TREND MICRO™

3.0 TREND MICRO™ Security

Administratorhandbuch

Für Großunternehmen und Mittelbetriebe

für MAC®

Endpoint Security

Protected Cloud

TREND MICRO SMART PROTECTION NETWORK™

Trend Micro Incorporated behält sich das Recht vor, ohne Vorankündigung Änderungen an diesem Dokument und den hierin beschriebenen Produkten vorzunehmen. Lesen Sie vor der Installation und Verwendung der Software die Readme-Dateien, die Anmerkungen zu dieser Version und die neueste Version der zugehörigen Benutzerdokumentation auf der Homepage von Trend Micro unter:

http://docs.trendmicro.com/de-de/enterprise/trend-micro-security-(for-mac).aspx

Trend Micro, das Trend Micro T-Ball-Logo, OfficeScan, 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© 2016 Trend Micro Incorporated. Alle Rechte vorbehalten.

Dokument-Nr.: TSGM37575/160929

Release-Datum: Oktober 2016

In der Benutzerdokumentation für Trend Micro Security (für Mac) werden die wesentlichen Funktionen der Software und Installationsanweisungen für Ihre Produktionsumgebung erläutert. Lesen Sie die Dokumentation vor der Installation und Verwendung der Software aufmerksam durch.

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

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

Bewerten Sie diese Dokumentation auf der folgenden Seite:

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

Inhaltsverzeichnis

Vorwort

Vorwort vii

Trend Micro Security (für Mac) Dokumentation viii

Zielgruppe viii

Textkonventionen ix

Begriff x

Kapitel 1: Einführung in Trend Micro Security (für Mac)

Informationen zu Trend Micro Security (für Mac) 1-2

Neu in dieser Version 1-2

Wichtigste Funktionen und Vorteile 1-5

Trend Micro Security (für Mac) Server 1-7

Trend Micro Security (für Mac) Agent 1-8

Kapitel 2: Server installieren

Server-Installationsvoraussetzungen 2-2

Update-Adresse 2-3

Trend Micro Security (für Mac) Server installieren 2-5

Produkt zum ersten Mal aktivieren 2-7

Tasks nach der Installation auf dem Server ausführen 2-8

Trend Micro Security (für Mac) Server deinstallieren 2-9

Kapitel 3: Erste Schritte

Die Webkonsole 3-2

Webkonsole öffnen 3-2

Sicherheitszusammenfassung 3-3

Agent-Struktur 3-4
Agent-Struktur – Allgemeine Tasks 3-5
Agent-Struktur – Besondere Tasks 3-6

Gruppen 3-8
Gruppen hinzufügen 3-8
Gruppen oder Agents löschen 3-9
Gruppen umbenennen 3-9
Agents verschieben 3-10

Widgets 3-11
Widget für Agent-Konnektivität (Mac) 3-11
Widget für Agent-Updates (Mac) 3-14
Widget für erkannte Sicherheitsrisiken (Mac) 3-15

Trend Micro Smart Protection 3-15
Smart Feedback 3-18

Kapitel 4: Agent installieren

Voraussetzungen für die Installation des Agents 4-2

Methoden und Setup-Dateien zur Agent-Installation 4-2
Auf einem einzelnen Endpunkt installieren 4-4
Auf mehreren Endpunkten mit Hilfe von Apple Remote Desktop installieren 4-9

Vorgänge nach der Agent-Installation 4-12

Agent-Deinstallation 4-14

Kapitel 5: Den Schutz auf dem neuesten Stand halten

Komponenten 5-2

Update-Übersicht 5-4

Server-Update 5-5
Update-Adresse des Servers konfigurieren 5-5
Proxy-Einstellungen für Server-Updates konfigurieren 5-6
Server-Update-Methoden 5-7

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 5-14

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 6-6
Suchmethode ändern 6-7
Wechsel von der intelligenten Suche zur herkömmlichen Suche 6-7
Wechsel von der herkömmlichen Suche zur intelligenten Suche 6-9

Suchtypen 6-12
Echtzeitsuche 6-13
Manuelle Suche 6-14
Zeitgesteuerte Suche 6-16
Jetzt durchsuchen 6-17

Gemeinsame Einstellungen für alle Suchtypen 6-18
Suchkriterien 6-18
Suchaktionen 6-21
Suchausschlüsse 6-26
Zwischenspeicher-Einstellungen für Suchen 6-31

Protokolle zu Suchvorgängen anzeigen 6-33

Benachrichtigungen und Protokolle für Sicherheitsrisiken 6-34
Einstellungen der Administratorbenachrichtigungen konfigurieren 6-34
Benachrichtigungen bei Sicherheitsrisiken für Administratoren konfigurieren 6-35
Ausbruchsbenachrichtigungen für Administratoren konfigurieren 6-36
Sicherheitsrisiko-Protokolle anzeigen 6-38
Zähler für Sicherheitsrisiken zurücksetzen 6-41

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 7-6
Web Reputation-Protokolle anzeigen 7-7

Kapitel 8: Server und Agents verwalten

Agent-Eigenschutz 8-2
Agent-Eigenschutz konfigurieren 8-3
Certified Safe Software Service aktivieren 8-3
Server und Agents aktualisieren 8-4
Server aktualisieren 8-4
Agents aktualisieren 8-6
Protokolle verwalten 8-7
Lizenzen verwalten 8-8
Server-Datenbank sichern 8-10
Serverdatenbank wiederherstellen 8-10
Trend Micro Control Manager 8-11
Control Manager-Integration in dieser Version 8-12
Leistungsindikatoren-Widget 8-13
Agent-Server-Kommunikationseinstellungen konfigurieren 8-16
Inaktive Agents 8-18
Inaktive Agents automatisch entfernen 8-18
Agent-Symbole 8-19

Kapitel 9: Hilfe anzeigen

Fehlerbehebung 9-2
Zugriff auf die Webkonsole 9-2
Server-Deinstallation 9-4

Agent-Installation 9-5
Allgemeiner Agent-Fehler 9-6

Die Knowledge Base von Trend Micro 9-7

Technischer Support 9-7
Ressourcen zur Fehlerbehebung 9-8
Kontaktaufnahme mit Trend Micro 9-9
Verdächtige Inhalte an Trend Micro senden 9-11
Sonstige Ressourcen 9-12

Anhang A: IPv6-Unterstützung in Trend Micro Security (für Mac)

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

IPv6-Voraussetzungen für Trend Micro Security (für Mac) Server A-2

IPv6-Voraussetzungen für Trend Micro Security (für Mac) Agent A-2

Einschränkungen eines reinen IPv6-Servers A-3

Einschränkungen eines reinen IPv6-Agents A-3

IPv6-Adressen konfigurieren A-4

Fenster mit Anzeige von IP-Adressen A-5

Stichwortverzeichnis

Stichwortverzeichnis IN-1

Vorwort

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

Trend Micro Security (für Mac) Dokumentation

Die Dokumentation zu Trend Micro Security (für Mac) umfasst Folgendes:

Dokumentation	Beschreibung
Administratorhandbuch	Ein PDF-Dokument mit Installationsanleitungen für Trend Micro Security (für 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.
Knowledge Base	Eine Online-Datenbank mit Informationen zur Problemlösung und Fehlerbehebung. Sie enthält die aktuellsten Hinweise zu bekannten Softwareproblemen. Die Knowledge Base finden Sie im Internet unter folgender Adresse: http://docs.trendmicro.com/de-de/enterprise/trend-micro-security-(for-mac).aspx

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

http://docs.trendmicro.com/de-de/enterprise/trend-micro-security-(for-mac).aspx

Zielgruppe

Die Dokumentation zu Trend Micro Security (für Mac) richtet sich an folgende Benutzer:

- Trend Micro Security (für Mac) Administratoren: Verantwortlich für die Verwaltung von Trend Micro Security (für Mac), einschließlich Installation und Verwaltung von Server und Agents. Es wird davon ausgegangen, dass diese Benutzer über umfassende Kenntnisse über Netzwerke und Server-Verwaltung verfügen.

- Endbenutzer: Benutzer, die den Trend Micro Security (für Mac) 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 Security (für 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\sample.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 Security (für Mac) Dokumentation verwendet werden:

Begriff	Beschreibung
Agent	Das auf einem Endpunkt installierte Trend Micro Security (für Mac) Agent-Programm
Endpunkt	Computer, auf dem der Agent installiert ist
Agent-Benutzer (oder Benutzer)	Person, die den Agent auf dem Endpunkt verwaltet
Server	Trend Micro Security (für Mac) Server-Programm
Server-Computer	Computer, auf dem der Trend Micro Security (für Mac) Server installiert ist
Administrator (oder Trend Micro Security (für Mac) Administrator)	Person, die den Trend Micro Security (für Mac) Server verwaltet
Konsole	Benutzerschnittstelle zur Konfiguration und Verwaltung der Trend Micro Security (für Mac) Server- und Agent-Einstellungen Die Konsole für das Serverprogramm wird ‚Webkonsole' genannt, die Konsole für den Agent heißt ‚Agent-Konsole'.
Sicherheitsrisiko	Oberbegriff für Viren, Malware, Spyware/Grayware und Internet-Bedrohungen
Produktdienst	Trend Micro Security (für Mac) Dienst, der von der Microsoft Management Console (MMC) aus verwaltet wird
Komponenten	Suchen und entdecken Sicherheitsrisiken und führen Aktionen gegen sie durch.

BEGRIFF	BESCHREIBUNG
`Agent-Installationsordner`	Der Ordner auf dem Endpunkt, der die Trend Micro Security (für Mac) Agent-Dateien enthält. `/Library/Application Support/TrendMicro`
`Server-Installationsordner`	Ordner auf dem Server-Computer, der die Programmdateien des Trend Micro Security (für Mac) Servers enthält Nach der Installation von Trend Micro Security (für Mac) Server wird der Ordner im gleichen Verzeichnis wie der OfficeScan Server-Ordner erstellt. Wenn Sie die Standardeinstellungen bei der Installation von OfficeScan Server übernehmen, ist der Server-Installationsordner einer der folgenden: • `C:\Programme\Trend Micro\OfficeScan\Addon\TMSM` • `C:\Programme (x86)\Trend Micro\OfficeScan\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	Entität, die nur eine IPv4-Adresse hat
Reine IPv6	Entität, die nur eine IPv6-Adresse hat

Kapitel 1

Einführung in Trend Micro Security (für Mac)

Dieses Kapitel stellt eine Einführung in Trend Micro™ Security (für Mac)™ dar und gibt eine Übersicht über die Funktionen und Fähigkeiten.

Informationen zu Trend Micro Security (für Mac)

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

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

Neu in dieser Version

Trend Micro Security (für Mac) bietet die folgenden neuen Funktionen und Verbesserungen:

FUNKTION/ VERBESSERUNG	DETAILS
Intelligente Suche	Trend Micro Security (für Mac) verwendet die intelligente Suche, um den Suchvorgang effizienter zu gestalten. Diese Technologie basiert darauf, dass eine Vielzahl von zuvor auf dem lokalen Endpunkt gespeicherten Signaturen auf Smart Protection Quellen 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 Agents finden Sie unter *Suchmethodentypen auf Seite 6-5*.

Funktion/ Verbesserung	Details
Damage Cleanup Services	Die Damage Cleanup Services™ beseitigen vollautomatisch dateibasierte Viren 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 Security (für Mac) den Benutzer auf, den Endpunkt neu zu starten, um den Vorgang zum Entfernen eines Trojaners abzuschließen.
Liste 'Gesperrt' der Web Reputation	Zu den Verbesserungen von Web Reputation gehört die Liste der gesperrten URLs. Sie können Websites, die Sie als gefährlich einstufen, in die Liste der gesperrten URLs aufnehmen. Wenn auf einem Endpunkt der Trend Micro Security (für Mac) Agent einen Zugriff auf eine dieser Websites erkennt, lehnt er die Verbindung automatisch ab, ohne eine Abfrage an die Smart Protection Quellen zu senden.
Leistungsindikatoren-Dashboard-Widget	Diese Version von Trend Micro Security (für Mac) kann in Control Manager integriert werden, wo Sie eine Bewertungsliste auf dem Control Manager Dashboard bezüglich des Status der Endpunktumgebung anpassen können.

