt und Erkennungen bestimmter Regeln ausgeschlossen werden.

- **Regelausnahmen**: Geben Sie an, welche Erkennungen mithilfe der Regel-ID ausgeschlossen werden sollen. Sie finden Regel-IDs auf dem Bildschirm für Abfrageprotokolle.
- **Liste der vertrauenswürdigen Programme**: Vertrauenswürdige Programme angeben, die bei der Durchführung von Scans übersprungen werden sollen. Für weitere Informationen siehe *Liste der vertrauenswürdigen Programme konfigurieren auf Seite 6-35*.

Liste der vertrauenswürdigen Programme konfigurieren

Die Liste der vertrauenswürdigen Programme schließt Programme und alle untergeordneten Prozesse aus, die über die Echtzeitsuche vom Programm aufgerufen werden.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon ( ), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Einstellungen** > **Liste der vertrauenswürdigen Programme**.
4. Geben Sie den vollständigen Programmpfad für das Programm an, das von der Liste ausgeschlossen werden soll.
5. Klicken Sie auf **+ Hinzufügen**.
6. Um ein Programm aus der Liste zu entfernen, klicken Sie auf das Symbol **Delete**.

7. Um die Liste der vertrauenswürdigen Programme zu exportieren, klicken Sie auf **Exportieren** und wählen Sie einen Speicherort für die Datei aus.

Hinweis

Trend Micro Apex One (Mac) speichert die Liste im `DAT`-Format.

8. Um eine Liste der vertrauenswürdigen Programme zu importieren, klicken Sie auf **Importieren** und wählen Sie einen Speicherort für die Datei aus.

   a. Klicken Sie auf **Durchsuchen...** und wählen Sie den Speicherort für die `DAT`-Datei aus.

   b. Klicken Sie auf **Importieren**.

9. Wenn Sie eine oder mehrere Gruppen oder Security Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die Gruppen oder Security Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:

   - **Für alle Agenten übernehmen**: Wendet die Einstellungen auf alle vorhandenen Security Agents und auf alle neuen Security Agent an, die einer vorhandenen/zukünftigen Gruppe hinzugefügt werden. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden sind.
   - **Nur auf zukünftige Gruppen anwenden**: Wendet die Einstellungen nur auf Security Agents an, die zukünftigen Gruppen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf Security Agents angewendet, die einer vorhandenen Gruppe hinzugefügt werden.

Protokolle zu Suchvorgängen anzeigen

Wenn die manuelle oder zeitgesteuerte Suche ausgeführt wird, erstellt der Trend Micro Apex One (Mac)Security Agent ein Suchprotokoll mit

Informationen über die Suche. Sie können über die Trend Micro Apex One (Mac) Server- oder Agent-Konsole das Suchprotokoll anzeigen.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon (), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Protokolle** > **Protokolle zu Suchvorgängen**.
4. Legen Sie die Protokollkriterien fest, und klicken Sie auf **Protokolle anzeigen**.

   Das Fenster **Protokolle zu Suchvorgängen** wird angezeigt.
5. Wenn Sie das Protokoll als komma-separierte Datei im CSV-Format speichern möchten, klicken Sie auf **Exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Nächste Schritte

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell oder nach einem festgelegten Zeitplan. Weitere Informationen zur Verwaltung von Protokollen finden Sie unter *Protokolle verwalten auf Seite 9-8*.

Benachrichtigungen und Protokolle für Sicherheitsrisiken

Trend Micro Apex One (Mac) umfasst zahlreiche Standardbenachrichtigungen, die Sie und andere Administratoren für Trend Micro Apex One (Mac) erhalten, wenn Sicherheitsrisiken oder Virenausbrüche erkannt werden.

Trend Micro Apex One (Mac) erstellt Protokolldateien, wenn Sicherheitsrisiken entdeckt werden.

Einstellungen der Administratorbenachrichtigungen konfigurieren

Wenn Sicherheitsrisiken erkannt werden oder ein Ausbruch auftritt, erhalten Administratoren für Trend Micro Apex One (Mac) eine Benachrichtigung per E-Mail.

Prozedur

1. Gehen Sie zu **Benachrichtigungen** > **Allgemeine Einstellungen**.
2. Geben Sie im Feld **SMTP-Server** eine IPv4- bzw. IPv6-Adresse oder den Namen eines Endpunkts ein.
3. Geben Sie eine Portnummer zwischen 1 und 65535 ein.
4. Geben Sie im Feld **Von** die E-Mail-Adresse des Absenders ein.
5. Klicken Sie auf **Save**.

Benachrichtigungen bei Sicherheitsrisiken für Administratoren konfigurieren

Sie können Trend Micro Apex One (Mac) so konfigurieren, dass entweder bei jedem entdeckten Sicherheitsrisiko eine Benachrichtigung gesendet werden soll oder nur dann, wenn die Aktion für das entdeckte Sicherheitsrisiko fehlschlägt und Ihr Eingreifen erfordert.

Sie können sich Benachrichtigungen per E-Mail zusenden lassen. Konfigurieren Sie die Einstellungen der Administratorbenachrichtigungen so, dass Trend Micro Apex One (Mac) Benachrichtigungen per E-Mail versenden kann.

Prozedur

1. Navigieren Sie zu **Benachrichtigungen** > **Standardbenachrichtigungen**.
2. Geben Sie auf der Registerkarte **Kriterien** an, ob Benachrichtigungen jedes Mal gesendet werden sollen, wenn Trend Micro Apex One (Mac) ein Sicherheitsrisiko entdeckt wird, oder nur dann, wenn die Aktion an den Sicherheitsrisiken fehlschlägt.

3. Klicken Sie auf **Save**.
4. Auf der Registerkarte **E-Mail**:
   a. Aktivieren Sie das Versenden von Benachrichtigungen per E-Mail.
   b. Geben Sie die die E-Mail-Empfänger an, und akzeptieren oder ändern Sie den Standardbetreff.

      Daten im Feld **Nachricht** werden mit Hilfe von Token-Variablen dargestellt.

Variable	Beschreibung
%v	Name des Sicherheitsrisikos
%s	Der Endpunkt, auf dem das Sicherheitsrisiko erkannt wurde
%m	Agent-Gruppenname
%ii	IP-Adresse des Endpunkts
%nm	MAC-Adresse des Endpunkts
%p	Fundort des Sicherheitsrisikos
%y	Datum und Uhrzeit der Erkennung
%a	Durchgeführte Suchaktion

5. Klicken Sie auf **Save**.

Ausbruchsbenachrichtigungen für Administratoren konfigurieren

Ausbrüche werden auf Grundlage der Anzahl von Sicherheitsrisiken definiert, die in einem bestimmten Zeitraum entdeckt wurden. Nach Festlegung der Ausbruchskriterien konfigurieren Sie Trend Micro Apex One (Mac) so, dass Sie und andere Administratoren für Trend Micro Apex One (Mac) bei einem Ausbruch benachrichtigt werden, um sofort eingreifen zu können.

Sie können sich Benachrichtigungen per E-Mail zusenden lassen. Konfigurieren Sie die Einstellungen der Administratorbenachrichtigungen so, dass Trend Micro Apex One (Mac) Benachrichtigungen per E-Mail versenden kann. Weitere Informationen finden Sie unter *Einstellungen der Administratorbenachrichtigungen konfigurieren auf Seite 6-38*.

Prozedur

1. Gehen Sie zu **Benachrichtigungen** > **Ausbruchsbenachrichtigungen**.
2. Geben Sie auf der Registerkarte **Kriterien** Folgendes an:
   - Anzahl der eindeutigen Quellen von Sicherheitsrisiken
   - Anzahl der Funde
   - Entdeckungszeitraum

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

   Trend Micro Apex One (Mac) löst einen Ausbruchalarm aus und sendet eine Benachrichtigung, wenn die festgelegte Anzahl von Entdeckungen überschritten wird. Wenn Sie z. B. 10 eindeutige Quellen, 100 Erkennungen und einen Zeitraum von 5 Stunden angeben, sendet Trend Micro Apex One (Mac) die Benachrichtigung, wenn 10 verschiedene Security Agents insgesamt 101 Sicherheitsrisiken innerhalb eines Zeitraums von 5 Stunden gemeldet haben. Werden alle Vorfälle über einen Zeitraum von 5 Stunden auf nur einem Security Agent entdeckt, sendet Trend Micro Apex One (Mac) keine Benachrichtigung.
3. Klicken Sie auf **Speichern**.
4. Auf der Registerkarte **E-Mail**:
   a. Aktivieren Sie das Versenden von Benachrichtigungen per E-Mail.
   b. Geben Sie die die E-Mail-Empfänger an, und akzeptieren oder ändern Sie den Standardbetreff.

Daten im Feld **Nachricht** werden mit Hilfe von Token-Variablen dargestellt.

Variable	Beschreibung
%CV	Gesamtzahl aller entdeckten Sicherheitsrisiken
%CC	Gesamtzahl aller Endpunkte mit Sicherheitsrisiken

5. Wählen Sie die zusätzlichen Informationen aus, die in der E-Mail enthalten sein sollen. Es können Security Agent oder Gruppenname, Name des Sicherheitsrisikos, Pfad und infizierte Datei, Datum und Uhrzeit der Entdeckung und das Suchergebnis ausgewählt werden.
6. Klicken Sie auf **Speichern**.

Sicherheitsrisiko-Protokolle anzeigen

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon (), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Protokolle** > **Sicherheitsrisiko-Protokolle**.
4. Legen Sie die Protokollkriterien fest, und klicken Sie auf **Protokolle anzeigen**.
5. Sehen Sie die Protokolle ein. Protokolle enthalten die folgenden Informationen:
   - Datum und Uhrzeit des Fundes des Sicherheitsrisikos
   - Endpunkt mit Sicherheitsrisiko
   - Name des Sicherheitsrisikos
   - Quelle des Sicherheitsrisikos

- Suchtyp, der das Sicherheitsrisiko entdeckt hat
- Suchergebnisse, die angeben, ob Suchaktionen erfolgreich ausgeführt wurden; Details zu den Suchergebnissen finden Sie unter *Suchergebnis auf Seite 6-42*.
- Plattform

6. Wenn Sie das Protokoll als komma-separierte Datei im CSV-Format speichern möchten, klicken Sie auf **Exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Hinweis

Falls Sie eine große Anzahl an Protokollen exportieren, warten Sie bis der Export abgeschlossen ist. Wenn Sie die Seite schließen, bevor der Export abgeschlossen ist, wird die CSV-Datei nicht erzeugt.

Nächste Schritte

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell oder nach einem festgelegten Zeitplan. Weitere Informationen zur Verwaltung von Protokollen finden Sie unter *Protokolle verwalten auf Seite 9-8*.

Suchergebnis

In den Viren-/Malware-Protokollen werden die folgenden Suchergebnisse angezeigt:

- **Gelöscht**
  - Die erste Aktion ist Löschen, und die infizierte Datei wurde gelöscht.
  - Die erste Aktion ist Säubern, aber die Säuberung ist fehlgeschlagen. Die zweite Aktion ist Löschen, und die infizierte Datei wurde gelöscht.
- **In Quarantäne verschoben**

  - Die erste Aktion ist Quarantäne, und die infizierte Datei wurde in die Quarantäne verschoben.
  - Die erste Aktion ist Säubern, aber die Säuberung ist fehlgeschlagen. Die zweite Aktion ist Quarantäne, und die infizierte Datei wurde in die Quarantäne verschoben.

- **Gesäubert**

  Eine infizierte Datei wurde gesäubert.

- **Übergangen**

  - Die erste Aktion ist Übergehen. Trend Micro Apex One (Mac) hat keine Aktion an der infizierten Datei durchgeführt.
  - Die erste Aktion ist Säubern, aber die Säuberung ist fehlgeschlagen. Die zweite Aktion ist Übergehen, und Trend Micro Apex One (Mac) hat demnach keine Aktion an der infizierten Datei durchgeführt.

- **Datei konnte nicht gesäubert oder in Quarantäne verschoben werden**

  Die erste Aktion ist Säubern. Die zweite Aktion ist Quarantäne, und beide Aktionen sind fehlgeschlagen.

  Lösung: Weitere Informationen finden Sie unter „Datei konnte nicht in Quarantäne verschoben werden“ weiter unten.

- **Datei konnte nicht gesäubert oder gelöscht werden**

  Die erste Aktion ist Säubern. Die zweite Aktion ist Löschen, und beide Aktionen sind fehlgeschlagen.

  Lösung: Weitere Informationen finden Sie unter „Datei konnte nicht gelöscht werden“ weiter unten.

- **Datei konnte nicht in Quarantäne verschoben werden**

  Die infizierte Datei wird möglicherweise von einer anderen Anwendung gesperrt, gerade ausgeführt oder befindet sich auf einer CD. Trend Micro Apex One (Mac) verschiebt die Datei in Quarantäne, nachdem sie wieder verfügbar ist oder ausgeführt wurde.

  Lösung

Bei infizierten Dateien auf einer CD empfiehlt es sich, die CD nicht zu verwenden, da der Virus auf andere Endpunkte im Netzwerk übertragen werden könnte.

- **Datei konnte nicht gelöscht werden**

  Die infizierte Datei wird möglicherweise von einer anderen Anwendung gesperrt, gerade ausgeführt oder befindet sich auf einer CD. Trend Micro Apex One (Mac) löscht die Datei, nachdem sie wieder verfügbar ist oder ausgeführt wurde.

  Lösung

  Bei infizierten Dateien auf einer CD empfiehlt es sich, die CD nicht zu verwenden, da der Virus auf andere Endpunkte im Netzwerk übertragen werden könnte.

- **Die Datei konnte nicht gesäubert werden**

  Die Säuberung der Datei ist möglicherweise nicht durchführbar. Weitere Informationen finden Sie unter *Dateien, die nicht gesäubert werden können auf Seite 6-44*.

Dateien, die nicht gesäubert werden können

Die Viren-Scan-Engine kann folgende Dateien nicht säubern:

Nicht zu säubernde Datei	Erklärung und Lösung
Mit Würmern infizierte Dateien	Ein Computerwurm ist ein eigenständiges Programm (oder eine Gruppe von Programmen), das funktionsfähige Kopien von sich selbst oder seinen Segmenten an andere Endpunktsysteme verteilen kann. Würmer verbreiten sich normalerweise über Netzwerkverbindungen oder E-Mail-Anhänge. Würmer sind eigenständige Programme und können deshalb nicht gesäubert werden. **Lösung**: Trend Micro empfiehlt, Würmer zu löschen.
Infizierte, schreibgeschützte Dateien	**Lösung**: Heben Sie den Schreibschutz auf, damit der Security Agent die Datei säubern kann.

Nicht zu säubernde Datei	Erklärung und Lösung
Kennwortgeschützte Dateien	Schließt kennwortgeschützte Dateien und komprimierte Dateien ein. **Lösung**: Heben Sie den Kennwortschutz für Security Agent auf, damit diese Dateien gesäubert werden können.
Sicherungsdateien	Bei Dateien mit den Erweiterungen RB0~RB9 handelt es sich um Sicherungskopien infizierter Dateien. Der Security Agent erstellt eine Sicherungskopie der infizierten Datei, für den Fall, dass der Virus bzw. die Malware die Datei während des Säuberungsvorgangs beschädigt hat. **Lösung**: Wenn die infizierte Datei von Security Agent gesäubert werden konnte, muss die Sicherungskopie nicht aufbewahrt werden. Wenn der Endpunkt fehlerfrei funktioniert, können Sie die Sicherungskopie löschen.

Zähler für Sicherheitsrisiken zurücksetzen

Sie können im Fenster **Statistik zurücksetzen** den Erkennungszähler für Sicherheitsrisiken auf Null zurücksetzen.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon (), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Protokolle** > **Statistik zurücksetzen**.

   Hinweis

   Das Feld **Sicherheitsrisiko** zeigt die Gesamtanzahl der Erkennungen für das ausgewählte Security Agents, alle Security Agents in den ausgewählten Gruppen oder alle Security Agents an.

4. Klicken Sie auf **Zurücksetzen**.

5. Klicken Sie auf **OK**.

Kapitel 7

Endpunkte vor webbasierten Angriffen schützen

In diesem Kapitel werden webbasierte Bedrohungen und die damit verbundenen Schutzfunktionen in Trend Micro Apex One (Mac) für Netzwerke und Endpunkte beschrieben.

Internet-Bedrohungen

Als Internet-Bedrohungen zählen vielfältige Sicherheitsrisiken, die ihren Ursprung im Internet haben. Sie setzen auf raffinierte Methoden und kombinierte Dateien und Techniken anstelle isolierter Infektionswege. Beispielsweise ändern die Urheber von Internet-Bedrohungen regelmäßig die Version oder die verwendete Variante. Da sich die Internetbedrohung eher an einem festen Speicherort auf einer Website und nicht auf einem infizierten Computer befindet, wird der Code ständig verändert, um einer Entdeckung zu entgehen.

Personen, die in der Vergangenheit als Hacker, Virenautoren, Spammer und Spyware-Hersteller bezeichnet wurden, werden seit einigen Jahren unter der Bezeichnung Cyberkriminelle zusammengefasst. Internet-Bedrohungen helfen diesen Personen eines von zwei Zielen zu verfolgen. Eines dieser Ziele ist es, Informationen zu stehlen, um sie anschließend zu verkaufen. Das Ergebnis ist die Preisgabe vertraulicher Informationen in Form von Identitätsverlust. Infizierte Endpunkte können außerdem als Überträger für Phishing-Angriffe eingesetzt oder anderweitig zur Informationsbeschaffung missbraucht werden. Unter anderem hat diese Bedrohung das Potenzial, das Misstrauen gegenüber E-Commerce zu verstärken und so das für Transaktionen im Internet notwendige Vertrauen zu zerstören. Das zweite Ziel ist die Nutzung der Rechenleistung eines fremden Computers für profitorientierte Aktivitäten. Solche Aktivitäten können das Versenden von Spam, Erpressungsversuche in Form verteilter Denial-of-Service-Attacken oder Pay-per-Click-Aktivitäten sein.

Web Reputation

Die Web-Reputation-Technologie bewertet die Glaubwürdigkeit von Webdomänen nach einem Scoring-Verfahren, indem Informationen wie das Alter einer Website, historische Änderungen des Speicherorts und Anzeichen von verdächtigen Aktivitäten zurückverfolgt werden, die durch die Malware-Verhaltensanalyse entdeckt wurden. Anschließend werden Websites durchsucht und Benutzer vom Zugriff auf infizierte Websites abgehalten.

Security Agents senden Anfragen an die Smart Protection Quellen, um die Reputation von Websites, auf die ein Benutzer zugreifen möchte, zu

überprüfen. Die Reputation einer Website wird mit einer spezifischen, auf dem jeweiligen Endpunkt gültigen Web-Reputation-Richtlinie abgeglichen. Die jeweils angewendete Richtlinie bestimmt, ob Security Agents den Zugriff auf eine Website zulässt oder sperrt.

Hinweis

Diese Funktion unterstützt die neuesten Versionen von Safari™, Mozilla™, Firefox™ und Google Chrome™-Browsern.

Einstellungen für Web Reputation konfigurieren

Die Web Reputation-Einstellungen umfassen Richtlinien, die festlegen, ob Apex One (Mac) den Zugriff auf eine Website sperren oder erlauben wird. Um die geeignete Richtlinie zu bestimmen, überprüft Apex One (Mac) den Standort des Security Agent. Der Standort eines Security Agent ist "intern", wenn der Security Agent eine Verbindung zum Apex One (Mac) Server herstellen kann. Andernfalls ist der Standort für den Security Agent "extern".

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon (), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für Web Reputation**.
4. So konfigurieren Sie eine Richtlinie für externe Security Agents:
   a. Klicken Sie auf die Registerkarte **Externe Agenten**.
   b. Wählen Sie **Aktivieren Sie "Web Reputation-Richtlinie"**.

      Wenn die Richtlinie aktiviert ist, senden externe Security Agents Web-Reputation-Abfragen an das Smart Protection Network.

Hinweis

Wenn ein Security Agent ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Web Reputation-Abfragen in *Einschränkungen bei reinen IPv6-Agents auf Seite A-3*.

c. Wählen Sie unter den vorhandenen Web Reputation-Sicherheitsstufen aus: **Hoch**, **Mittel** oder **Niedrig**

Hinweis

Die Sicherheitsstufen legen fest, ob Apex One (Mac) den Zugriff auf eine URL zulässt oder sperrt. Wenn zum Beispiel die Sicherheitsstufe auf "Niedrig" festgelegt ist, sperrt Apex One (Mac) nur URLs, die als Internet-Bedrohungen bekannt sind. Bei einer Erhöhung der Sicherheitsstufe verbessert sich die Erkennungsrate von Internet-Bedrohungen, doch gleichzeitig steigt auch die Wahrscheinlichkeit von Fehlalarmen.

d. Um Web Reputation-Feedback anzugeben, klicken Sie auf die entsprechende URL. In einem Browserfenster wird das Web Reputation-Hilfesystem von Trend Micro geöffnet.