Funktion/ Verbesserung	Details
Agent-Eigenschutz	Der Trend Micro Security (für Mac) Agent implementiert die folgenden Eigenschutzfunktionen: • Verhindert das Entfernen oder Verändern von Trend Micro Security (für Mac)-Agent-Programmdateien oder -ordnern • Verhindert das Sperren von Trend Micro Security (für Mac) Agent-Prozessen
Überwachen von Suchvorgängen	Trend Micro Security (für Mac) bietet mehr Transparenz und Kontrolle über Suchfunktionen durch Folgendes: • Protokolle zu Suchvorgängen Überwachen Sie die Dauer, den Status und die Ergebnisse von Suchvorgängen unter Verwendung der Webkonsole und der Agent-Konsole. • Filtern des Sicherheitsrisiko-Protokolls nach Suchaktionen auf der Agent-Konsole. • Zurücksetzen des Viren/Malware-Zählers für ausgewählte Agents oder Agent-Gruppen.
Externes Laufwerk durchsuchen	Administratoren konfigurieren Agents zum Durchsuchen von Netzwerklaufwerken oder Zeitmaschinen-Laufwerken.
Certified Safe Software Service	Der Certified Safe Software Service fragt Trend Micro Datenzentren ab, um die Sicherheit eines Programms zu überprüfen, das von einer Antiviren-Suche erkannt wurde, und die Wahrscheinlichkeit von falschen Erkennungen reduzieren.
Erweiterte Funktionen für Agent-Updates und Upgrades	Diese Version von Trend Micro Security (für Mac) enthält die folgenden Funktionen für Agent-Updates: • Automatisches Update für Agent: Der Trend Micro Security (für Mac) Server kann aktualisierte Komponenten für Agents bereitstellen, wenn ein Agent-Endpunkt neu gestartet wird oder eine neue Komponente auf dem Server zur Verfügung steht. • Granuläres Agent-Update: Option für das Aktualisieren von Komponenten, ohne ein Upgrade des Agent-Programms durchführen zu müssen.

Funktion/ Verbesserung	Details
Migration von Agents	Administratoren können Trend Micro Security (für Mac) Agents auf einen anderen Trend Micro Security (für Mac) Server migrieren, ohne Trend Micro Security (für Mac) Agents auf Endpunkten neu installieren zu müssen.
Bereitstellung von Agents	Diese Version von Trend Micro Security (für Mac) unterstützt das Bereitstellen von Agents mit Hilfe von Betriebssystem-Images. Wenn Sie den Trend Micro Security (für Mac) Agent in ein Betriebssystem-Image aufnehmen, das auf mehreren Endpunkten bereitgestellt wird, registriert sich der Trend Micro Security (für Mac) Agent nach der Installation automatisch beim Trend Micro Security (für Mac) Server, und die Endpunkte werden geschützt, ohne dass eine manuelle Konfiguration durchgeführt werden muss.
Neues Design der Trend Micro Security (für Mac) Benutzeroberfläche für Agents	Die Trend Micro Security (für Mac) Benutzeroberfläche für Agents wurde neu gestaltet, um ein einfacheres, schlankeres und moderneres Benutzererlebnis zu bieten. Alle der verfügbaren Funktionen der vorherigen Trend Micro Security (für Mac) Client-Version befinden sich noch in der aktualisierten Version.
Verbesserung der Trend Micro Security (für Mac) Serverschnittstelle	Das Hauptmenü der Webkonsole des Trend Micro Security (für Mac) Servers wurde an das Webkonsolenmenü von OfficeScan angepasst, um eine einheitliche Bedienung zu bieten. Alle der verfügbaren Funktionen des vorherigen Trend Micro Security (für Mac) Servers befinden sich noch in der aktualisierten Version.
Browser-Unterstützung	Die Webkonsole des Trend Micro Security (für Mac) Servers unterstützt die folgenden Browser auf unterstützten OS X™- bzw. macOS™-Plattformen: • Chrome • Firefox • Safari

Wichtigste Funktionen und Vorteile

Trend Micro Security (für Mac) bietet die folgenden Funktionen und Vorteile:

TABELLE 1-1. Wichtigste Funktionen und Vorteile

FUNKTION	VORTEILE
Intelligente Suche	Trend Micro Security (für Mac) verwendet die intelligente Suche, um den Suchvorgang effizienter zu gestalten. Diese Technologie basiert darauf, dass eine Vielzahl von zuvor auf dem lokalen Endpunkt gespeicherten Signaturen auf Smart Protection Quellen 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 Agents finden Sie unter *Suchmethodentypen auf Seite 6-5*.
Damage Cleanup Services	Die Damage Cleanup Services™ beseitigen vollautomatisch dateibasierte Viren 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 Security (für Mac) den Benutzer auf, den Endpunkt neu zu starten, um den Vorgang zum Entfernen eines Trojaners abzuschließen.

FUNKTION	VORTEILE
Schutz vor Sicherheitsrisiken	Trend Micro Security (für 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 Security (für 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.
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 OfficeScan 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 Agents im Netzwerk. Über die Webkonsole wird außerdem die automatische Verteilung von Sicherheitsrichtlinien, Pattern-Dateien und Software-Updates auf allen Agents koordiniert. Der Administrator kann das Netzwerk remote verwalten und Einstellungen für einzelne Agents Clients oder Agent-Gruppen vornehmen.

Trend Micro Security (für Mac) Server

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

Der Server erfüllt zwei wichtige Funktionen:

- Überwacht und verwaltet Trend Micro Security (für Mac) Agents

- Lädt von Agents benötigte Komponenten herunter. Standardmäßig lädt der Trend Micro Security (für Mac) Server die Komponenten vom Trend Micro ActiveUpdate Server herunter und stellt sie dann den Agents zur Verfügung.

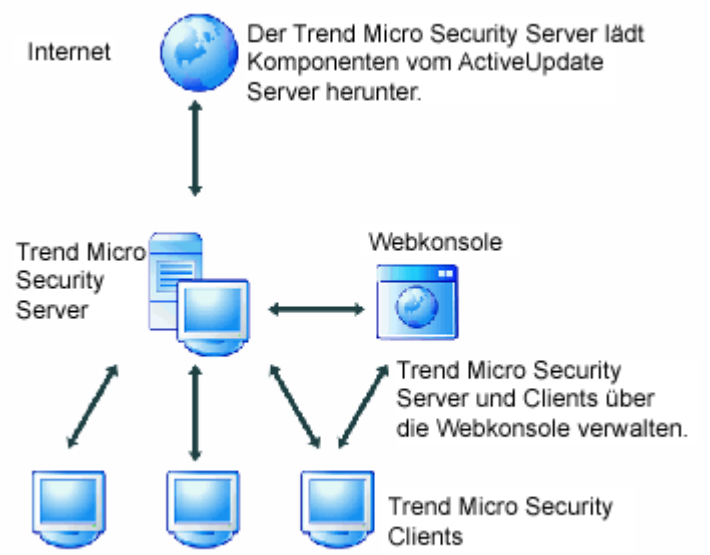


ABBILDUNG 1-1. Funktionsweise von Trend Micro Security (für Mac) Server

Trend Micro Security (für Mac) ermöglicht die bidirektionale Kommunikation zwischen Server und Agents in Echtzeit. Die Verwaltung der Agents erfolgt über eine browserbasierte Webkonsole, die Sie praktisch überall im Netzwerk aufrufen können. Server und Agent kommunizieren über das Protokoll ActiveMQ™.

Trend Micro Security (für Mac) Agent

Schützen Sie Ihre Endpunkte vor Sicherheitsrisiken, indem Sie den Trend Micro Security (für Mac) Agent auf jedem Endpunkt installieren. Der Agent stellt drei Suchmethoden zur Verfügung:

- Echtzeitsuche
- Zeitgesteuerte Suche
- Manuelle Suche

Der Agent berichtet an den übergeordneten Trend Micro Security (für Mac) Server, von dem aus er installiert wurde. Der Agent sendet Ereignis- und Statusinformationen in Echtzeit an den Server. Agents kommunizieren mit dem Server über das Protokoll ActivMQ.

Kapitel 2

Server installieren

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

Server-Installationsvoraussetzungen

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

TABELLE 2-1. Server-Installationsvoraussetzungen

RESSOURCE	VORAUSSETZUNGEN
OfficeScan server	10.6 oder höher
Plug-in Manager	2.0 und höher
RAM	Mindestens 1 GB, 2 GB empfohlen

Verfügbarer Speicherplatz	• Mindestens 1,5 GB, wenn der OfficeScan Server auf dem Systemlaufwerk installiert wird (in der Regel Laufwerk C:)
	• Falls der OfficeScan Server nicht auf dem Systemlaufwerk installiert wird:
	  • Mindestens 600 MB auf dem Laufwerk, auf dem der OfficeScan Server installiert wird. Der Trend Micro Security (für Mac) Server wird auf diesem Laufwerk installiert.
	  • Mindestens 900 MB auf dem Systemlaufwerk. Vom Trend Micro Security (für Mac) Server genutzte Programme von Drittanbietern werden auf diesem Laufwerk installiert.

RESSOURCE	VORAUSSETZUNGEN

Andere	• Microsoft™ .NET Framework 3.0 SP2 oder 3.5 SP1
	• Microsoft Windows™ Installer 3.1 und höher
	• Java Runtime Environment™ (JRE) 1.7 oder höher mit dem aktuellsten Update
	
	Hinweis
	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.
	
	• Die folgenden Programme anderer Hersteller werden automatisch installiert, wenn sie nicht vorhanden sind:
	  • Microsoft SQL Server 2005 oder 2008 R2 Express
	  • Apache™ ActiveMQ 5.14.0
	  • Microsoft Visual C++ 2005 Redistributable

Update-Adresse

Bevor Sie Trend Micro Security (für Mac) Server installieren, überprüfen Sie die Update-Adresse von Plug-in Manager in der OfficeScan 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 OfficeScan. 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 Security (für 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 Security (für Mac) enthält. Wenden Sie sich an Ihren Support-Anbieter, um Unterstützung beim Einrichten einer Intranet-Adresse zu erhalten.

Trend Micro Security (für Mac) Server installieren

Prozedur

1. Führen Sie Folgendes NUR dann aus, wenn Sie Trend Micro Security (für Mac) auf einem Server mit einer Domänencontroller-Rolle installieren:

   - Installieren Sie Trend Micro Security (für Mac) auf einem OfficeScan 10.6 Server:

     a. Erstellen Sie eine Textdatei mit folgendem Inhalt:

     ```
     [SQLSERVER2005]
     SQLACCOUNT="NT AUTHORITY\SYSTEM"
     [SQLSERVER2008]
     SQLSVCACCOUNT="NT AUTHORITY\SYSTEM"
     ```

     b. Speichern Sie die Datei unter `InstallCfgFile.ini` im Ordner `...OfficeScan\PCCSRV\Admin\Utility\SQL`.

   - Installieren Sie Trend Micro Security (für Mac) auf einem OfficeScan 11.0 Server:

     a. Wechseln Sie in den Ordner `...OfficeScan\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 OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.

3. Klicken Sie im Abschnitt **Trend Micro Security (für Mac)** auf **Download**.

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

Plug-in Manager lädt das Paket nach `<OfficeScan Server-Installationsordner>\PCCSRV\Download` herunter.

`<OfficeScan Server-Installationsordner>` ist meistens `C:\Programme\Trend Micro\OfficeScan`.

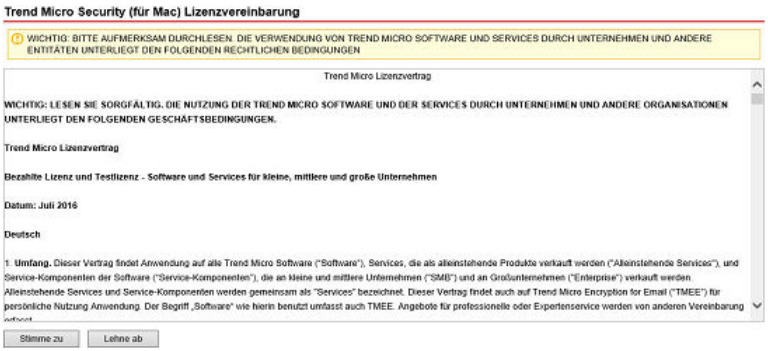
4. Verfolgen Sie den Download-Fortschritt.