5. Um eine Richtlinie für interne Security Agents zu konfigurieren:

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

b. Wählen Sie **Aktivieren Sie "Web Reputation-Richtlinie"**.

Wenn die Richtlinie aktiviert ist, senden interne Security Agents Web Reputation-Abfragen an:

- Smart Protection Server, wenn die Option **Anfragen an Smart Protection Server senden** aktiviert ist.
- Smart Protection Network, wenn die Option **Anfragen an Smart Protection Server senden** deaktiviert ist.

Hinweis

Wenn ein Security Agent ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Web Reputation-Abfragen in *Einschränkungen bei reinen IPv6-Agents auf Seite A-3*.

c. Wählen Sie **Anfragen an Smart Protection Server senden**, wenn Sie möchten, dass interne Security Agents Web Reputation-Abfragen an Smart Protection Server senden.

- Wenn Sie diese Option aktivieren, verweist Security Agents auf dieselbe Smart Protection-Quellenliste, die von Apex One Security Agents verwendet wird, um die Smart Protection Server zu bestimmen, an die Anfragen gesendet werden.

  Wichtig

  Lesen Sie vor dem Aktivieren dieser Option die Hinweise unter *Trend Micro Smart Protection auf Seite 3-17*.

- Wenn Sie diese Option deaktivieren, senden Security Agents Web Reputation-Abfragen an das Smart Protection Network. Für ein erfolgreiches Senden der Abfragen müssen die Endpunkte mit dem Internet verbunden sein.

d. Wählen Sie unter den vorhandenen Web Reputation-Sicherheitsstufen aus: **Hoch**, **Mittel** oder **Niedrig**

Hinweis

Die Sicherheitsstufen legen fest, ob Apex One (Mac) den Zugriff auf eine URL zulässt oder sperrt. Wenn zum Beispiel die Sicherheitsstufe auf "Niedrig" festgelegt ist, sperrt Apex One (Mac) nur URLs, die als Internet-Bedrohungen bekannt sind. Bei einer Erhöhung der Sicherheitsstufe verbessert sich die Erkennungsrate von Internet-Bedrohungen, doch gleichzeitig steigt auch die Wahrscheinlichkeit von Fehlalarmen.

Security Agents sperren Sie nicht getestete Websites nicht, unabhängig von der Sicherheitsstufe.

e. Um Web Reputation-Feedback anzugeben, klicken Sie auf die entsprechende URL. In einem Browserfenster wird das Web Reputation-Hilfesystem von Trend Micro geöffnet.

f. Wählen Sie, ob der Security Agents Web Reputation-Protokolle an den Server senden darf. Gestatten Sie Security Agents das Senden von Protokollen, wenn Sie die von Apex One (Mac) gesperrten URLs analysieren und bei als sicher eingestuften URLs eine entsprechende Aktion durchführen möchten.

6. Wenn Sie eine oder mehrere Gruppen oder Security Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die Gruppen oder Security Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:

- **Für alle Agenten übernehmen**: Wendet die Einstellungen auf alle vorhandenen Security Agents und auf alle neuen Security Agent an, die einer vorhandenen/zukünftigen Gruppe hinzugefügt werden. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden sind.
- **Nur auf zukünftige Gruppen anwenden**: Wendet die Einstellungen nur auf Security Agents an, die zukünftigen Gruppen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf

Security Agents angewendet, die einer vorhandenen Gruppe hinzugefügt werden.

Liste 'Zulässige/Gesperrte URL' konfigurieren

Fügen Sie Websites, die Sie als sicher bzw. gefährlich einstufen, zur Liste der zulässigen bzw. gesperrten URLs hinzu. Wenn Trend Micro Apex One (Mac) einen Zugriff auf eine dieser Websites erkennt, wird der Zugriff automatisch zugelassen bzw. gesperrt und es wird keine Abfrage an Smart Protection Quellen gesendet.

Prozedur

1. Navigieren Sie zu **Agents** > **Liste der zulässigen/gesperrten Web Reputation-URLs**.
2. Geben Sie eine URL in das Textfeld ein. Sie können an einer beliebigen Stelle der URL ein Platzhalterzeichen (*) einfügen.

   Beispiele:

   - `www.trendmicro.com/*` steht für alle Seiten der Domäne www.trendmicro.com.
   - `*.trendmicro.com/*` steht für alle Seiten auf allen Unterdomänen von trendmicro.com.

   Sie können auch URLs eingeben, die IP-Adressen enthalten. Bei URLs mit IPv6-Adressen müssen Sie diese zwischen eckige Klammern setzen.
3. Klicken Sie auf **Zur Liste der zulässigen URLs hinzufügen** oder **Zur Liste der gesperrten URLs hinzufügen**.
4. Um einen Einträge zu löschen, wählen Sie eine Option aus dem Listenfeld **Ansicht**, und klicken Sie auf das Symbol neben dem URL.
5. Klicken Sie auf **Save**.

Web Reputation-Protokolle anzeigen

Vorbereitungen

Sie können interne Security Agents so konfigurieren, dass sie Web Reputation-Protokolle an den Server senden. Dadurch können Sie die von Trend Micro Apex One (Mac) gesperrten URLs analysieren und bei URLs, die Sie als sicher einstufen, entsprechende Aktionen durchführen.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon ( ), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Protokolle** > **Web Reputation-Protokolle**.
4. Legen Sie die Protokollkriterien fest, und klicken Sie auf **Protokolle anzeigen**.
5. Sehen Sie die Protokolle ein. Protokolle enthalten die folgenden Informationen:
   - Datum/Uhrzeit der URL-Sperrung durch Trend Micro Apex One (Mac)
   - Endpunkt, dessen Benutzer auf die URL zugegriffen hat
   - Gesperrte URL
   - Risikostufe der URL
   - Link zum Trend Micro Web Reputation Hilfesystem, das weitere Informationen über die gesperrte URL enthält.
6. Wenn Sie Protokolle als komma-separierte Datei im `CSV`-Format speichern möchten, klicken Sie auf **Exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Hinweis

Falls Sie eine große Anzahl an Protokollen exportieren, warten Sie bis der Export abgeschlossen ist. Wenn Sie die Seite schließen, bevor der Export abgeschlossen ist, wird die CSV-Datei nicht erzeugt.

Nächste Schritte

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell oder nach einem festgelegten Zeitplan.

Weitere Informationen zur Verwaltung von Protokollen finden Sie unter *Protokolle verwalten auf Seite 9-8*.

Kapitel 8

Die Gerätesteuerung verwenden

In diesem Kapitel wird erläutert, wie Sie Endpunkte mit der Funktion "Gerätesteuerung" vor Sicherheitsrisiken schützen.

Gerätesteuerung

Die Gerätesteuerung reguliert den Zugriff auf externe Speichergeräte und Netzwerkressourcen, die mit Endpunkten verbunden sind. Die Gerätesteuerung trägt dazu bei, Datenverluste und Datenlecks zu verhindern und bietet, gemeinsam mit der Dateiprüfung, Schutz vor Sicherheitsrisiken.

Sie können Gerätesteuerungsrichtlinien für interne und externe Agents konfigurieren. In der Regel konfigurieren Administratoren eine strengere Richtlinie für externe Agents.

Richtlinien sind granulare Einstellungen im Agentenbaum. Sie können spezifische Richtlinien für Agentengruppen oder einzelne Security Agents durchsetzen. Sie können auch eine einzelne Richtlinie für alle Security Agents durchsetzen.

Berechtigungen für Speichergeräte

Gerätesteuerung-Berechtigungen für Speichergeräte werden verwendet, wenn Sie:

- Erlauben Sie den Zugriff auf USB-Speichergeräte, CD/DVD, SD-Karten, Netzwerklaufwerke und Thunderbolt SATA-Speichergeräte. Sie können den Zugriff auf diese Geräte entweder uneingeschränkt zulassen oder die Zugriffsstufe einschränken.
- Konfigurieren Sie die Liste der zulässigen USB-Speichergeräte. Mit der Gerätesteuerung können Sie den Zugriff auf alle USB-Speichergeräte sperren, mit Ausnahme der Geräte, die Sie in der Liste zulässiger Geräte hinzugefügt haben. Sie können den Zugriff auf die zulässigen Geräte entweder uneingeschränkt zulassen oder die Zugriffsstufe einschränken.

Die folgende Tabelle enthält eine Liste der Berechtigungen für Speichergeräte.

TABELLE 8-1. Gerätesteuerungsberechtigungen für Speichergeräte

BERECHTIGUNGEN	DATEIEN AUF DEM GERÄT	EINGEHENDE DATEIEN
Vollständiger Zugriff	Zulässige Aktionen: Kopieren, Verschieben, öffnen, Speichern, Löschen, Ausführen	Zulässige Aktionen: Speichern, Verschieben, Kopieren Das bedeutet, dass eine Datei kann auf dem Gerät gespeichert, verschoben und kopiert werden kann.
Nur lesen	Zulässige Aktionen: Kopieren, öffnen Unzulässige Aktionen: Speichern, Verschieben, Löschen, Ausführen	Unzulässige Aktionen: Speichern, Verschieben, Kopieren
Sperren	Unzulässige Aktionen: Alle Aktionen Das Gerät und die darin enthaltenen Dateien sind nicht für den Benutzer sichtbar (zum Beispiel über Finder).	Unzulässige Aktionen: Speichern, Verschieben, Kopieren

Hinweis

Die Nur-Lese-Berechtigung ist für Netzlaufwerke nicht verfügbar.

Einstellungen der Gerätesteuerung konfigurieren

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon (), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Einstellungen** > **Einstellungen der Gerätesteuerung**.

4. Klicken Sie auf die Registerkarte **Externe Agents**, um Einstellungen für externe Agents zu konfigurieren, oder auf die Registerkarte **Interne Agents**, um Einstellungen für interne Agents zu konfigurieren.
5. Wählen Sie **Gerätesteuerung aktivieren**.
6. Unter **Geräte** wählen Sie eine Berechtigung für jedes Speichermedium aus.

   Weitere Informationen zu Berechtigungen finden Sie unter *Berechtigungen für Speichergeräte auf Seite 8-2*.
7. (Optional) Wenn die Berechtigung für USB-Speichergeräte **Sperren** lautet, können Sie unter **USB-Speichergerät Zulässige Liste** eine Liste zulässiger Geräte konfigurieren. Benutzer können auf diese Geräte zugreifen, und Sie können die Zugriffsstufe durch Berechtigungen steuern.

   Tipp

   Die Liste der zulässigen USB-Geräte unterstützt die Verwendung des Sterns (*) als Platzhalter. Verwenden Sie den Stern (*) in beliebigen Feldern, um alle Geräte einzuschließen, die den Kriterien der übrigen Felder entsprechen. Beispiel: [manufacturer]-[Produkt-ID]-* platziert alle Geräte des angegebenen Herstellers und Produkttyps in die Liste der zulässigen Geräte, unabhängig von der Seriennummer.

   a. Geben Sie den Gerätehersteller, die Produkt-ID und die Seriennummer für ein USB-Speichergerät ein.
   b. Klicken Sie auf **Hinzufügen**.

      Tipp

      Um ein Gerät aus der Liste zu löschen, wählen Sie einen Eintrag aus und klicken Sie auf **Entfernen**.

   c. Wählen Sie die Berechtigung für dieses Gerät.

Weitere Informationen zu Berechtigungen finden Sie unter *Berechtigungen für Speichergeräte auf Seite 8-2*.

Hinweis

USB-Speichergeräte auf der zulässigen Liste müssen eine höhere Berechtigungsstufe haben als die Berechtigungseinstellung für USB-Speichergeräte im **Geräte**-Abschnitt.

8. Unter **Benachrichtigung** wählen Sie die Option **Eine Benachrichtigung auf dem Agent anzeigen, wenn ein neues Gerät erkannt wird**, um eine Benachrichtigung anzuzeigen, wenn ein neues Speichermedium mit dem Endpunkt verbunden wird. Die Benachrichtigung zeigt die Zugriffsberechtigung für das neue Speichermedium an.

9. Wenn Sie eine oder mehrere Gruppen oder Security Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die Gruppen oder Security Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:

   - **Für alle Agenten übernehmen**: Wendet die Einstellungen auf alle vorhandenen Security Agents und auf alle neuen Security Agent an, die einer vorhandenen/zukünftigen Gruppe hinzugefügt werden. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden sind.

   - **Nur auf zukünftige Gruppen anwenden**: Wendet die Einstellungen nur auf Security Agents an, die zukünftigen Gruppen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf Security Agents angewendet, die einer vorhandenen Gruppe hinzugefügt werden.

Gerätelisten-Tool

Führen Sie Device List an einem Windows-Computer lokal aus, um externe Geräte abzufragen, die mit dem Computer verbunden sind. Das Tool überprüft nach externen Geräten und zeigt die entdeckten Geräte

dann in einem Browser-Fenster an. Diese Informationen können Sie zur Konfiguration von Geräteeinstellungen bei der Gerätesteuerung verwenden.

Das Gerätelisten-Tool ausführen

Hinweis

Das Gerätelisten-Tool unterstützt keine Endpunkte, die macOS oder OS X ausführen.

Prozedur

1. Navigieren Sie auf dem Trend Micro Apex One (Mac) Server-Computer zu <Installationsordner des Servers>`\PCCSRV\Admin\Utility\ListDeviceInfo`.
2. Externe Geräte mit einem Ziel-Windows-Computer verbinden.
3. Kopieren Sie `listDeviceInfo.exe` auf den Windows-Computer.
4. Führen Sie `listDeviceInfo.exe` auf dem Windows-Computer aus.
5. Es öffnet sich ein Browser-Fenster mit Informationen zu den Geräten. Die Gerätesteuerung verwendet folgende Informationen:
   - Anbieter oder Hersteller
   - Modell- oder Produkt-ID
   - Seriennummer oder Seriennummer

Konfigurieren von Benachrichtigungen zur Gerätesteuerung für Security Agents

Sie können Trend Micro Apex One (Mac) so konfigurieren, dass Benachrichtigungen auf Security Agent-Endpunkten angezeigt werden, um Endbenutzer über Verstöße gegen die Gerätesteuerung zu informieren.

Prozedur

1. Navigieren Sie zu **Benachrichtigungen** > **Agent-Benachrichtigungen**.
2. Unter **Verstöße gegen die Gerätesteuerung** die Standardnachricht akzeptieren oder ändern.

   Die folgende Tabelle beschreibt die Token-Variablen, die Sie verwenden können, um Daten für die Anzeige von Benachrichtigungsnachrichten darzustellen.

Token	Beschreibung
%DeviceType%	Gerätetyp (zum Beispiel "USB-Speichergerät") für einen Security Agent Endpunkt
%Permission%	Gerätesteuerung Richtlinieneinstellung (zum Beispiel, "Sperren")

3. Klicken Sie auf **Save**.

Protokolle der Gerätesteuerung anzeigen

Wenn ein neues Speichergerät mit einem Endpunkt verbunden wird, erstellt der Trend Micro Apex One (Mac)Security Agent einen Protokolleintrag für das Ereignis mit der Zugriffsberechtigung basierend auf den Einstellungen der Gerätesteuerung.

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon (), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Protokolle** > **Protokolle der Gerätesteuerung**.
4. Legen Sie die Protokollkriterien fest, und klicken Sie dann auf **Protokolle anzeigen**.

   Das Fenster **Protokolle der Gerätesteuerung** wird angezeigt.

5. Wenn Sie Protokolle als kommagetrennte Datei im `CSV`-Format speichern möchten, klicken Sie auf **In CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.

Kapitel 9

Server und Security Agents verwalten

In diesem Kapitel werden die Verwaltung und zusätzliche Konfigurationen von Trend Micro Apex One (Mac) Server und Agents erläutert.

Berechtigungen und andere Einstellungen

Auf dem **Berechtigungen und andere Einstellungen**-Bildschirm können Sie die Selbstschutzfunktion des Agenten konfigurieren, um zu verhindern, dass andere Programme und sogar der Benutzer Dateien, die Security Agent verwendet, ändern oder löschen.

Wenn Sie **Dateien schützen, die vom Agent verwendet werden** aktivieren und Security Agent auf einem Endpunkt ausgeführt wird, sperrt Apex One (Mac) die folgenden Dateien und Ordner:

- /Library/Application Support/TrendMicro/RPD
- /Users/*/Library/Application Support/TrendMicro/dlpmac.app
- /Library/LaunchDaemons/com.trendmicro.tmes.plugin.plist
- /Library/LaunchDaemons/com.trendmicro.tmsm.rpd.plist
- /Users/*/Library/Application Support/TrendMicro/chromeNativeDLP
- /Users/*/Library/Application Support/TrendMicro/firefoxNativeDLP

Hinweis

Apex One (Mac) lässt zu, dass Dateien dem Ordner `/Library/Application Support/TrendMicro/Tools` hinzugefügt werden. Die darin enthaltenen Dateien können jedoch nicht gelöscht werden.

Agent-Eigenschutz konfigurieren

Prozedur

1. Navigieren Sie zu **Agent-Verwaltung**.
2. Klicken Sie im Agentenbaum auf das Stamm-Icon (), um alle Security Agents einzuschließen, oder wählen Sie spezifische Gruppen oder Security Agents aus.
3. Klicken Sie auf **Einstellungen** > **Berechtigungen und andere Einstellungen**

4. Wählen Sie unter Security Agent-Eigenschutz **Dateien schützen, die vom Agent verwendet werden** aus.

5. Wenn Sie eine oder mehrere Gruppen oder Security Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die Gruppen oder Security Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:

   - **Für alle Agenten übernehmen**: Wendet die Einstellungen auf alle vorhandenen Security Agents und auf alle neuen Security Agent an, die einer vorhandenen/zukünftigen Gruppe hinzugefügt werden. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden sind.

   - **Nur auf zukünftige Gruppen anwenden**: Wendet die Einstellungen nur auf Security Agents an, die zukünftigen Gruppen hinzugefügt werden. Bei dieser Option werden die Einstellungen nicht auf Security Agents angewendet, die einer vorhandenen Gruppe hinzugefügt werden.

Certified Safe Software Service aktivieren

Der Certified Safe Software Service fragt Trend Micro Datenzentren ab, um die Sicherheit eines Programms zu überprüfen, das durch eine Antiviren-Suche erkannt wurde. Aktivieren Sie den Certified Safe Software Service, um die Häufigkeit von Fehlalarmen zu verringern.

Prozedur

1. Navigieren Sie zu **Agents** > **Certified Safe Software Service**.

2. Wählen Sie **Certified Safe Software Service für Antiviren-Suche aktivieren**.

3. Klicken Sie auf **Save**.

Hinweis

- Wenn Endpunkte innerhalb Ihres Netzwerks einen Proxy-Server benötigen, um auf das Internet zuzugreifen, konfigurieren Sie die Proxy-Einstellungen für interne Agents.
- Weitere Informationen finden Sie unter *Agent-Server-Kommunikationseinstellungen konfigurieren auf Seite 9-15*.

Vorausschauendes Maschinenlernen aktivieren

Das Trend Micro Vorausschauendes Maschinenlernen setzt moderne Technologien ein, um Bedrohungsinformationen zu korrelieren und ausführliche Dateianalysen durchzuführen und so unbekannte neue Sicherheitsrisiken durch digitale DNS-Fingerabdrücke, API-Zuordnung und weitere Funktionen zu erkennen. Beim 'Vorausschauendes Maschinenlernen' wird außerdem eine Verhaltensanalyse für unbekannte Prozesse oder Prozesse mit geringer Prävalenz durchgeführt, um zu ermitteln, ob eine neue oder unbekannte Bedrohung versucht, das Netzwerk zu infizieren.

Beim 'Vorausschauendes Maschinenlernen' handelt es sich um ein leistungsstarkes Tool, mit dem Ihre Umgebung vor unbekannten und Zero-Day-Angriffen geschützt wird.

Um diese Funktion zu aktivieren, wechseln Sie zu **Agents** > **Agent-Verwaltung** > **Einstellungen** > **Einstellungen für Vorausschauendes Maschinenlernen**, und wählen Sie **Vorausschauendes Maschinenlernen aktivieren**.

Hinweis

Wenn Endpunkte innerhalb Ihres Netzwerks einen Proxy-Server benötigen, um auf das Internet zuzugreifen, konfigurieren Sie die Proxy-Einstellungen für interne Agents.