   Sie können während des Downloads zu anderen Fenstern navigieren.

   Wenn beim Herunterladen des Pakets Probleme auftreten, überprüfen Sie über die 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 Security (für Mac) zu installieren.

6. Lesen Sie die Lizenzvereinbarung durch und nehmen Sie die Bedingungen durch Klicken auf **Stimme zu** an.



   Die Installation beginnt.

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

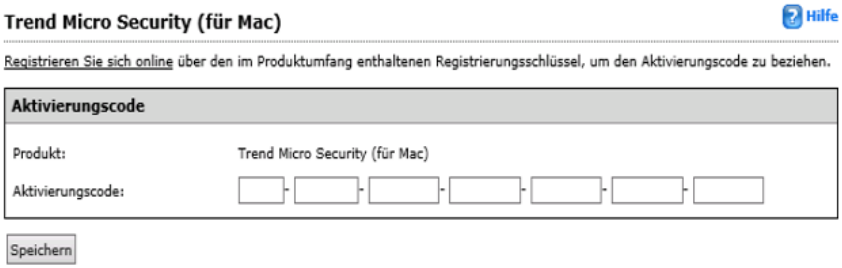
Produkt zum ersten Mal aktivieren

Prozedur

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

2. Navigieren Sie zum Bereich **Trend Micro Security (für 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 Trend Micro Security**
   - **SQL Server (TMSM)**
   - **Trend Micro Security für (Mac)**
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 Security (für Mac) Serverdateien im <*Server-Installationsordner*> befinden.

Trend Micro Security (für Mac) Server deinstallieren

Prozedur

1. Öffnen Sie die OfficeScan Webkonsole und klicken Sie im Hauptmenü auf **Plug-ins**.
2. Klicken Sie im Abschnitt Trend Micro Security (für Mac) auf **Deinstallieren**.
3. Verfolgen Sie den Deinstallationsfortschritt. Sie können während der Deinstallation zu anderen Fenstern navigieren. Nach Abschluss der Deinstallation kann der Trend Micro Security (für Mac) Server wieder installiert werden.

Hinweis

Die von Trend Micro Security (für 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 Security (für Mac) und Einstellungen für die Erstkonfiguration beschrieben.

Die Webkonsole

Die Webkonsole ist die zentrale Stelle zur Überwachung von Trend Micro Security (für Mac) Agents und zur Konfiguration der Einstellungen, die von den 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:

- Auf Endpunkten installierte Agents verwalten
- Agents zur gleichzeitigen Konfiguration und Verwaltung in logische Gruppen organisieren
- Auf einem oder mehreren Endpunkten die Virensucheinstellungen festlegen und die Suche starten
- Benachrichtigungen über Sicherheitsrisiken konfigurieren und die von Agents gesendeten Protokolle anzeigen
- 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 × 768 bei 256 Farben oder mehr
- Web browser:
  - Microsoft Internet Explorer 8.0, Microsoft Edge oder höhere Versionen
  - Firefox
  - Chrome
  - Safari

Prozedur

1. Geben Sie im Webbrowser die URL des OfficeScan Servers ein.
2. Geben Sie den Benutzernamen und das Kennwort ein, um sich am OfficeScan Server anzumelden.
3. Klicken Sie im Hauptmenü auf **Plug-in Manager**.
4. Navigieren Sie zum Bereich **Trend Micro Security (für Mac)** und klicken Sie auf **Programm verwalten**.

Sicherheitszusammenfassung

Das Fenster **Zusammenfassung** wird angezeigt, wenn Sie die Webkonsole von Trend Micro Security (für Mac) öffnen oder im Hauptmenü auf **Zusammenfassung** klicken.

Tipp

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

Agents

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

- Status der Verbindung zwischen allen Agents und dem Trend Micro Security (für Mac) Server: Durch Klicken auf einen Link wird die Agent-Struktur geöffnet, über die Sie Einstellungen für die 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 einen oder mehrere Agents aus, klicken Sie auf **Protokolle** > **Sicherheitsrisiko-Protokolle**, und geben Sie die Protokollkriterien an.

Überprüfen Sie im daraufhin angezeigten Fenster die Spalte **Ergebnisse**, um zu erkennen, ob die Suchaktionen bei den Sicherheitsrisiken erfolgreich durchgeführt wurden.

Eine Liste aller Suchergebnisse finden Sie unter *Suchergebnis auf Seite 6-39*.

- Wählen Sie einen oder mehrere 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 7-6*.

Update-Status

In der Tabelle **Update-Status** sind Informationen über die Komponenten von Trend Micro Security (für Mac) und das 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 die Agent-Upgrades auf die aktuellste Programmversion bzw. den aktuellsten Build, wenn Sie kürzlich den Server aktualisiert haben.

  Eine Anleitung für Agent-Upgrades finden Sie unter *Server und Agents aktualisieren auf Seite 8-4*.

Agent-Struktur

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

Menüeinträge über der Agent-Struktur, um eine Konfiguration gleichzeitig für alle 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** (

), 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	TASK
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 6-17*.

MENÜSCHALTFLÄCHE	TASK

Einstellungen	• Konfigurieren Sie die Suchmethode.
	Weitere Informationen finden Sie unter *Suchmethodentypen auf Seite 6-5*.
	• Sucheinstellungen konfigurieren.
	  • *Manuelle Suche auf Seite 6-14*
	  • *Echtzeitsuche auf Seite 6-13*
	  • *Zeitgesteuerte Suche auf Seite 6-16*
	  • *Suchausschlüsse auf Seite 6-26*
	  • *Zwischenspeicher-Einstellungen für Suchen auf Seite 6-31*
	• 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 8-3*.
	• Aktualisierungseinstellungen konfigurieren.
	Weitere Informationen finden Sie unter *Agent-Update-Einstellungen konfigurieren auf Seite 5-12*.

Protokolle	Sehen Sie Protokolle ein und setzen Sie Statistiken zurück. • *Sicherheitsrisiko-Protokolle anzeigen auf Seite 6-38* • *Web Reputation-Protokolle anzeigen auf Seite 7-7* • *Protokolle zu Suchvorgängen anzeigen auf Seite 6-33* • *Zähler für Sicherheitsrisiken zurücksetzen auf Seite 6-41*
Agent-Struktur verwalten	Trend Micro Security (für Mac) Gruppen verwalten. Weitere Informationen finden Sie unter *Gruppen auf Seite 3-8*.

Gruppen

Eine Gruppe in Trend Micro Security (für Mac) umfasst eine Gruppe von Agents mit derselben Konfiguration, die die gleichen Tasks ausführen. Durch die Übersicht der Agents in Gruppen kann die Konfiguration für alle Agents einer Gruppe gleichzeitig konfiguriert, verwaltet und angewandt werden.

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.

Gruppen oder Agents löschen

Vorbereitungen

Vergewissern Sie sich vor dem Löschen einer Gruppe, ob in dieser noch Agents enthalten sind, und verschieben Sie diese wenn nötig in eine andere Gruppe.

Details zum Verschieben von Agents finden Sie unter *Agents in eine andere Gruppe verschieben auf Seite 3-10*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Wählen Sie in der Agent-Struktur bestimmte Gruppen oder Agents auf.
3. Klicken Sie auf **Agent-Struktur verwalten** > **Gruppe/Agent entfernen**.
4. Klicken Sie auf **OK**, um den Löschvorgang 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.

Agents verschieben

Sie können Agents in eine andere Gruppe oder auf einen anderen Trend Micro Security (für 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-Struktur 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**.

Agents auf einen anderen Server verschieben

Hinweis

Sie können Agents nur auf einen anderen Trend Micro Security (für Mac)-Server mit derselben oder einer höheren Version verschieben.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Wählen Sie in der Agent-Struktur mindestens einen Agent aus.
3. Klicken Sie auf **Agent-Struktur verwalten** > **Agent verschieben**.
4. Wählen Sie **Ausgewählte Agents auf anderen Server verschieben:**.
5. Geben Sie den Servernamen oder die IPv4-/IPv6-Adresse und die HTTP-Portnummer ein.
6. Wählen Sie **Verschieben von Offline-Agents erzwingen**, um Offline-Agents auf den angegebenen Server zu verschieben.

   Hinweis

   Wenn ein Offline-Agent nicht nach 7 Tagen online ist, bleibt der Offline-Agent auf dem ursprünglichen Server und wird nicht auf den angegebenen Server verschoben.

7. Klicken Sie auf **Verschieben**.

Widgets

Sie verwalten Trend Micro Security (für Mac) Widgets auf dem OfficeScan Dashboard. Die Widgets stehen sofort nach der Aktivierung von Trend Micro Security (für Mac) zur Verfügung.

Um Widgets anzeigen zu können, müssen OfficeScan Version 10.6 oder höher und Plug-in Manager Version 1.5 oder höher installiert sein.

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

Widget für Agent-Konnektivität (Mac)

Das Widget für Agent-Konnektivität (Mac) zeigt den Status der Verbindung zwischen den Agents und dem Trend Micro Security (für Mac) Server an. Die 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 Security (für Mac) anzuzeigen. Anschließend können Sie Tasks für diese Agents starten oder ihre Einstellungen ändern.

Widget für Agent-Konnektivität (Mac) als Kreisdiagramm

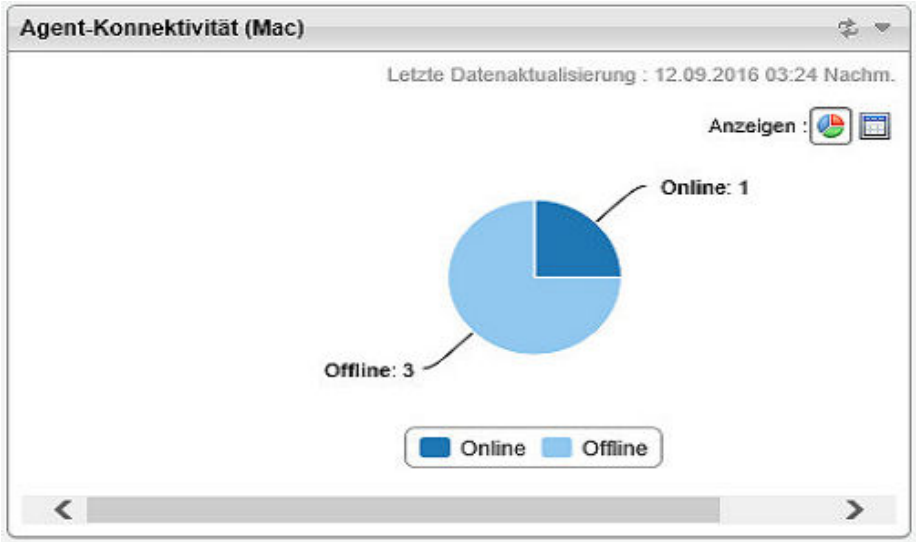
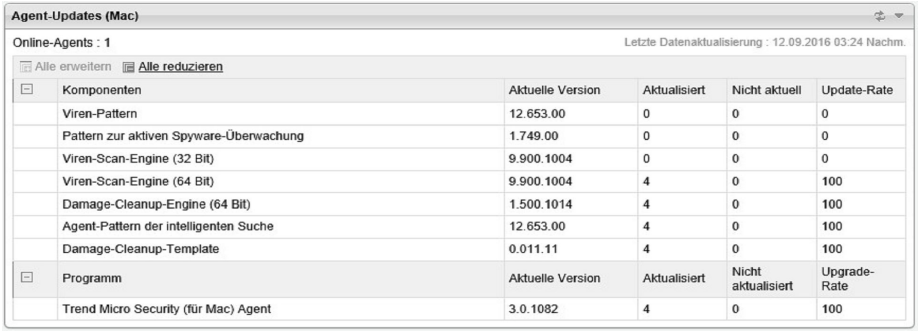


ABBILDUNG 3-2. Widget für Agent-Konnektivität (Mac) als Kreisdiagramm

Das Kreisdiagramm zeigt die Anzahl der im jeweiligen Status befindlichen Agents an, stellt aber keine Links zur Agent-Struktur von Trend Micro Security (für 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 : 1 — Letzte Datenaktualisierung : 12.09.2016 03:24 Nachm.

Alle erweitern | Alle reduzieren

Komponenten	Aktuelle Version	Aktualisiert	Nicht aktuell	Update-Rate
Viren-Pattern	12.653.00	0	0	0
Pattern zur aktiven Spyware-Überwachung	1.749.00	0	0	0
Viren-Scan-Engine (32 Bit)	9.900.1004	0	0	0
Viren-Scan-Engine (64 Bit)	9.900.1004	4	0	100
Damage-Cleanup-Engine (64 Bit)	1.500.1014	4	0	100
Agent-Pattern der intelligenten Suche	12.653.00	4	0	100
Damage-Cleanup-Template	0.011.11	4	0	100
Programm	**Aktuelle Version**	**Aktualisiert**	**Nicht aktualisiert**	**Upgrade-Rate**
Trend Micro Security (für Mac) Agent	3.0.1082	4	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 Security (für 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.

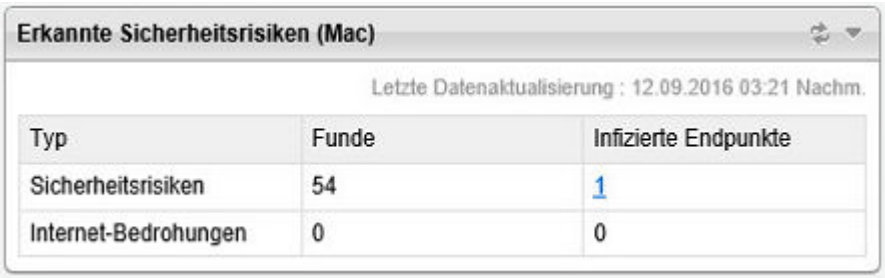


ABBILDUNG 3-4. Widget für erkannte Sicherheitsrisiken (Mac)

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 Security (für 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-Dienste

Smart Protection Services beinhaltet:

- **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.

  Weitere Informationen finden Sie unter *Web Reputation auf Seite 7-2*.

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

  Weitere Informationen finden Sie unter *Smart Feedback auf Seite 3-18*.

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 Agents

Externe Agents (d. h. Agents ohne funktionsfähige Verbindung mit dem Trend Micro Security (für Mac) Server) 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 Agents

Interne Agents (d. h. Agents mit funktionsfähiger Verbindung zum Trend Micro Security (für Mac) 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 Agents

Bei dieser Option senden Trend Micro Security (für Mac) Agents Abfragen an Smart Protection Server, die für OfficeScan Clients konfiguriert wurden.

Sie ist erst ab OfficeScan Version 10.6 SP3 Patch 1 Critical Patch oder höher verfügbar.

Wenn auf Ihrem Trend Micro Security (für Mac) Server eine frühere Version von OfficeScan installiert ist, aktualisieren Sie OfficeScan auf Version 10.6 oder höher.

Wenn Sie bereits mit OfficeScan 10.6 oder höher arbeiten, lesen Sie die folgenden Richtlinien, um 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 Trend Micro Security (für Mac) Server 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

Diese Option kann nicht aktiviert werden, wenn der Trend Micro Security (für Mac) Server mit OfficeScan 10.6 installiert wurde. Wenn Sie diese Option in der Richtlinienverwaltung von Control Manager aktivieren und anschließend einem mit OfficeScan 10.6 installierten Trend Micro Security (für Mac) Server bereitstellen, 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 stets ein aktueller Schutz gewährleistet 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:

- Dateiprüfsummen
- Dateiinformationen, einschließlich Größen 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.

Weitere Informationen zum Smart Protection Network finden Sie unter:

http://www.trendmicro.de/technologie-innovationen/technologie/smart-protection-network/

Kapitel 4

Agent installieren

Dieses Kapitel beschreibt Anforderungen und Vorgehensweisen für die Installation von Trend Micro Security (für Mac) Agent.

Informationen zum Aktualisieren des Agents finden Sie unter *Server und Agents aktualisieren auf Seite 8-4*.

Voraussetzungen für die Installation des Agents

Nachfolgend sind die Systemvoraussetzungen für die Installation des Trend Micro Security (für Mac) Agents auf einem Endpunkt aufgeführt.

TABELLE 4-1. Voraussetzungen für die Installation des Agents

RESSOURCE	VORAUSSETZUNG
Betriebssystem	• macOS™ Sierra 10.12 • OS X™ El Capitan 10.11 • OS X™ Yosemite 10.10 oder höher • OS X™ Mavericks 10.9 oder höher • OS X™ Mountain Lion 10.8.3 oder höher • OS X™ Lion 10.7.5 oder höher (nur 64-Bit)
Hardware	• **Prozessor**: Intel® Core™-Prozessor • **RAM**: Mindestens 512MB • **Verfügbarer Speicherplatz**: Mindestens 300MB

Hinweis

Diese Produktversion unterstützt Mac OS X Snow Leopard™ 10.6.8 oder frühere Versionen nicht mehr. Falls Agents unter Mac OS X Snow Leopard installiert sind, aktualisieren Sie die Agents nicht, und stellen Sie sicher, dass ein Server mit Trend Micro Security (für Mac) 2.0 SP1 zur Verwaltung dieser Agents vorhanden ist.

Methoden und Setup-Dateien zur Agent-Installation

Sie haben folgende Möglichkeiten, um den Trend Micro Security (für Mac) Agent zu installieren:

- Installation auf einem einzelnen Endpunkt durch Starten des Installationspakets (`tmsminstall.zip`) auf dem Endpunkt
- Installation auf verschiedenen Endpunkten durch Starten des Installationspakets (`tmsminstall.mpkg.zip`) über Apple Remote Desktop
- Sie können die Installation auf mehreren Endpunkten vornehmen, indem Sie ein Betriebssystem-Image installieren, das den Trend Micro Security (für Mac) Agent enthält. Nach der Installation registriert sich der Trend Micro Security (für Mac) Agent automatisch bei dem Trend Micro Security (für Mac) Server.

Hinweis

Informationen zum Upgrade von Agents finden Sie unter *Server und Agents aktualisieren auf Seite 8-4*.

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

Es gibt zwei Möglichkeiten, das Paket zu beziehen:

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

  Hinweis

  Die Links zu den Agent-Deinstallationspaketen werden ebenfalls in diesem Fenster angezeigt. Verwenden Sie diese Pakete zum Entfernen des Agent-Programms von den Endpunkten. Wählen Sie das Paket je nach Version des Agent-Programms, das Sie entfernen möchten.

  Informationen zur Deinstallation des Trend Micro Security (für Mac) Agents finden Sie unter *Agent-Deinstallation auf Seite 4-14*.

- Wechseln Sie zu <*Server-Installationsordner*>`TMSM_HTML\ActiveUpdate\ClientInstall\`.

Auf einem einzelnen Endpunkt installieren

Die Installation des Trend Micro Security (für Mac) Agents 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 Agents 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 4-2*.

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:

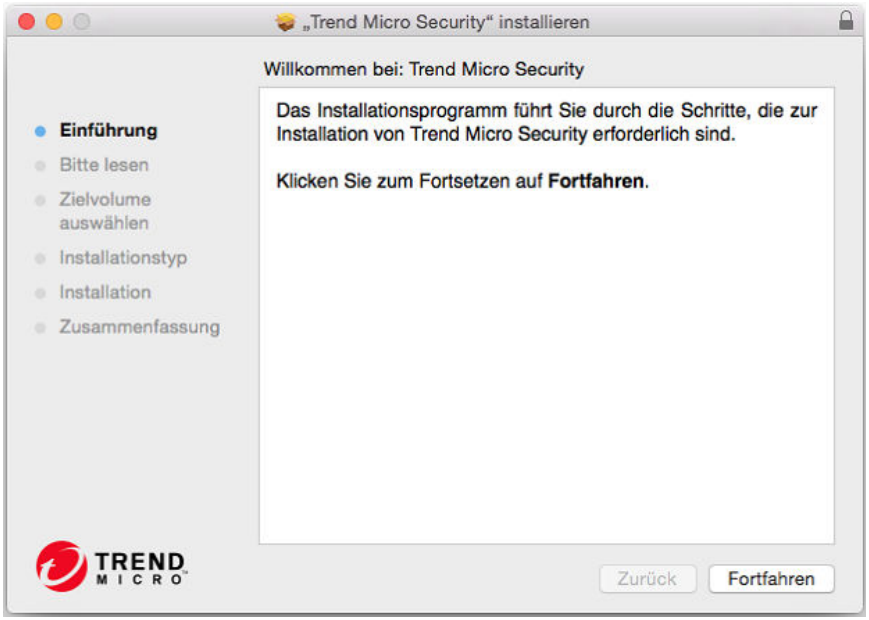
   ```
   ditto -xk users/mac/Desktop/tmsminstall.zip users/mac/Desktop
   ```

   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 **Fortfahren**.

6. Klicken Sie im Einführungsfenster auf **Fortfahren**.



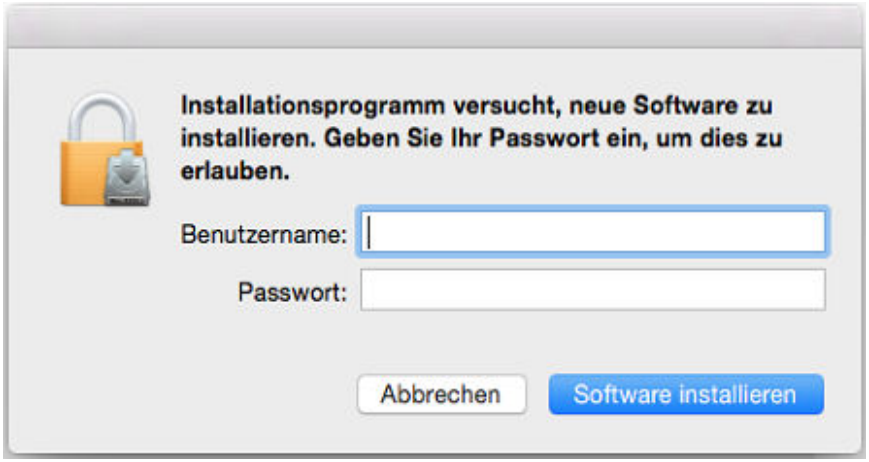
7. Lesen Sie die Erinnerungsnachrichten und klicken Sie auf **Weiter**.

8. Klicken Sie im Fenster Installationstyp auf **Installieren**.

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. Klicken Sie nach erfolgreicher Installation auf **Schließen**, um die Installation abzuschließen.

Der Agent registriert sich automatisch an dem Server, von dem das Agent-Installationspaket heruntergeladen wurde. Außerdem aktualisiert sich der Agent zum ersten Mal.

Nächste Maßnahme

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

Auf mehreren Endpunkten mit Hilfe von Apple Remote Desktop installieren

Die Installation des Trend Micro Security (für Mac) Agents auf mehreren Endpunkten kann mit Hilfe von Apple Remote Desktop vereinfacht werden.

Hinweis

Falls Endpunkte nur eine IPv6-Adresse besitzen, lesen Sie die IPv6-Einschränkungen für die Agent-Bereitstellung mit Apple Remote Desktop in *Einschränkungen eines reinen IPv6-Agents auf Seite A-3* durch.

Prozedur

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

   Weitere Informationen zum Erhalt des Pakets finden Sie unter *Methoden und Setup-Dateien zur Agent-Installation auf Seite 4-2*.
3. Kopieren Sie `tmsminstall.mpkg.zip` mit Apple Remote Desktop auf den Endpunkt, und starten Sie es dann über das integrierte Archivierungsprogramm.

Warnung!