Weitere Informationen finden Sie unter *Agent-Server-Kommunikationseinstellungen konfigurieren auf Seite 9-15*.

Aktualisierung des Servers und Security Agents

Die Konsole von Plug-in Manager zeigt an, wenn ein neuer Build oder eine neue Version von Trend Micro Apex One (Mac) verfügbar ist.

Aktualisieren Sie den Server und Security Agents sofort, wenn der neue Build oder die neue Version verfügbar wird.

Stellen Sie vor dem Upgrade sicher, dass Server und Security Agents über die unter *Server-Installationsvoraussetzungen auf Seite 2-2* und *Voraussetzungen für die Installation des Agents auf Seite 4-2* beschriebenen Ressourcen verfügen.

Server aktualisieren

Vorbereitungen

Wichtig

Bevor Sie Apex One (Mac) Patch 2 und höher installieren oder aktualisieren, stellen Sie sicher, dass das Zertifikat für Microsoft-Internetinformationsdienste (IIS) nicht abgelaufen ist.

Weitere Informationen finden Sie unter https://success.trendmicro.com/solution/000283033.

Trend Micro empfiehlt die Erstellung einer Sicherungskopie der Programmdateien und Datenbank des Servers, die bei eventuellen Problemen mit dem Upgrade wiederhergestellt werden können.

- Programmdateien
  - Standardpfad:
    - `C:\Program Files\Trend Micro\OfficeScan\Addon\TMSM`
    - `C:\Program Files\Trend Micro\Apex One\Addon\TMSM`

    oder

    - `C:\Program Files (x86)\Trend Micro\OfficeScan\Addon\TMSM`
    - `C:\Program Files (x86)\Trend Micro\Apex One\Addon\TMSM`
  - Zu sichernde Dateien:
    - `..\apache-activemq\conf\.*`
    - `..\apache-activemq\bin\wrapper.conf`
    - `.\ServerInfo.plist`
- Datenbankdateien. Weitere Informationen erhalten Sie unter *Server-Datenbank sichern auf Seite 9-10*.

Prozedur

1. Öffnen Sie die Apex One oder OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
2. Navigieren Sie zum Bereich **Trend Micro Apex One (Mac)** und klicken Sie auf **Download**.

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

   Plug-in Manager lädt das Paket nach `<server installation folder>\PCCSRV\Download` herunter.

   `<server installation folder>` ist normalerweise `C:\Program Files\Trend Micro\OfficeScan` oder `C:\Program Files\Trend Micro\Apex One`.

3. Verfolgen Sie den Download-Fortschritt.

   Sie können während des Downloads zu anderen Fenstern navigieren.

   Wenn beim Herunterladen des Pakets Probleme auftreten, überprüfen Sie über die Apex One oder OfficeScan Webkonsole die Server-Update-Protokolle. Klicken Sie im Hauptmenü auf **Protokolle** > **Server-Update**.

4. Um Trend Micro Apex One (Mac) sofort zu aktualisieren, klicken Sie auf **Jetzt upgraden**, oder führen Sie Folgendes aus, um die Installation zu einem späteren Zeitpunkt durchzuführen:

   a. Klicken Sie auf **Später aktualisieren**.

   b. Öffnen Sie das Fenster Plug-in Manager.

   c. Navigieren Sie zum Bereich **Trend Micro Apex One (Mac)** und klicken Sie auf **Aktualisieren**.

5. Verfolgen Sie den Upgrade-Fortschritt. Nach dem Upgrade wird das Fenster von Plug-in Manager neu geladen.

Security Agents upgraden

Achtung

Um Agenten-Upgrades zu ermöglichen, deaktivieren Sie das Kontrollkästchen **Agents können Komponenten aktualisieren, nicht jedoch das Agent-Programm upgraden oder Hotfixes installieren** auf dem Bildschirm **Agent-Verwaltung** > **Einstellungen** > **Update-Einstellungen**.

Prozedur

1. Führen Sie einen der folgenden Schritte durch:

   - Führen Sie ein manuelles Update durch. Stellen Sie sicher, dass Sie in der Liste der Komponenten **Trend Micro Apex One (Mac) Agent** auswählen.
   - Wählen Sie in der Agent-Hierarchie die Security Agents für das Upgrade aus und klicken Sie dann auf **Tasks** > **Update**.

- Wenn das zeitgesteuerte Update aktiviert wurde, stellen Sie sicher, dass **Trend Micro Apex One (Mac) Agent** ausgewählt wurde.
- Weisen Sie die Benutzer an, in der Agent-Konsole auf **Aktualisieren** zu klicken.

Security Agents, die die Benachrichtigung erhalten, beginnen mit dem Upgrade. Am Endpunkt zeigt das Trend Micro Apex One (Mac)-Symbol in der Menüleiste an, dass das Produkt aktualisiert wird. Benutzer können keine Aufgaben von der Konsole ausführen, bis das Upgrade abgeschlossen ist.

2. Überprüfen Sie den Upgrade-Fortschritt.
   a. Klicken Sie im Hauptmenü auf „Übersicht“ und wechseln Sie unter **Update-Status** zum Abschnitt **Programm**.
   b. Klicken Sie auf den Link in der Spalte **Nicht aktualisiert**. Die Agent-Struktur wird geöffnet, und es werden alle Security Agents angezeigt, für die das Upgrade nicht durchgeführt wurde.
   c. Um die Security Agents zu aktualisieren, die noch nicht aktualisiert wurden, klicken Sie auf **Tasks** > **Update**.

Protokolle verwalten

Trend Micro Apex One (Mac) führt umfassende Protokolle über Sicherheitsrisikoerkennung, blockierte URLs, Suchvorgänge und Ereignisse zur Gerätesteuerung. Mit Hilfe dieser Protokolle können Sie die Schutzrichtlinien Ihres Unternehmens bewerten und Security Agents ermitteln, die einem höheren Infektions- oder Angriffsrisiko ausgesetzt sind.

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell oder nach einem festgelegten Zeitplan über die Webkonsole.

Prozedur

1. Gehen Sie zu **Administration** > **Protokollwartung**.

2. Wählen Sie **Zeitgesteuertes Löschen von Protokollen aktivieren**.
3. Wählen Sie aus, ob alle Protokolle gelöscht werden sollen oder nur diejenigen, die älter als eine bestimmte Anzahl an Tagen sind.
4. Geben Sie Startzeitpunkt und Zeitintervall für die Protokolllöschung an.
5. Klicken Sie auf **Save**.

Lizenzen verwalten

Die Lizenz für Trend Micro Apex One (Mac) kann in der Webkonsole angezeigt, aktiviert und erneuert werden.

Der Status der Produktlizenz bestimmt, welche Funktionen den Benutzern zur Verfügung stehen. Genaue Angaben finden Sie in der nachfolgenden Tabelle.

Lizenztyp und Status	Funktionen			
	Echtzeitsuche	Zeitgesteuerte Suche	Web Reputation	Pattern-Update
Vollversion und Aktiviert	Aktiviert	Aktiviert	Aktiviert	Aktiviert
Testversion (Demo) und aktiviert	Aktiviert	Aktiviert	Aktiviert	Aktiviert
Vollversion und abgelaufen	Aktiviert	Aktiviert	Aktiviert	Deaktiviert
Testversion und abgelaufen	Deaktiviert	Deaktiviert	Deaktiviert	Deaktiviert
Nicht aktiviert	Deaktiviert	Deaktiviert	Deaktiviert	Deaktiviert

Hinweis

Wenn der Server nur eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Lizenzaktualisierungen in *Einschränkungen eines reinen IPv6-Servers auf Seite A-2*.

Prozedur

1. Navigieren Sie zu **Administration** > **Produktlizenz**.
2. Informationen zur Produktlizenz anzeigen. Um die neuesten Lizenzinformationen zu erhalten, klicken Sie auf **Informationen aktualisieren**.

   Der Abschnitt **Lizenzinformationen** bietet Ihnen folgende Informationen:

   - **Status**: Zeigt entweder „Aktiviert“ oder „Abgelaufen“ an
   - **Version**: Zeigt entweder „Vollversion“ oder „Testversion“ an. Wenn Sie die Testversion verwenden, können Sie jederzeit auf die Vollversion upgraden. Um Upgrade-Anweisungen zu erhalten, klicken Sie auf **Hinweise für das Upgrade der Lizenz anzeigen**.
   - **Arbeitsplätze**: Die maximale Anzahl von Agenteninstallationen, die die Lizenz unterstützt
   - **Lizenz läuft ab am**: Das Ablaufdatum der Lizenz
   - **Aktivierungscode**: Der Code zur Aktivierung der Lizenz
   - **Zuletzt aktualisiert**: Datum und Uhrzeit des letzten Updates der Lizenz.
3. Um einen neuen Aktivierungscode anzugeben, klicken Sie auf **Neuer Aktivierungscode**.
4. Geben Sie den Aktivierungscode im daraufhin angezeigten Fenster ein, und klicken Sie auf **Speichern**.

   Dieses Fenster enthält außerdem einen Link zur Trend Micro Website, auf der Einzelheiten zu Ihrer Lizenz zur Verfügung stehen.

Server-Datenbank sichern

Prozedur

1. Halten Sie die folgenden Dienste über die Microsoft Management Console an:
   - **ActiveMQ für Apex One (Mac)**
   - **Apex One (Mac) Hauptdienst**
2. Öffnen Sie SQL Server Management Studio (z. B. über **Windows Start-Menü** > **Programme** > **Microsoft SQL Server {Version}** > **SQL Server Management Studio**.
3. Suchen Sie nach `db_TMSM` und verwenden Sie dann die **Sicherung**sfunktion in SQL Server Management Studio, um die Datenbankdateien zu sichern.

   Details finden Sie in der SQL Server Management Studio-Dokumentation.
4. Starten Sie die angehaltenen Dienste.

Serverdatenbank wiederherstellen

Vorbereitungen

Bereiten Sie die Sicherung der während der Sicherung erstellten Datenbankdateien vor. Weitere Informationen finden Sie unter *Server-Datenbank sichern auf Seite 9-10*.

Prozedur

1. Halten Sie die folgenden Dienste über die Microsoft Management Console an:
   - **ActiveMQ für Apex One (Mac)**
   - **Apex One (Mac) Hauptdienst**
2. Öffnen Sie SQL Server Management Studio (z. B. über **Windows Start-Menü** > **Programme** > **Microsoft SQL Server {Version}** > **SQL Server Management Studio**.