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

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

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

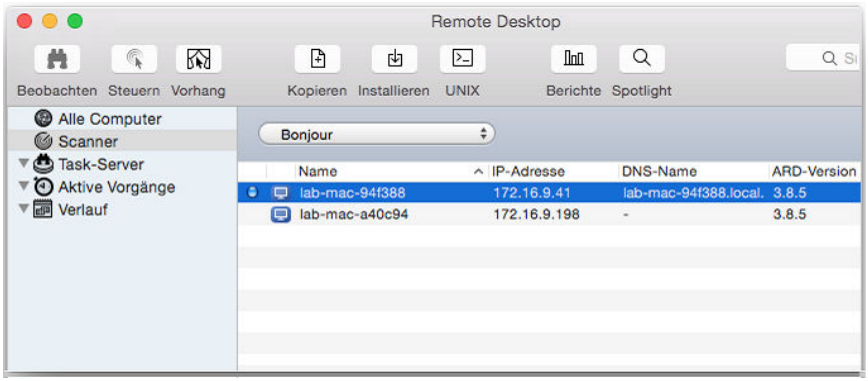
Zum Beispiel:

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

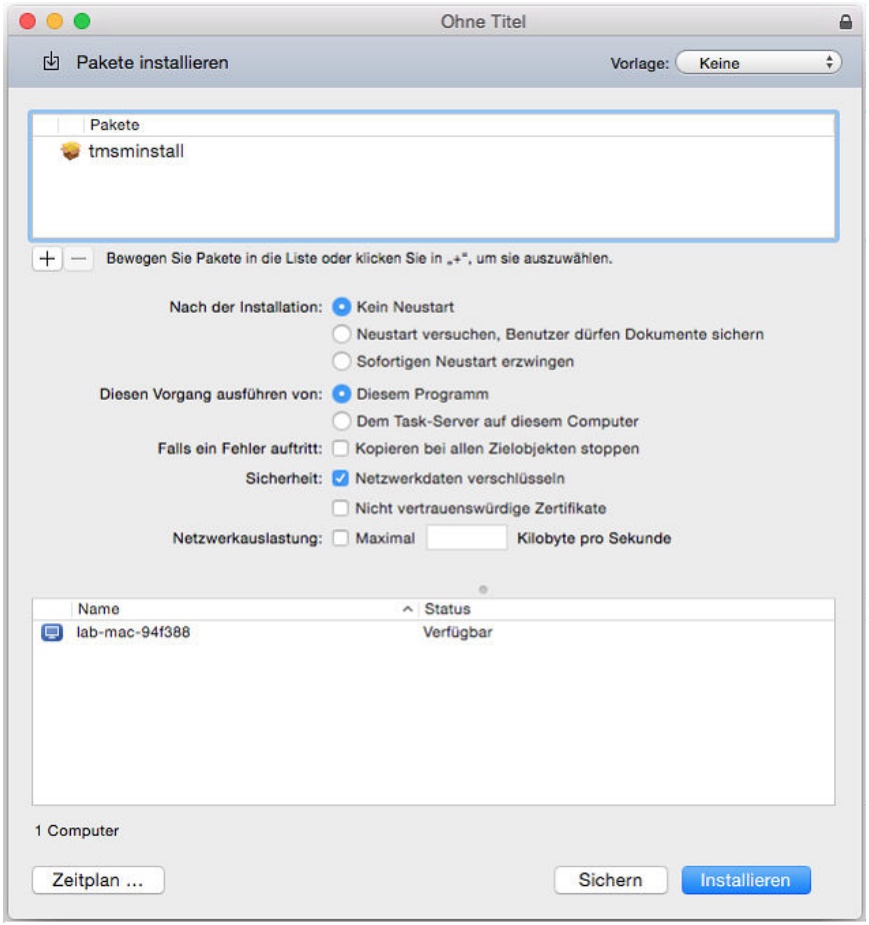
Durch Starten des Pakets `tmsminstall.mpkg.zip` wird die Datei `tmsminstall.mpkg` extrahiert.

4. Öffnen Sie Apple Remote Desktop auf dem Endpunkt.

5. Wählen Sie die Endpunkte aus, auf denen Sie den Trend Micro Security (für Mac) Agent installieren möchten, und klicken Sie auf **Installieren**.



6. Ziehen Sie das Installationspaket ins Fenster Pakete installieren, oder klicken Sie auf ‚+', um das Installationspaket zu suchen.

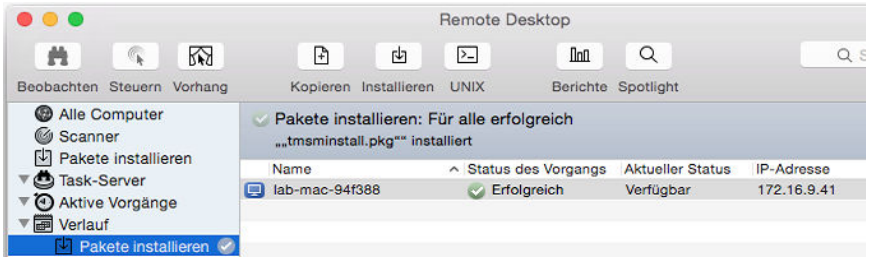


7. (Optional) Klicken Sie auf **Speichern**, um die Installation automatisch auf allen neuen Endpunkten durchzuführen, die mit dem Netzwerk verbunden sind.

8. Klicken Sie auf **Installieren**.

   Der Apple Remote Desktop beginnt mit der Installation des Agents auf den ausgewählten Endpunkten. Nach erfolgreicher Installation auf allen Endpunkten wird die Meldung `Pakete installieren: Für alle erfolgreich`

angezeigt. Andernfalls erscheint die Meldung `Erfolgreich` unter **Task-Status** auf jedem Endpunkt, auf dem die Installation ordnungsgemäß durchgeführt wurde.



Die Agents registrieren sich automatisch an dem Server, von dem das Agent-Installationspaket heruntergeladen wurde. Außerdem aktualisieren sich die Agents zum ersten Mal.

Nächste Maßnahme

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

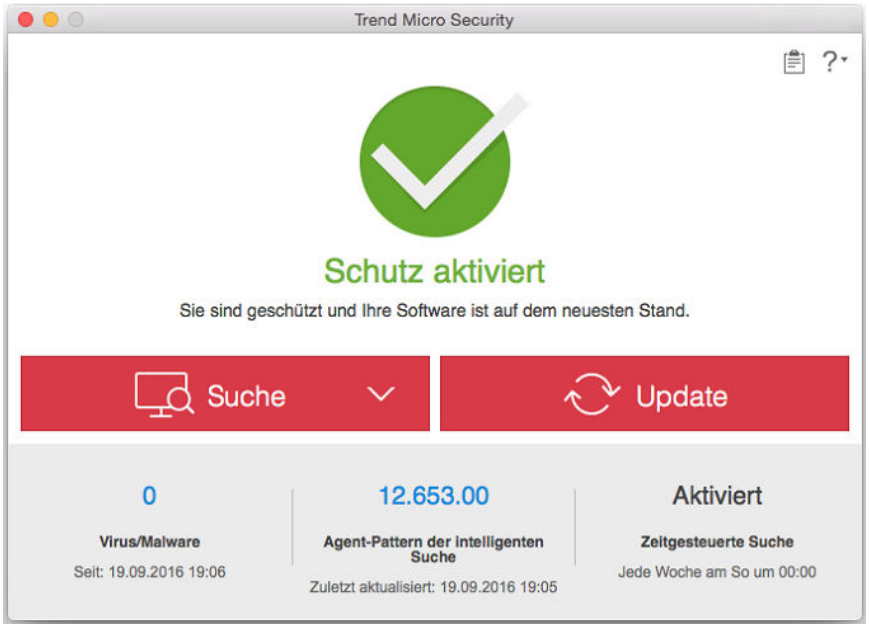
Vorgänge nach der Agent-Installation

Prozedur

1. Überprüfen Sie Folgendes:

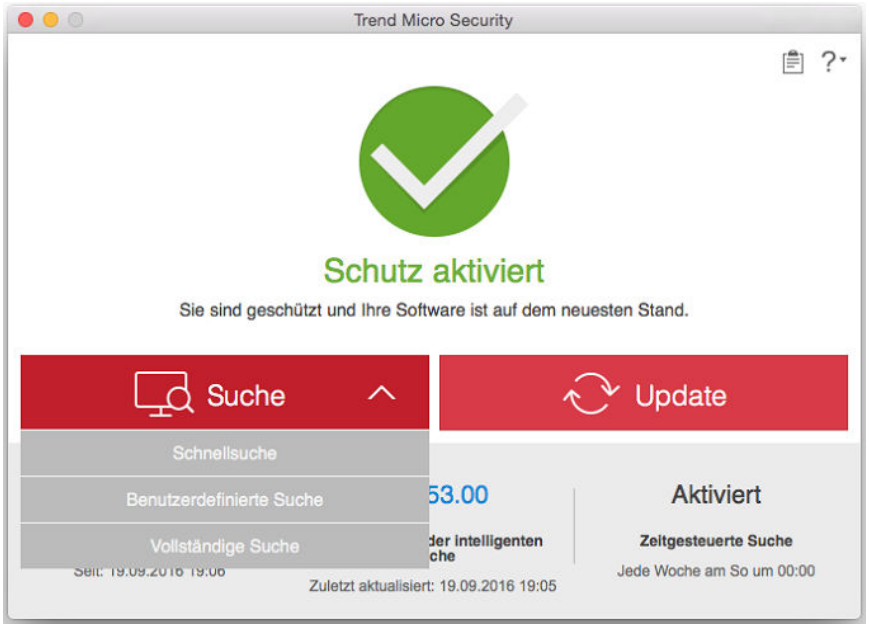
   - Das Symbol für den Trend Micro Security (für Mac) Agent ( ) wird in der Menüleiste des Endpunkts angezeigt.
   - Die Agent-Dateien von Trend Micro Security (für Mac) befinden sich im <*Agent-Installationsordner*>.
   - Der Agent wird in der Agent-Struktur der Webkonsole angezeigt. Klicken Sie im Hauptmenü auf **Agent-Verwaltung**, um die Agent-Struktur anzuzeigen.

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



Wenn der 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.

3. Starten Sie eine manuelle Suche auf dem Endpunkt.



Nächste Maßnahme

Wenn nach der Installation des Agents Probleme auftreten, deinstallieren Sie ihn und installieren Sie ihn erneut.

Agent-Deinstallation

Deinstallieren Sie den Agent nur, wenn Probleme mit dem Programm auftreten. Installieren Sie ihn anschließen umgehend neu, damit Ihr Endpunkt wieder vor Sicherheitsrisiken geschützt ist.

Prozedur

1. Laden Sie das Agent-Deinstallationspaket `tmsmuninstall.mpkg.zip` vom Trend Micro Security (für Mac) Server herunter. Navigieren Sie in der Webkonsole

von Trend Micro Security (für Mac) 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. Klicken Sie nach erfolgreicher Deinstallation auf **Schließen**, um die Deinstallation abzuschließen.

Nächste Maßnahme

Melden Sie den Agent vom Server ab.

1. Klicken Sie in der Webkonsole auf **Agent-Verwaltung** und wählen Sie den deinstallierten Agent aus.

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 Security (für Mac) Komponenten und Update-Verfahren erläutert.

Komponenten

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

KOMPONENTE	BESCHREIBUNG
Agent-Programm	Das Trend Micro Security (für Mac) Agent-Programm bietet den eigentlichen Schutz vor Sicherheitsrisiken.
Damage-Cleanup-Engine (64 Bit)	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.
Agent-Pattern der intelligenten Suche	Die Pattern-Datei, die der Agent zum Identifizieren von Bedrohungen verwendet. Diese Pattern-Datei wird auf dem Agent-Endpunkt gespeichert.
Spyware-Aktivmonitor-Pattern	Das Spyware-Aktivmonitor-Pattern enthält Informationen, mit denen Trend Micro Security (für Mac) Spyware und Grayware erkennt.

KOMPONENTE	BESCHREIBUNG
Viren-Scan-Engine (32 Bit/64 Bit)	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 Security (für 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 Security (für Mac) Server die aktualisierten Komponenten herunter.