3. Suchen Sie `db_TMSM` und verwenden Sie die Option **Trennen** (Detach) in SQL Server Management Studio zum Abtrennen der aktuellen Datenbankdateien.

   Details finden Sie in der SQL Server Management Studio-Dokumentation.

4. Hängen Sie die gesicherten Datenbankdateien mit der Option **Anhängen** (Attach) an.

5. Starten Sie die angehaltenen Dienste.

Trend Micro Apex Central und Control Manager-Integration in dieser Version

Diese Version von Trend Micro Apex One (Mac) unterstützt Trend Micro Apex Central v4476 oder höher. In dieser Version können Sie Trend Micro Apex One (Mac) Richtlinien erstellen, verwalten und verteilen und Endpunkte von Trend Micro Apex Central überwachen.

Sie können Endpunkte mit dem **Wichtigste Leistungsindikatoren für Apex One (Mac)**-Widget in Trend Micro Apex Central überwachen.

Weitere Informationen finden Sie unter *Leistungsindikatoren-Widget auf Seite 9-13*.

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

Hinweis

Sie können auch Trend Micro Apex Central oder Control Manager als Update-Adresse des Trend Micro Apex One (Mac) Servers angeben. Weitere Informationen finden Sie unter *Update-Adresse des Servers konfigurieren auf Seite 5-5*.

Leistungsindikatoren-Widget

Verwenden Sie dieses Widget im Trend Micro Apex Central **Dashboard**-Fenster, um basierend auf ausgewählten Kriterien Leistungsindikatoren (KPI) für Apex One (Mac) anzuzeigen.

Informationen dazu, wie Sie ein Widget zum **Dashboard**-Fenster hinzufügen, finden Sie in der Dokumentation zu Trend Micro Apex Central oder Control Manager.

Tipp

Standardmäßig markiert das Widget bei 15 Vorkommnissen von Ereignissen diese als „Wichtig“ ( ) und bei 30 Vorkommnissen als „Kritisch“ ( ).

Optional können Sie durch das Konfigurieren von Ereignisschwellenwerten Ereignisse als 'Wichtig' oder 'Kritisch' markieren.

Einstellungen für Serververbindungen konfigurieren

Geben Sie den Trend Micro Apex Central Server an, um Daten für die Widget-Anzeige zu erhalten.

1. Navigieren Sie zum **Dashboard**-Fenster auf Trend Micro Apex Central.
2. Klicken Sie auf die Registerkarte, auf der das **Wichtigste Leistungsindikatoren für Apex One (Mac)**-Widget hinzugefügt wurde.
3. Wählen Sie das Symbol **Servereinstellungen** ( ) aus dem Menü oben rechts ( ) im Widget aus.
4. Wählen Sie einen oder mehrere Apex One (Mac)-Server aus.
5. Klicken Sie auf **Save**.

Leistungsindikatoren konfigurieren

Greifen Sie in Trend Micro Apex Central oder Control Manager auf das Widget **Wichtigste Leistungsindikatoren für Apex One (Mac)** auf dem **Dashboard** zu, um die folgenden indikatorbezogenen Tasks durchzuführen.

Tabelle 9-1. KPI-Widget-Indikator-Tasks

Aufgabe	Schritte
Neuen Indikator hinzufügen	1. Klicken Sie auf **Add Indicator**. Das Fenster **Add Indicator** wird angezeigt. 2. Wählen Sie eine Option aus dem Listenfeld **Name** und passen Sie ggfs. die Einstellungen an. 3. Klicken Sie auf **Save**.
Indikator bearbeiten	1. Klicken Sie auf den Indikator in der Liste. Das Fenster **Edit Indicator** wird angezeigt. 2. Passen Sie die Einstellungen an. 3. Klicken Sie auf **Save**.
Indikator löschen	1. Klicken Sie auf den Indikator in der Liste. Das Fenster **Edit Indicator** wird angezeigt. 2. Klicken Sie auf **Löschen**. 3. Klicken Sie auf **OK**.
Einstellungen für den Ereignisschwellenwert konfigurieren	1. Wählen Sie im Fenster **Add Indicator** oder **Edit Indicator** die Option **Enable alerts at the following thresholds** aus. 2. Geben Sie die Mindestanzahl an Ereignisvorkommen für jeden Ereignistyp ein. 3. Klicken Sie auf **Save**. **Hinweis** Das Symbol 'Wichtig' oder 'Kritisch' wird in der Spalte **Vorkommen** angezeigt, wenn beide der folgenden Aussagen wahr sind: • Die Anzahl der Ereignisvorkommen, die diesem Indikator entsprechen, ist gleich oder größer als der Schwellenwert. • **Warnungen bei folgendem Schwellenwert aktivieren** ist ausgewählt.

Widget-Einstellungen konfigurieren

Wählen Sie auf dem Trend Micro Apex Central oder im Control Manager **Dashboard** Bildschirm **Widget-Einstellungen** im Menü im oberen rechten Bereich des Widgets, um die folgenden Tasks durchzuführen.

TABELLE 9-2. KPI-Widget-Einstellungen

AUFGABE	SCHRITTE
Widget-Titel bearbeiten	Geben Sie den Widget-Titel in das Textfeld ein.
Tägliche Update-Zeit konfigurieren	Wählen Sie im Listenfeld die Stunde aus, zu der die Widget-Daten täglich erzeugt werden sollen. **Tipp** Klicken Sie auf das Aktualisierungssymbol ( ), um die Widget-Daten manuell zu aktualisieren.

Agent-Server-Kommunikationseinstellungen konfigurieren

Security Agents identifizieren den Server, der sie verwaltet, anhand des Servernamens oder der IPv4/IPv6-Adresse. Während der Installation des Trend Micro Apex One (Mac) Servers ermittelt das Installationsprogramm die IP-Adressen des Servers. Diese werden dann im Fenster **Kommunikation zwischen Agent und Server** angezeigt.

Wichtig

Wenn Sie planen, alle bestehenden Servernamen und IPv4/IPv6-Adressen zu aktualisieren oder zu ersetzen oder den Listening-Port (in Apex One) oder die Proxy-Einstellungen zu ändern, tun Sie dies vor der Installation von Security Agents. Wenn Sie Security Agents installiert haben und dann Änderungen vornehmen, verliert Security Agents die Verbindung zum Server und die einzige Möglichkeit, die Verbindung wiederherzustellen, besteht darin, Security Agents erneut bereitzustellen.

Je nach Version des Security Agents kommuniziert der Server mit Security Agents über einen der folgenden Abhörports:

- Für Security Agent Version 3.5.3xxx oder später: 4343

  Security Agents verwenden denselben Abhörport (standardmäßig 4343), wie in Apex One konfiguriert.

- Für Security Agent Version 3.5.2xxx oder früher: 61617

  Security Agents verwenden die bestehenden Server- und Abhörporteinstellungen. Sie können die Einstellungen nicht ändern.

Hinweis

- Vergewissern Sie sich, dass die Portnummern noch nicht durch andere Anwendungen genutzt werden, um Konflikte und Probleme bei der Agent/Server-Kommunikation zu vermeiden.
- Falls auf dem Server eine Firewall verwendet wird, stellen Sie sicher, dass sie nicht den Listening-Port für die Agent/Server-Kommunikation blockiert. Falls auf dem Endpunkt beispielsweise die Apex One Security Agent Firewall aktiviert wurde, fügen Sie eine Richtlinienausnahme hinzu, die eingehenden und ausgehenden Datenverkehr über den Listening-Port zulässt.
- Sie können Security Agents so konfigurieren, dass sie sich über einen Proxy-Server mit dem Server verbinden. Für gewöhnlich ist für die Agent/Server-Kommunikation innerhalb eines Unternehmensnetzwerks kein Proxy-Server notwendig.

Prozedur

1. Wechseln Sie zu **Administration** > **Kommunikation zwischen Agent und Server**.

   Der Abschnitt **Servername und Listening-Port** zeigt die Serveradresse und Informationen zum Abhörport an.

2. Unter **Proxy-Einstellungen** wählen Sie eine Option aus.
   - Kein Proxy: Wählen Sie diese Option, wenn Security Agents direkt mit dem Server verbunden ist.
   - System-Proxy-Einstellungen auf Agenten verwenden: Wählen Sie diese Option, um die auf der Agentenkonsole konfigurierten System-Proxy-Einstellungen zu verwenden.
   - Verwenden Sie die folgenden Proxy-Einstellungen, wenn Agenten eine Verbindung zum Server herstellen: Wählen Sie diese Option und füllen Sie die folgenden Felder aus, um die Proxy-Einstellungen zu konfigurieren.
     a. Wählen Sie das Proxy-Server-Protokoll.
     b. Geben Sie den Namen des Proxy-Servers oder seine IPv4/IPv6-Adresse und die Portnummer ein.
     c. Falls der Proxy-Server einen Benutzernamen und ein Kennwort erfordert, geben Sie diese in die dafür vorgesehenen Textfelder ein.
3. Klicken Sie auf **Save**.
4. Wenn Sie aufgefordert werden, die Trend Micro Apex One (Mac) Dienste neu zu starten, damit die Einstellungen wirksam werden, führen Sie die folgenden Schritte aus:
   a. Navigieren Sie zum <*Server-Installationsordner*>.
   b. Doppelklicken Sie auf `restart_TMSM.bat`.
   c. Warten Sie, bis alle Dienste neu gestartet sind.

Inaktive Security Agents

Trend Micro Apex One (Mac) zeigt Security Agents als inaktiv an:

- Wenn Sie das Agent-Programm mit Hilfe des Agent-Deinstallationsprogramms von den Endpunkten entfernen, Security Agent aber nicht vom Server abmelden.

- Wenn Sie die Festplatte des Endpunkts neu formatiert haben, ohne das Security Agent vom Server abzumelden.
- Wenn Sie die Agent-Dateien manuell entfernt haben.
- Wenn ein Benutzer das Security Agent für einen längeren Zeitraum entlädt oder deaktiviert.

Damit in der Agent-Hierarchie nur aktive Security Agents angezeigt werden, können Sie Trend Micro Apex One (Mac) so konfigurieren, dass inaktive Security Agents automatisch aus der Agent-Hierarchie gelöscht werden.

Automatisches Entfernen von inaktiven Security Agents

Prozedur

1. Wählen Sie **Administration** > **Inaktive Agents** aus.
2. Wählen Sie **Automatische Entfernung inaktiver Agents aktivieren** aus.
3. Legen Sie fest, nach wie vielen Tagen Trend Micro Apex One (Mac) den Security Agent als inaktiv einstufen soll.
4. Klicken Sie auf **Save**.