Der Trend Micro Security (für 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 werden verschiedene Optionen für Komponenten-Updates für die Trend Micro Security (für Mac) Server und Agents beschrieben:

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

UPDATE-OPTION	BESCHREIBUNG
ActiveUpdate Server Trend Micro Security (für Mac) Server Agents	Der Trend Micro Security (für 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 die Agents.
ActiveUpdate Server Agents	Trend Micro Security (für Mac) Agents erhalten die aktualisierten Komponenten direkt vom ActiveUpdate Server, wenn sie keine Verbindung zum Trend Micro Security (für Mac) Server herstellen können.

Server-Update

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

- Viren-Pattern
- Spyware-Aktivmonitor-Pattern
- Viren-Scan-Engine (32 Bit/64 Bit)
- Damage-Cleanup-Engine (64 Bit)
- Damage-Cleanup-Template
- Agent-Pattern der intelligenten Suche

Sie können die aktuellen Versionen der Komponenten in der Webkonsole im Übersichtsfenster anzeigen und die Anzahl der 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 Security (für 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-3*.

Nach dem Download verfügbarer Updates benachrichtigt der Server automatisch die Agents, damit diese die Updates ihrer Komponenten durchführen. Ist das Komponenten-Update kritisch, sollte der Server die Agents umgehend benachrichtigen.

Die entsprechenden Einstellungen nehmen Sie unter **Agents** > **Agent-Verwaltung** > **Tasks** > **Aktualisieren** vor.

Prozedur

1. Navigieren Sie zu **Updates** > **Server** > **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 Security (für 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.
     - Updates von Control Manager können Sie durch Eingabe der HTTP-Adresse von Control Manager beziehen.
3. Klicken Sie auf **Speichern**.

Proxy-Einstellungen für Server-Updates konfigurieren

Sie können den Trend Micro Security (für 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-3*.

Prozedur

1. Gehen 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 **Speichern**.

Server-Update-Methoden

Sie können das Update der Komponenten von Trend Micro Security (für 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 Security (für 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 Security (für 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** > **Server** > **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 Security (für Mac) das Update durchführt. Trend Micro Security (für 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 Security (für Mac) das Update am letzten Tag des Monats durch.
4. Klicken Sie auf **Speichern**.

Server manuell aktualisieren

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

Prozedur

1. Navigieren Sie zu **Updates** > **Server** > **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 Agents vor den neuesten Sicherheitsrisiken geschützt sind, müssen Sie die Agent-Komponenten regelmäßig aktualisieren. Aktualisieren Sie die Agents auch, wenn die Komponenten stark veraltet sind oder ein Ausbruch auftritt. Komponenten veralten stark, wenn der Agent seine Komponenten über einen längeren Zeitraum nicht über den Trend Micro Security (für Mac) Server oder den ActiveUpdate Server aktualisieren kann.

Agent-Update-Methoden

Es gibt mehrere Möglichkeiten, Agent-Updates durchzuführen.

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

UPDATE-METHODE	BESCHREIBUNG
Automatisches Update	• Nachdem ein Server-Update abgeschlossen ist, wird der Agent umgehend zum Update aufgefordert. Weitere Informationen finden Sie unter *Automatisches Update des Agents konfigurieren auf Seite 5-11*. • Die Updates können anhand eines von Ihnen konfigurierten Zeitplans durchgeführt werden. Der konfigurierte Zeitplan kann auf eine(n) oder auf mehrere Agents oder Domänen oder auf alle vom Server verwalteten Agents angewendet werden. 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-Adressen

Standardmäßig laden Agents die Komponenten vom Trend Micro Security (für Mac) Server herunter. Zusätzlich zu den Komponenten erhalten Trend Micro Security (für Mac) Agents beim Update vom Trend Micro Security (für Mac) Server auch aktualisierte Konfigurationsdateien. Agents benötigen diese Konfigurationsdateien, um neue Einstellungen zu übernehmen. Bei jeder Änderung der Einstellungen für Trend Micro Security (für Mac) in der Webkonsole ändern sich auch die Konfigurationsdateien.

Überprüfen Sie, ob der Trend Micro Security (für Mac) Server über die neuesten Komponenten verfügt, bevor Sie die Agents aktualisieren.

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

Sie können einen, mehrere oder alle Agents so konfigurieren, dass sie Komponenten vom Trend Micro ActiveUpdate Server herunterladen, wenn der Trend Micro Security (für Mac) Server nicht verfügbar sein sollte.

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

Hinweis

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

Hinweise und Erinnerungen für Agent-Updates

- Trend Micro Security (für Mac) Agents können auch Proxy-Einstellungen für Updates verwenden. Proxy-Einstellungen werden über die Agent-Konsole konfiguriert.
- Während eines Updates zeigt das Symbol für Trend Micro Security (für Mac) in der Menüleiste des Endpunkts den laufenden Aktualisierungsvorgang an. Ist ein Upgrade für das Agent-Programm verfügbar, führen die 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.
- Überprüfen Sie im Übersichtsfenster, ob alle Agents aktualisiert wurden.

Automatisches Update des Agents konfigurieren

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

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

Der Trend Micro Security (für Mac) Server kann Online-Agents per Benachrichtigung auffordern, Komponenten zu aktualisieren, wenn er die neuesten Komponenten heruntergeladen hat. Offline-Agents werden benachrichtigt, sobald sie neu gestartet wurden und sich wieder mit dem Server verbinden. Sie können nach dem Update optional die Funktion **Jetzt durchsuchen** (manuelle Suche) auf Trend Micro Security (für Mac) Agent-Endpunkten durchführen.

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

TABELLE 5-2. Ereignisbedingtes Update

OPTION	BESCHREIBUNG
Komponenten-Update auf Agents direkt initiieren, nachdem der Server eine neue Komponente heruntergeladen hat	Der Server benachrichtigt die Agents, eine Aktualisierung durchzuführen, sobald er ein Update abgeschlossen hat.
Komponenten-Update von Agents nach dem Neustarten und Verbinden mit dem Server initiieren lassen	Verpasst ein Agent ein Update, lädt dieser die Komponenten herunter, sobald eine Verbindung mit dem Server hergestellt wurde. Ein Agent kann ein Update verpassen, wenn er offline ist, oder wenn der Endpunkt, auf dem der Agent installiert ist, nicht hochgefahren ist.

Hinweis

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

3. Klicken Sie auf **Speichern**.

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 Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für Updates**.

4. Wählen Sie **Agents laden Updates vom Trend Micro ActiveUpdate Server, wenn sie keine Verbindung zum Trend Micro Security (für Mac) Server herstellen können**, um es externen Agents zu ermöglichen, Updates vom Trend Micro ActiveUpdate Server herunterzuladen.

Hinweis

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

5. Wählen Sie **Agents können Komponenten aktualisieren, nicht jedoch das Agent-Programm upgraden oder Hotfixes installieren** aus, um Komponenten-Updates durchzuführen, aber ein Upgrade des Trend Micro Security (für Mac) Agents 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 Trend Micro Security (für Mac) Server die 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 Agents zum Update auf. Mit dieser Einstellung wird verhindert, dass sich alle Agents gleichzeitig zum festgelegten Zeitpunkt mit dem Server verbinden, damit es zu keiner Überlastung des Servers kommt.

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

   - **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.

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. Klicken Sie im Bereich **Update-Status** auf den Link in der Spalte **Nicht aktuell**.

   Die Agent-Struktur wird geöffnet, und es werden alle Agents angezeigt, die aktualisiert werden müssen.
3. Wählen Sie die Agents aus, die Sie aktualisieren möchten.
4. Klicken Sie auf **Tasks** > **Update**.

   Das Update wird auf allen Agents durchgeführt, die die Benachrichtigung erhalten. Auf Endpunkten zeigt das Symbol für Trend Micro Security (für Mac) in der Menüleiste den laufenden Aktualisierungsvorgang an. Bis zum Abschluss des Updates können keine Tasks über die Konsole gestartet werden.

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 in der Agent-Struktur auf das Stammdomänensymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Tasks** > **Update**.

   Das Update wird auf allen Agents durchgeführt, die die Benachrichtigung erhalten. Auf Endpunkten zeigt das Symbol für Trend Micro Security (für Mac) in der Menüleiste den laufenden Aktualisierungsvorgang an. Bis zum Abschluss des Updates können keine Tasks über die Konsole gestartet werden.

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 Security (für 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 Security (für 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 Security (für 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 Security (für 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

Bei der Suche nach Sicherheitsrisiken können Trend Micro Security (für Mac) Agents eine von zwei Suchmethoden anwenden. die intelligente Suche und die herkömmliche Suche.

- **Intelligente Suche**

  Agents, die die intelligente Suche anwenden, werden in diesem Dokument als „Agents mit intelligenter Suche“ bezeichnet. Agents mit intelligenter Suche profitieren von der lokalen Suche und von webbasierten Abfragen, die die File-Reputation-Dienste ermöglichen.

- **Herkömmliche Suche**

  Agents, die keine intelligente Suche anwenden, werden als „Agents mit herkömmlicher Suche“ bezeichnet. Ein Agent mit herkömmlicher Suche speichert alle Trend Micro Security (für Mac) Komponenten auf dem Agent-Endpunkt und durchsucht die Dateien lokal.

Standard-Suchmethode

Wenn Trend Micro Security (für Mac) auf einem Server mit OfficeScan 10.6 SP3 P1 Critical Patch oder höher installiert ist, ist die intelligente Suche die Standard-Suchmethode für Neuinstallationen.

Wenn Trend Micro Security (für Mac) auf einem Server mit einer Version von OfficeScan, die früher als Version 10.6 SP3 P1 Critical Patch ist, installiert ist, ist die herkömmliche Suche die Standard-Suchmethode für Neuinstallationen.

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	In dieser und allen früheren Versionen von Trend Micro Security (für Mac) verfügbar.	Verfügbar ab Trend Micro Security (für Mac) 3.0.
Suchverhalten	Die herkömmliche Suche agent durchsucht den lokalen endpoint.	• Der intelligente Suchagent durchsucht den lokalen Endpunkt. • Wenn der Agent das Risiko der Datei während der Suche nicht ermitteln kann, überprüft er dies, indem er eine Suchabfrage an die Smart Protection Quelle sendet. • Der Agent legt die Suchabfrageergebnisse zur Verbesserung der Suchleistung in einem Zwischenspeicher ab.
Verwendete und aktualisierte Komponenten	Alle unter der Update-Adresse verfügbaren Komponenten, außer 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 Security (für Mac) Server	Trend Micro Security (für Mac) Server

Suchmethode ändern

Prozedur

1. Navigieren Sie zu **Agents** > **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Suchmethoden**.
4. Wählen Sie **Herkömmliche Suche** oder **Intelligente Suche**.
5. Wenn Sie Gruppe(n) oder Agent(s) 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 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.

Wechsel von der intelligenten Suche zur herkömmlichen Suche

Die folgende Tabelle enthält weitere Überlegungen zur Umstellung von Agents auf die herkömmliche Suche:

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

ÜBERLEGUNG	DETAILS
Anzahl der Agents, die umgeschaltet werden sollen	Wenn Sie eine relativ kleine Anzahl von Agents gleichzeitig umschalten, werden Trend Micro Security (für Mac) Server- und Smart Protection Server-Ressourcen effizient genutzt. Diese Server können andere kritische Aufgaben ausführen, während Agents ihre Suchmethoden ändern.
Timing	Wenn Sie wieder auf die herkömmliche Suche umschalten, werden die Agents wahrscheinlich die vollständige Version des Viren-Patterns und des Spyware-Aktivmonitor-Patterns vom Trend Micro Security (für 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 Agents über den Server geplant ist.

Überlegung	Details
Einstellungen der Agent-Struktur	Die Suchmethode ist eine granuläre Einstellung, die auf Stamm- oder Domänenebene oder für einzelne Agents festgelegt werden kann. Bei der Umschaltung zur herkömmlichen Suche können Sie Folgendes tun: • Erstellen Sie eine neue Gruppe, und ordnen Sie die herkömmliche Suche als Suchmethode zu. Alle Agents, die Sie in diese Gruppe verschieben, werden die herkömmliche Suche verwenden. Wenn Sie den 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 Agents konfiguriert haben.

Wechsel von der herkömmlichen Suche zur intelligenten Suche

Wenn Sie Agents von der herkömmlichen Suche auf die intelligente Suche umstellen, stellen Sie sicher, dass die Smart Protection Dienste auf dem OfficeScan Server eingerichtet sind. Details finden Sie in der Dokumentation zu OfficeScan.

Die folgende Tabelle enthält weitere Überlegungen zur Umstellung von Agents auf die intelligente 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 OfficeScan Server aktiviert haben und die Lizenzen nicht abgelaufen sind: • Antivirus • Web Reputation und Spyware-Schutz
Trend Micro Security (für Mac) Server	Stellen Sie sicher, dass die Agents eine Verbindung zum Trend Micro Security (für Mac) Server herstellen können. Nur Online-Agents erhalten die Benachrichtigung, die intelligente Suche zu aktivieren. Offline-Agents erhalten die Benachrichtigung erst dann, wenn sie wieder online gehen. Roaming-Agents werden benachrichtigt, wenn sie wieder online gehen, oder, falls der Agent über Berechtigungen für zeitgesteuerte Updates verfügt, wenn das zeitgesteuerte Update ausgeführt wird. Vergewissern Sie sich auch, dass der Trend Micro Security (für Mac) Server über die neuesten Komponenten verfügt, da die Agents der intelligenten Suche das Agent-Pattern der intelligenten Suche vom Server herunterladen müssen. Informationen zum Update von Komponenten finden Sie unter *Server-Update auf Seite 5-5*.
Anzahl der Agents, die umgeschaltet werden sollen	Wenn Sie eine relativ kleine Anzahl von Agents gleichzeitig umschalten, werden die Ressourcen von Trend Micro Security (für Mac) effizient genutzt. Der Trend Micro Security (für Mac) Server kann weitere kritische Aufgaben ausführen, während Agents ihre Suchmethode ändern.

Überlegung	Details
Timing	Wenn Sie zum ersten Mal auf die intelligente Suche umschalten, müssen Agents die vollständige Version des Agent-Patterns der intelligenten Suche vom Trend Micro Security (für Mac) Server herunterladen. Das Pattern der intelligenten Suche wird nur von Agents der intelligenten Suche verwendet. Die Umschaltung sollte bei geringem Netzaufkommen durchgeführt werden, um sicherzustellen, dass der Download-Prozess in kurzer Zeit beendet wird. Außerdem sollten Sie dann umschalten, wenn keine Aktualisierung eines Agents über den Server geplant ist.
Einstellungen der Agent-Struktur	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 Agents, die Sie in diese Gruppe verschieben, werden die intelligente Suche verwenden. Wenn Sie den 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 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 Agents konfiguriert haben.

ÜBERLEGUNG	DETAILS
Unterstützung für IPv6	Die Agents der intelligenten Suche senden Suchanfragen an Smart Protection Quellen. Ein reiner IPv6-Agent der intelligenten Suche kann Anfragen 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 mit intelligenter Suche ebenfalls keine Anfragen an reine IPv6 Smart Protection Server senden. Ein Dual-Stack-Proxy-Server wie DeleGate, der IP-Adressen konvertieren kann, muss ermöglichen, dass Agents mit intelligenter Suche eine Verbindung zu den Quellen herstellen können.

Suchtypen

Trend Micro Security (für Mac) bietet die folgenden Suchtypen, mit denen Endpunkte vor Sicherheitsrisiken geschützt werden können:

SUCHTYP	BESCHREIBUNG
Echtzeitsuche	Beim Empfangen, Öffnen, Herunterladen, Kopieren oder Ändern einer Datei wird diese automatisch durchsucht. Weitere Informationen erhalten Sie unter *Echtzeitsuche auf Seite 6-13*.

SUCHTYP	BESCHREIBUNG
Manuelle Suche	Eine vom Benutzer gestartete Suche, bei der eine oder mehrere vom Benutzer angegebene Dateien durchsucht werden. Weitere Informationen erhalten Sie unter *Manuelle Suche auf Seite 6-14*.
Zeitgesteuerte Suche	Dateien auf dem Endpunkt werden automatisch gemäß dem vom Administrator festgelegten Zeitplan durchsucht. Weitere Informationen erhalten Sie unter *Zeitgesteuerte Suche auf Seite 6-16*.
Jetzt durchsuchen	Eine vom Administrator gestartete Suche, bei der Dateien auf einem oder mehreren Zielendpunkten durchsucht werden. Weitere Informationen erhalten Sie unter *Jetzt durchsuchen auf Seite 6-17*.

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 Security (für Mac) kein Sicherheitsrisiko erkennt, verbleibt die Datei an ihrem Speicherort und Benutzer können darauf zugreifen. Wenn Trend Micro Security (für Mac) ein Sicherheitsrisiko entdeckt, wird eine Nachricht mit dem Namen der infizierten Datei und dem jeweiligen Sicherheitsrisiko angezeigt.

Konfigurieren Sie die Einstellungen der Echtzeitsuche und wenden Sie sie auf einen oder mehrere Agents und Gruppen oder auf alle vom Server verwalteten Agents an.

Einstellungen für Echtzeitsuche konfigurieren

Prozedur

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

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

4. Folgende Suchkriterien konfigurieren:

   - *Benutzerdefinierte Aktionen für Dateien auf Seite 6-18*
   - *Sucheinstellungen auf Seite 6-19*

5. Klicken Sie auf die Registerkarte **Aktion** , um die Suchaktionen zu konfigurieren, die Trend Micro Security (für Mac) bei entdeckten Sicherheitsrisiken durchführen soll.

   Details zu den Suchoptionen finden Sie unter *Suchaktionsoptionen und zusätzliche Einstellungen auf Seite 6-23*.

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

   - **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.

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.

Konfigurieren Sie die Einstellungen der manuellen Suche und wenden Sie sie auf einen oder mehrere Agents und Gruppen oder auf alle vom Server verwalteten Agents an.

Einstellungen für manuelle Suche konfigurieren

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für manuelle Suche**.
4. Folgende Suchkriterien konfigurieren:
   - *Sucheinstellungen auf Seite 6-19*
   - *CPU-Auslastung auf Seite 6-21*
5. Klicken Sie auf die Registerkarte **Aktion** , um die Suchaktionen zu konfigurieren, die Trend Micro Security (für Mac) bei entdeckten Sicherheitsrisiken durchführen soll.

   Details zu den Suchoptionen finden Sie unter *Suchaktionsoptionen und zusätzliche Einstellungen auf Seite 6-23*.
6. Wenn Sie Gruppen oder Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die ausgewählten Gruppen oder Agents anzuwenden. Wenn Sie auf das Stammsymbol () geklickt haben, haben Sie folgende Optionen:
   - **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.

Zeitgesteuerte Suche

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

Konfigurieren Sie die Einstellungen der zeitgesteuerten Suche und wenden Sie sie auf einen oder mehrere Agents und Gruppen oder auf alle vom Server verwalteten Agents an.

Einstellungen für zeitgesteuerte Suche konfigurieren

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für zeitgesteuerte Suche**.
4. Aktivieren Sie das Kontrollkästchen, um die zeitgesteuerte Suche zu aktivieren.
5. Folgende Suchkriterien konfigurieren:
   - *Zeitplan auf Seite 6-21*
   - *Suchziel auf Seite 6-19*
   - *Sucheinstellungen auf Seite 6-19*
   - *CPU-Auslastung auf Seite 6-21*
6. Klicken Sie auf die Registerkarte **Aktion** , um die Suchaktionen zu konfigurieren, die Trend Micro Security (für Mac) bei entdeckten Sicherheitsrisiken durchführen soll.

   Details zu den Suchoptionen finden Sie unter *Suchaktionsoptionen und zusätzliche Einstellungen auf Seite 6-23*.

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

   - **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.

Jetzt durchsuchen

"Jetzt durchsuchen" wird per Fernzugriff durch einen Administrator für Trend Micro Security (für 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

Jetzt durchsuchen verwendet alle Einstellungen der zeitgesteuerten Suche mit Ausnahme des Zeitplans. Zum Konfigurieren der Einstellungen vor dem Start von Jetzt durchsuchen befolgen Sie die Schritte in *Einstellungen für zeitgesteuerte Suche konfigurieren auf Seite 6-16*.

Prozedur

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

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

3. Klicken Sie auf **Tasks** > **Jetzt durchsuchen**.

Gemeinsame Einstellungen für alle Suchtypen

Konfigurieren Sie für alle Sucharten drei Einstellungsgruppen: Suchkriterien, Suchausschlüsse und Suchaktionen. Verteilen Sie diese Einstellungen auf einen oder mehrere Agents und Gruppen oder auf alle vom Server verwalteten Agents.

Suchkriterien

Geben Sie an, welche Dateien ein bestimmter Suchtyp durchsuchen soll. Verwenden Sie dafür Dateiattribute wie Dateityp und Dateierweiterung. Geben Sie auch die Bedingungen an, die die Suche auslösen sollen. Konfigurieren Sie z. B. die Echtzeitsuche so, dass jede Datei durchsucht wird, die auf den Endpunkt heruntergeladen wird.

Benutzerdefinierte Aktionen für Dateien

Wählen Sie Aktivitäten für Dateien aus, die die Echtzeitsuche auslösen. Wählen Sie unter folgenden Optionen:

- **Dateien durchsuchen, die erstellt/bearbeitet werden**: Durchsucht Dateien, die dem Endpunkt neu hinzugefügt werden (z. B. nach dem Herunterladen einer Datei) oder gerade verändert werden.
- **Dateien durchsuchen, die abgerufen/ausgeführt werden:** Durchsucht Dateien beim Öffnen.
- **Dateien durchsuchen, die erstellt/bearbeitet und abgefragt/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.

Suchziel

Wählen Sie unter folgenden Optionen:

- **Alle durchsuchbaren Dateien**: Alle Dateien durchsuchen
- **Von IntelliScan durchsuchte Dateitypen**: Durchsucht nur Dateien, die potenziell bösartigen Code enthalten, selbst wenn dieser sich hinter einer scheinbar harmlosen Erweiterung verbirgt.
- **Datei- oder Ordnername mit vollständigem Pfad**: Durchsucht nur die angegebene(n) Datei(en) in einem bestimmten Ordner.

  1. Geben Sie einen vollständigen Dateipfad oder einen Verzeichnispfad ein und klicken Sie auf **Hinzufügen**.

     - Beispiel eines vollständigen Dateipfads: `/Benutzer/Benutzername/temp.zip`
     - Beispiel eines Verzeichnispfads: `/Benutzer/Benutzername`

  2. Zum Löschen eines Verzeichnispfads oder eines vollständigen Pfads wählen Sie ihn aus und klicken auf **Entfernen**.

Sucheinstellungen

Aktivieren Sie mindestens eine der folgenden Optionen:

- **Komprimierte Dateien durchsuchen**: Trend Micro Security (für Mac) kann einzelne Dateien innerhalb von komprimierten Dateien durchsuchen. Trend Micro Security (für Mac) unterstützt die folgenden Komprimierungstypen:

ERWEITERUNG	TYP
.zip	Mit Pkzip erstelltes Archiv
.rar	Mit RAR erstelltes Archiv

ERWEITERUNG	TYP
.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
.bz2	Mit Unix BZ2 Bzip komprimierte Datei
.uu	UUEncode
.ace	WinAce

- **Zeitmaschine durchsuchen**: Ermöglicht Trend Micro Security (für Mac) das Erkennen und Durchsuchen von Zeitmaschinen-Laufwerken.

Hinweis

Nach der Aktivierung der Option **Zeitmaschine durchsuchen** für die manuelle und zeitgesteuerte Suche kann Trend Micro Security (für Mac) Malwarebedrohungen nur erkennen. Aufgrund von Berechtigungseinschränkungen im Mac-Betriebssystem können keine entsprechenden Aktionen (bereinigen, in Quarantäne verschieben oder löschen) ergriffen werden. Alle konfigurierten Aktionen werden in den Produktprotokollen als nicht erfolgreich angezeigt.