Agent-Symbole

Symbole im Systemtray des Endpunkts und in der Hauptkonsole zeigen den Status eines Security Agent und die aktuell ausgeführte Aufgabe an.

Task-Leisten-Symbol	Menüsymbol	Beschreibung
		Der Security Agent läuft und ist mit seinem übergeordneten Server verbunden.
		Die Produktlizenz wurde aktiviert.
		Der Security Agent ist in Betrieb, aber von seinem übergeordneten Server getrennt.

Task-Leisten-Symbol	Menüsymbol	Beschreibung
		Eine neue Komponentenversion ist verfügbar. Aktualisieren Sie Security Agent sofort.
		Der Security Agent hat eine Sicherheitsbedrohung erkannt, die einen Neustart des Computers erfordert, um sie zu beheben.
		Der Security Agent scannt nach Sicherheitsrisiken und ist mit seinem übergeordneten Server verbunden.
		Der Security Agent aktualisiert Komponenten von seinem übergeordneten Server.
		Ein Komponenten-Update erfordert, dass Sie den Security Agent neu starten, um die Installation abzuschließen.
		Intelligente Suche oder Web Reputation-Dienst ist auf dem Security Agent nicht verfügbar. Überprüfen Sie Ihre Netzwerkverbindung.
		Das Security Agent wurde beim übergeordneten Server registriert, aber die Produktlizenz wurde nicht aktiviert. Einige Funktionen von Security Agent stehen nicht zur Verfügung, wenn die Lizenz nicht aktiviert wurde. Weitere Informationen finden Sie unter *Lizenzen verwalten auf Seite 9-9*.
		Der Security Agent wurde nicht beim übergeordneten Server registriert. Die Produktlizenz kann aktiviert oder nicht aktiviert sein. Wenn das Security Agent nicht beim übergeordneten Server registriert ist, sind alle Funktionen (einschließlich Echtzeitsuche, Manuelle Suche, Zeitgesteuerte Suche, Web Reputation und Pattern-Updates) deaktiviert.

Task-Leisten-Symbol	Menüsymbol	Beschreibung
		Die Produktlizenz (Voll- oder Testversion) wurde aktiviert, ist aber abgelaufen. Einige Security Agent-Funktionen sind nicht verfügbar, wenn die Lizenz abgelaufen ist.
		Das Security Agent wurde auf einer nicht unterstützten Plattform installiert.
		Das Security Agent funktioniert nicht ordnungsgemäß. Aktualisieren Sie das Security Agent auf die neueste Version oder kontaktieren Sie den Technischen Support.
		Der Security Agent hat eine DURCHSUCHEN abgeschlossen oder eine Sicherheitsbedrohung erkannt.

Kapitel 10

Hilfe anzeigen

Dieses Kapitel beschreibt die Behebung von Problemen, die auftreten können, und die Kontaktaufnahme mit dem Support.

Fehlerbehebung

Zugriff auf die Webkonsole

Problem:

Es kann nicht auf die Webkonsole zugegriffen werden.

Prozedur

1. Überprüfen Sie, ob der Endpunkt die Voraussetzungen zum Installieren und Ausführen von Trend Micro Apex One (Mac) Server erfüllt.

   Weitere Informationen finden Sie unter *Server-Installationsvoraussetzungen auf Seite 2-2*.

2. Überprüfen Sie, ob die folgenden Dienste gestartet sind:

   - **ActiveMQ für Apex One (Mac)**
   - **Apex One Plug-in Manager**
   - **Apex One (Mac) Hauptdienst**

3. Durchsuchen Sie die Debug-Protokolle. Durchsuchen Sie die Protokolle mit Hilfe der Suchfunktion nach den Schlüsselwörtern ‚Fehler' oder ‚Fehlgeschlagen'.

   - **Installationsprotokolle**: `C:\TMSM*.log`
   - **Allgemeine Debug-Protokolle**: <*Server-Installationsordner*>`\debug.log`
   - **Apex One**: `C:\Program Files\Trend Micro\Apex One\PCCSRV\Log\ofcdebug.log`

     a. Aktivieren Sie die Debug-Protokollierung, wenn die Datei nicht vorhanden ist. Klicken Sie im Banner der Apex One Webkonsole auf das erste „A" in „Apex One", legen Sie die Einstellungen für die Debug-Protokollierung fest, und klicken Sie auf **Speichern**.

b. Wiederholen Sie die Schritte, die zum Problem mit dem Zugriff auf die Webkonsole geführt haben.

c. Durchsuchen Sie die Debug-Protokolle.

4. Überprüfen Sie die Registrierungsschlüssel von Trend Micro Apex One (Mac). Wechseln Sie dafür zu `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\TMSM`.

5. Überprüfen Sie die Datenbankdateien und Registrierungsschlüssel.

a. Überprüfen Sie, ob die folgenden Dateien unter `C:\Program Files\Microsoft SQL Server\MSSQL.x\MSSQL\Data\` oder `C:\Program Files(x86)\Microsoft SQL Server\MSSQL.x\MSSQL\Data\` existieren:

- `db_TMSM.mdf`
- `db_TMSM_log.LDF`

b. Überprüfen Sie, ob die Datenbankinstanz für Trend Micro Apex One (Mac) im Registrierungsschlüssel von Microsoft SQL Server vorhanden ist:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\TMSM`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\ TMSM\ MSSQLServer\CurrentVersion`

6. Senden Sie die folgenden Informationen an Trend Micro:

- Registrierungsdateien

  a. Gehen Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL server\TMSM`.

  b. Klicken Sie auf **Datei** > **Exportieren** und speichern Sie dann den Registrierungsschlüssel in einer `.reg`-Datei.

- Angaben zum Server

- Version des verwendeten Betriebssystems
- Verfügbarer Speicherplatz
- Verfügbarer Arbeitsspeicher
- Informationen darüber, ob andere Plug-in-Programme installiert sind, z. B. Intrusion Defense Firewall.

7. Starten Sie die Dienste für Trend Micro Apex One (Mac) neu.
   a. Navigieren Sie zum <*Server-Installationsordner*>.
   b. Doppelklicken Sie auf `restart_TMSM.bat`.
   c. Warten Sie, bis alle Dienste neu gestartet sind.
8. Der Dienst Trend Micro Apex One (Mac) sollte immer ausgeführt werden. Sollte dieser Dienst nicht aktiv sein, liegt möglicherweise ein Problem mit dem Dienst ‚ActiveMQ' vor.
   a. Sichern Sie ActiveMQ-Daten in `C:\Program Files\Trend Micro\OfficeScan\Addon\TMSM\apache-activemq\data\*.*` oder `C:\Program Files\Trend Micro\Apex One\Addon\TMSM\apache-activemq\data\*.*`.
   b. Löschen Sie die ActiveMQ-Daten.
   c. Versuchen Sie, den Dienst für Trend Micro Apex One (Mac) durch Doppelklicken auf `restart_TMSM.bat` neu zu starten.
   d. Versuchen Sie erneut, auf die Webkonsole zuzugreifen, um zu überprüfen, ob das Problem gelöst wurde.

Server-Deinstallation

Problem:

Die folgende Meldung wird angezeigt:

```
Unable to uninstall the plug-in program. The uninstallation
command for the plug-in program is missing in the registry key.
```

Prozedur

1. Öffnen Sie den Registrierungseditor und wechseln Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Wow6432Node\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`.
2. Setzen Sie den Wert auf `1.0.1000` zurück.
3. Löschen Sie den Registrierungsschlüssel des Plug-in-Programms, z. B. `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_xxxx`.
4. Starten Sie den Apex One Plug-in Manager Dienst neu.
5. Laden Sie das Plug-in-Programm herunter, installieren Sie es, und deinstallieren Sie es anschließend.

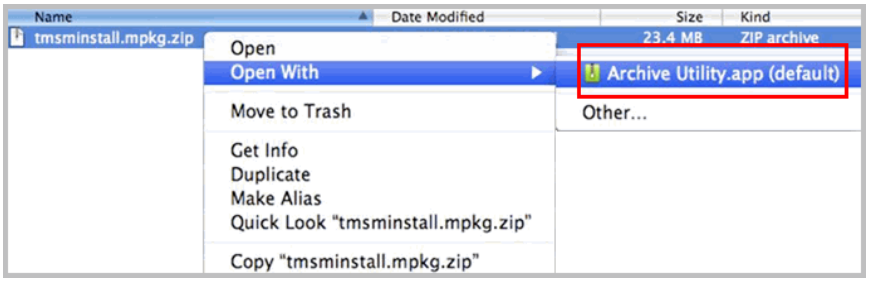
Agent-Installation

Problem:

Die Installation ist fehlgeschlagen. Das Installationspaket (`tmsminstall.zip` oder `tmsminstall.mpkg.zip`) wurde mit einem nicht im Mac-Computer integrierten Archivierungsprogramm oder einem nicht unterstützten Befehl (z. B. `unzip`) aus einem Befehlszeilenprogramm gestartet, wodurch der entpackte Ordner (`tmsminstall`) bzw. die entpackte Datei (`tmsminstall.mpkg`) beschädigt wurden.

Prozedur

1. Entfernen Sie den entpackten Order (`tmsminstall`) bzw. die entpackte Datei (`tmsminstall.mpkg`).
2. Starten Sie das Installationspaket mit einem integrierten Archivierungsprogramm.



Mit dem folgenden Befehl kann das Paket auch von der Befehlszeile ausgeführt werden:

- Wenn das Paket `tmsminstall.zip` lautet:

  ```
  ditto -xk <Pfad der Datei tmsminstall.zip> <Zielordner>
  ```

  Beispiel:

  ```
  ditto -xk users/mac/Desktop/tmsminstall.zip users/mac/
  Desktop
  ```

- Wenn das Paket `tmsminstall.mpkg.zip` lautet:

  ```
  ditto -xk <Pfad der Datei tmsminstall.mpkg.zip>
  <Zielordner>
  ```

  Beispiel:

  ```
  ditto -xk users/mac/Desktop/tmsminstall.mpkg.zip
  users/mac/Desktop
  ```

Kommunikation zwischen Agent und Server

Problem:

Security Agents kann nicht mit dem Server kommunizieren.

Wenn Sie das Webhost-Zertifikat auf dem Apex One-Server aktualisiert haben, authentifiziert Security Agents das neue Zertifikat automatisch, bevor die Verbindung zum Server wiederhergestellt wird. Dies kann einige Zeit

in Anspruch nehmen. Während dieses Vorgangs wird Security Agents vom Server getrennt.

Um zu überprüfen, ob Security Agents das neue Zertifikat authentifiziert haben, stellen Sie sicher, dass die folgenden Dateien mit einem aktuellen Zeitstempel aktualisiert wurden:

- Auf dem Security Agent-Endpunkt:

  `/Library/Application Support/TrendMicro/common/conf/website.pem`

- Auf dem Apex One Server:
  - `<TMSM>\TMSM_HTML\ActiveUpdate\ClientInstall\tmsminstall.zip`
  - `<TMSM>\TMSM_HTML\A0FB621601F4D0FAB00B64F415A2C68C\ClientInstall\ServerInfoHttps.zip`
  - `<TMSM>\TMSM_HTML\A0FB621601F4D0FAB00B64F415A2C68C\ClientInstall\ServerInfoHttpsLocal.zip`

Wenn Security Agents nach Abschluss der Zertifikatsauthentifizierung nicht mit dem Server verbunden sind, führen Sie die folgenden Schritte aus, um die Protokolle zu überprüfen:

Prozedur

1. Auf dem Server die Protokolle aus <Server-Installationsordner>\debug.log abrufen
2. Am Security Agent-Endpunkt folgen Sie den Schritten in *Allgemeiner Agent-Fehler auf Seite 10-7*, um Protokolle zu sammeln.
3. Durchsuchen Sie die Protokolle mit dem Schlüsselwort "Fehler" oder "fehlgeschlagen".

Allgemeiner Agent-Fehler

Problem:

Ein Fehler oder Problem wurde auf dem Security Agent festgestellt.

Prozedur

1. Öffnen Sie `<agent installation folder>/Tools` und starten Sie den Trend Micro Debug Manager.
2. Folgen Sie den Programmanweisungen, um die Informationen zu ermitteln.

Warnung!

Das Programm funktioniert nicht, wenn es in einen anderen Ordner auf dem Endpunkt verschoben wurde. Falls es verschoben wurde, deinstallieren Sie den Security Agent und installieren Sie ihn neu.

Wenn das Programm in einen anderen Ordner kopiert wurde, entfernen Sie die Kopie und starten Sie das Programm aus dem ursprünglichen Ordner.

Technischer Support

Erfahren Sie mehr über die folgenden Themen:

- *Ressourcen zur Fehlerbehebung auf Seite 10-8*
- *Kontaktaufnahme mit Trend Micro auf Seite 10-10*
- *Verdächtige Inhalte an Trend Micro senden auf Seite 10-11*
- *Andere Ressourcen auf Seite 10-12*

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

In den Vereinigten Staaten erreichen Sie Ihre Trend Micro Ansprechpartner 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
- Kontaktaufnahme mit Trend Micro:

  http://www.trendmicro.de/ueber-uns/kontakt/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

IPv6-Unterstützung in Trend Micro Apex One (Mac)

Dieser Anhang enthält kritische Informationen für die Bereitstellung von Trend Micro Apex One (Mac) in einer Umgebung mit IPv6-Adressierung. Er bietet wichtige Hinweise zum Ausmaß der IPv6-Unterstützung in Trend Micro Apex One (Mac).

Trend Micro geht davon aus, dass der Leser über die erforderlichen Kenntnisse der Konzepte von IPv6 und der Arbeitsschritte verfügt, die zur Einrichtung eines Netzwerks mit IPv6-Adressierung benötigt werden.

IPv6-Unterstützung für Trend Micro Apex One (Mac) Server und Security Agents

IPv6-Unterstützung wird automatisch aktiviert nach der Installation oder Aktualisierung des Trend Micro Apex One (Mac)-Servers und Security Agents, die die IPv6-Anforderungen erfüllen.

Trend Micro Apex One (Mac)Security Agent IPv6-Anforderungen

Alle Mac OS X-Versionen, die vom Trend Micro Apex One (Mac)Security Agent unterstützt werden, bieten auch Unterstützung für IPv6.

Der Security Agent sollte vorzugsweise sowohl über IPv4- als auch IPv6-Adressen verfügen, da einige Elemente, zu denen er sich verbindet, nur IPv4-Adressierung unterstützen.

Einschränkungen eines reinen IPv6-Servers

Die folgende Tabelle enthält eine Liste von Einschränkungen von Trend Micro Apex One (Mac) Servern, die nur über eine IPv6-Adresse verfügen.

Tabelle A-1. Einschränkungen eines reinen IPv6-Servers

Element	Einschränkung
Agent-Verwaltung	Reine IPv4-Agents können nicht über einen reinen IPv6-Server verwaltet werden.
Updates und zentrale Verwaltung	Reine IPv6-Server können nicht aus reinen IPv4-Aktualisierungsquellen aktualisiert werden oder an reine IPv4-Produkte für zentrale Verwaltung wie die folgenden melden: • Trend Micro ActiveUpdate Server • Jede reine IPv4-Quelle für benutzerdefinierte Updates
Produktregistrierung, -aktivierung und -verlängerung	Reine IPv6-Server können keine Verbindung mit dem Trend Micro Online-Registrierungsserver herstellen, um das Produkt zu registrieren, die Lizenz abzurufen und die Lizenz zu aktivieren oder zu verlängern.

Element	Einschränkung
Proxyverbindung	Reine IPv6-Server können keine Verbindungen über reine IPv4-Proxyserver herstellen.

Die meisten dieser Einschränkungen können mit Hilfe eines Dualstapel-Proxyservers umgangen werden, der IPv4- in IPv6-Adressen und umgekehrt umwandeln kann (z. B. DeleGate). Setzen Sie den Proxyserver zwischen den Trend Micro Apex One (Mac) Server und die Entitäten, mit denen er zusammenarbeitet.

Einschränkungen bei reinen IPv6-Agents

Die folgende Tabelle enthält eine Liste von Einschränkungen, wenn Security Agents nur über eine IPv6-Adresse verfügen.

Tabelle A-2. Einschränkungen bei reinen IPv6-Agents

Vorgang	Einschränkung
Übergeordneter Server	Reine IPv6-Agents können nicht über einen reinen IPv4-Server verwaltet werden.
Updates	Reine IPv6-Agents können nicht aus reinen IPv4-Aktualisierungsquellen wie die folgenden aktualisiert werden: • Trend Micro ActiveUpdate Server • Ein reiner IPv4-Apex One (Mac) Server
Web Reputation-Abfragen	Reine IPv6-Agents können keine Web Reputation-Abfragen an das Trend Micro Smart Protection Network senden.
Proxy-Verbindung	Reine IPv6-Agents können keine Verbindungen über reine IPv4-Proxyserver herstellen.
Bereitstellung von Agents	Apple Remote Desktop ist nicht in der Lage, reinen IPv6-Endpunkten Agents bereitzustellen, da diese Endpunkte immer als offline angezeigt werden.

Die meisten dieser Einschränkungen können mit Hilfe eines Dualstapel-Proxyservers umgangen werden, der IPv4- in IPv6-Adressen und umgekehrt

umwandeln kann (z. B. DeleGate). Setzen Sie den Proxyserver zwischen die Agents und die Entitäten, mit denen sie sich verbinden sollen.

IPv6-Adressen konfigurieren

In der Webkonsole können Sie eine IPv6-Adresse oder einen Bereich von IPv6-Adressen konfigurieren. Im Folgenden erhalten Sie einige Richtlinien für die Konfiguration.

- Trend Micro Apex One (Mac) akzeptiert die Standarddarstellung von IPv6-Adressen.

  Beispiel:

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

- Trend Micro Apex One (Mac) akzeptiert ebenso verbindungslokale IPv6-Adressen wie:

  `fe80::210:5aff:feaa:20a2`

  Warnung!
  Seien Sie vorsichtig, wenn Sie verbindungslokale IPv6-Adressen angeben, da sie unter bestimmten Umständen nicht wie erwartet funktionieren könnten, auch wenn Trend Micro Apex One (Mac) sie akzeptiert. Beispielsweise können Agents nicht aus einer Aktualisierungsquelle in einem anderen Netzwerksegment aktualisiert werden, wenn dieses durch eine verbindungslokale IPv6-Adresse angegeben wird.

- IPv6-Adressen, die Teil einer URL sind, müssen zwischen eckige Klammern gesetzt werden.

- Bei IPv6-Adressbereichen ist üblicherweise ein Präfix und eine Präfixlänge erforderlich.

Fenster mit Anzeige von IP-Adressen

In der Agent-Struktur werden die IPv6-Adressen der Agents in der Spalte **IPv6-Adresse** angezeigt.

Stichwortverzeichnis

A

Agent-Eigenschutz, 9-2
Agent-Server-Kommunikation, 9-15, 10-6
Agent-Struktur, 3-6
    allgemeine Tasks, 3-6
Agent verschieben, 3-12
Apex Central-Integration, 9-12

D

Damage Cleanup Services, 1-3
device control, 8-2
    permissions, 8-2
    storage devices, 8-2

E

Erste Schritte, 3-2

F

Fehlerbehebung
    Agent-Server-Kommunikation, 10-6
File-Reputation-Dienste, 3-17

G

Gerätelisten-Tool, 8-5
Gerätesteuerung, 8-1, 8-2
    Benachrichtigungen, 8-6
    Protokolle, 8-7

H

Herkömmliche Suche, 6-6, 6-7
    Wechseln zur intelligenten Suche, 6-7

I

Integration des Control Managers, 9-12
intelligente Suche, 6-7
    Wechsel von der herkömmlichen Suche, 6-7
Intelligente Suche, 6-6
Internet-Bedrohungen, 7-2
IPv6-Unterstützung, A-2
    Einschränkungen, A-2

K

Komponenten, 3-16
Konfiguration
    Überblick, 3-2

P

permissions
    storage devices, 8-2
Programme, 3-16

S

Smart Feedback, 3-18
Smart Protection
    File-Reputation-Dienste, 3-17
    Web-Reputation-Dienste, 3-17
storage devices
    permissions, 8-2
Suchmethode
    Standard, 6-5
Suchtypen, 6-11
support
    Probleme schneller beheben, 10-11

T

Trojaner, 1-3

U

Unterstützung für IPv6
    Einschränkungen, A-3

V

Viren-/Malware-Suche
    Ergebnisse, 6-42

W

Webkonsole, 3-2
    Über, 3-2
web reputation, 7-2
Web-Reputation-Dienste, 3-17
Widgets, 3-13, 3-16

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: APGM1810082/251127