- **Netzlaufwerke durchsuchen**: Durchsucht Netzlaufwerke oder Ordner, die dem Endpunkt zugeordnet sind.

- **Zeitgesteuerte Suche überspringen, wenn die Akkulebensdauer eines drahtlosen Endpunkts weniger als __ % beträgt und das Netzteil nicht angeschlossen ist**: Trend Micro Security (für Mac) überspringt eine zeitgesteuerte Suche, wenn festgestellt wird, dass die Akkulebensdauer eines drahtlosen Endpunkts niedrig ist 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.

CPU-Auslastung

Trend Micro Security (für Mac) kann nach dem Durchsuchen einer Datei und vor dem Durchsuchen der nächsten eine Pause einlegen. Diese Einstellung wird für die manuelle Suche, die zeitgesteuerte Suche und Jetzt durchsuchen verwendet.

Wählen Sie unter folgenden Optionen:

- **Hoch**: Keine Pause zwischen den einzelnen Suchläufen
- **Niedrig**: Pause zwischen den einzelnen Dateisuchläufen

Zeitplan

Stellen Sie ein, wie oft (täglich, wöchentlich oder monatlich) und wann die zeitgesteuerte Suche durchgeführt werden soll.

Wenn Sie für die monatliche zeitgesteuerte Suche den 29., 30. oder 31. Tag des Monats ausgewählt haben, dieser Tag im betreffenden Monat jedoch nicht vorkommt, führt Trend Micro Security (für Mac) die zeitgesteuerte Suche am letzten Tag des Monats durch.

Suchaktionen

Geben Sie die Aktion an, die Trend Micro Security (für Mac) durchführen soll, wenn ein bestimmter Suchtyp ein Sicherheitsrisiko erkannt hat.

Die Aktion, die von Trend Micro Security (für Mac) ausgeführt wird, ist abhängig vom Suchtyp, der das Sicherheitsrisiko erkannt hat. Wenn beispielsweise bei der manuellen

Suche (Suchtyp) ein Sicherheitsrisiko von Trend Micro Security (für Mac) erkannt wird, wird die infizierte Datei gesäubert (Aktion).

Trend Micro Security (für Mac) kann die folgenden Aktionen gegen Sicherheitsrisiken durchführen:

SUCHAKTION	DETAILS
Löschen	Trend Micro Security (für Mac) entfernt die infizierte Datei vom Endpunkt.
Quarantäne	Die infizierte Datei wird von Trend Micro Security (für Mac) umbenannt und in das Quarantäneverzeichnis des Endpunkts (<*Agent-Installationsordner*>`/common/lib/vsapi/quarantine`) verschoben. Nachdem die Datei in das Quarantäneverzeichnis verschoben wurde, kann Trend Micro Security (für Mac) weitere Aktionen für diese Datei durchführen, je nachdem, welche Aktion vom Benutzer angegeben wurden. Trend Micro Security (für 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.
Säubern	Trend Micro Security (für Mac) entfernt das Sicherheitsrisiko aus einer infizierten Datei und ermöglicht dann erst den Zugriff auf die Datei. Lässt sich die Datei nicht säubern, führt Trend Micro Security (für 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**.

Suchaktion	Details
Übergehen	Trend Micro Security (für Mac) führt keine Aktion an der infizierten Datei aus. Das erkannte Sicherheitsrisiko wird jedoch in den Protokolldateien verzeichnet. Die Datei wird nicht verschoben. Trend Micro Security (für 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 „Wahrscheinlich Virus/Malware“ ein tatsächliches Sicherheitsrisiko darstellt, wird ein neues Pattern veröffentlicht, damit Trend Micro Security (für Mac) die entsprechende Suchaktion durchführen kann. Wenn sich wahrscheinliche Viren/Malware als unbedenklich herausstellen, werden diese nicht mehr entdeckt. Zum Beispiel: Trend Micro Security (für Mac) entdeckt in der Datei „123.pdf“ das Sicherheitsrisiko „x_wahrscheinlicher_Virus“ und führt zum Zeitpunkt der Erkennung keine Aktion aus. 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 Trend Micro Security (für Mac) „x_wahrscheinlicher_Virus“ als Trojaner und löscht „123.pdf“, wenn für Trojaner die Aktion „Löschen“ festgelegt wurde.

Suchaktionsoptionen und zusätzliche Einstellungen

Wählen Sie für die Einstellung der Suchaktion unter folgenden Optionen:

Option	Details
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.

OPTION	DETAILS
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 zweite Aktion an, die Trend Micro Security (für Mac) durchführen soll, 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 6-21*.

Zusätzliche Einstellungen für Echtzeitsuche

EINSTELLUNG	DETAILS
Bei Erkennung eines Sicherheitsrisikos Benachrichtigung anzeigen	Erkennt Trend Micro Security (für Mac) während der Echtzeitsuche ein Sicherheitsrisiko, kann dem Benutzer eine entsprechende Benachrichtigung angezeigt werden.

Zeitgesteuerte Suche – Berechtigungen

Wenn auf dem Endpunkt die zeitgesteuerte Suche aktiviert ist, kann sie vom Benutzer übersprungen und angehalten werden.

BERECHTIGUNG	DETAILS
Zeitgesteuerte Suche verschieben	Ein Benutzer mit der Berechtigung „Zeitgesteuerte Suche verschieben“ darf folgende Aktionen durchführen: • Der Benutzer kann die zeitgesteuerte Suche vor der Ausführung verschieben und die Dauer der Verschiebung angeben. Ein zeitgesteuerte Suche kann nur einmal verschoben werden. • Wenn die zeitgesteuerte Suche bereits ausgeführt wird, kann sie durch den Benutzer angehalten und zu einem späteren Zeitpunkt neu gestartet werden. Anschließend gibt der Benutzer an, wie viel Zeit bis zum Neustart der Suche verstreichen soll. Wenn die Suche neu startet, werden alle vorher durchsuchten Dateien erneut durchsucht. Die zeitgesteuerte Suche kann nur einmal angehalten 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 anhalten	Mit dieser Berechtigung darf ein Benutzer folgende Aktionen durchführen: • zeitgesteuerte Suche vor der Ausführung überspringen • zeitgesteuerte Suche während der Ausführung anhalten

Zusätzliche Einstellungen für zeitgesteuerte Suche

Einstellung	Details
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 Agent bricht die Suche ab, sobald der angegebene Zeitraum erreicht wird, auch wenn die Suche noch nicht vollständig ist. Der Agent informiert den Benutzer umgehend über etwaige bei der Suche erkannte Sicherheitsrisiken.

Suchausschlüsse

Konfigurieren Sie die Suchausschlüsse, um die Suchleistung zu verbessern und bekannte Dateien zu überspringen, die keinen Schaden anrichten können. Beim Ausführen eines bestimmten Suchtyps überprüft Trend Micro Security (für Mac) die Ausschlussliste, um die Dateien auf dem Endpunkt zu bestimmen, die von der Suche ausgeschlossen werden.

Ausschlussliste	Details
Dateien	Trend Micro Security (für Mac) wird eine Datei nicht durchsuchen, wenn: • 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

AUSSCHLUSSLISTE	DETAILS
Dateierweiterungen	Trend Micro Security (für Mac) wird eine Datei nicht durchsuchen, wenn ihre Erweiterung einer der Erweiterungen in der Ausschlussliste entspricht.

Ausschlusslisten für die Suche konfigurieren

Details zu Ausschlusslisten für die Virensuche finden Sie unter *Suchausschlüsse auf Seite 6-26*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für den Suchausschluss**.
4. Aktivieren Sie das Kontrollkästchen, um den Suchausschluss zu aktivieren.
5. So konfigurieren Sie die **Ausschlussliste für Virensuche (Dateien)**

   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`

PFAD	BEISPIELE FÜR DIE VERWENDUNG VON PLATZHALTERZEICHEN

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 „user“ enden, etwa „end_user“ oder „new_user“.

b. Um einen Pfad zu löschen, wählen Sie ihn aus und klicken Sie auf **Entfernen**.

6. So konfigurieren Sie die **Ausschlussliste für Virensuche (Dateierweiterungen)**

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

   - **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.

Zwischenspeicher-Einstellungen für Suchen

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

- Ist dies der Fall, durchsucht der Agent die Datei und fügt sie dem Zwischenspeicher für durchsuchte Dateien hinzu.

- Wurde die Datei nicht geändert, sieht der Agent nach, ob sich die Datei im Zwischenspeicher für durchsuchte Dateien befindet.

  - Wenn sie dort vorhanden ist, wird sie bei der Suche übersprungen.

  - Wenn sie sich nicht im Zwischenspeicher für durchsuchte Dateien befindet, sieht der Agent im Zwischenspeicher für genehmigte Dateien nach.

Hinweis

Der Zwischenspeicher für genehmigte Dateien enthält alle Dateien, die von Trend Micro Security (für 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 die Datei im Zwischenspeicher für genehmigte Dateien vorhanden ist, wird sie bei der Suche übersprungen.
- Ist dies nicht der Fall, durchsucht der 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 *Zwischenspeicher-Einstellungen für Suchen auf Seite 6-31*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol (), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Zwischenspeicher-Einstellungen für Suchen**.
4. Wählen Sie **Zwischenspeicher der On-Demand-Suche aktivieren**.

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

   - **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.

Protokolle zu Suchvorgängen anzeigen

Wenn die manuelle oder zeitgesteuerte Suche ausgeführt wird, erstellt der Trend Micro Security (für Mac) Agent ein Suchprotokoll mit Informationen über die Suche. Sie können über die Trend Micro Security (für Mac) Server- oder die Trend Micro Security (für Mac) Agent-Konsole das Suchprotokoll anzeigen.

Prozedur

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

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 8-7*.

Benachrichtigungen und Protokolle für Sicherheitsrisiken

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

Trend Micro Security (für Mac) erstellt Protokolldateien, wenn Sicherheitsrisiken entdeckt werden.

Einstellungen der Administratorbenachrichtigungen konfigurieren

Wenn Sicherheitsrisiken erkannt werden oder ein Ausbruch auftritt, erhalten Administratoren für Trend Micro Security (für 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 **Speichern**.

Benachrichtigungen bei Sicherheitsrisiken für Administratoren konfigurieren

Sie können Trend Micro Security (für 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 Security (für Mac) Benachrichtigungen per E-Mail versenden kann. Weitere Informationen finden Sie unter *Einstellungen der Administratorbenachrichtigungen konfigurieren auf Seite 6-34*.

Prozedur

1. Gehen Sie zu **Benachrichtigungen** > **Standardbenachrichtigungen**.
2. Geben Sie auf der Registerkarte **Kriterien** an, ob Benachrichtigungen jedes Mal gesendet werden sollen, wenn Trend Micro Security (für Mac) ein Sicherheitsrisiko entdeckt wird, oder nur dann, wenn die Aktion an den Sicherheitsrisiken fehlschlägt.
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
%v	Name des Sicherheitsrisikos
%s	Der Endpunkt, auf dem das Sicherheitsrisiko erkannt wurde
%m	Agent-Gruppenname

VARIABLE	BESCHREIBUNG
%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 **Speichern**.

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 Security (für Mac) so, dass Sie und andere Administratoren für Trend Micro Security (für 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 Security (für Mac) Benachrichtigungen per E-Mail versenden kann. Weitere Informationen finden Sie unter *Einstellungen der Administratorbenachrichtigungen konfigurieren auf Seite 6-34*.

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 Security (für Mac) löst einen Virenausbruchalarm 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 Security (für Mac) die Benachrichtigung, wenn 10 verschiedene Agents insgesamt 101 Sicherheitsrisiken innerhalb eines Zeitraums von 5 Stunden gemeldet haben. Werden alle Vorfälle über einen Zeitraum von 5 Stunden auf nur einem Agent entdeckt, sendet Trend Micro Security (für 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 Agent-/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 in der Agent-Struktur auf das Stammsymbol (), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
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 6-39*.
   - Betriebssystem
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 Maßnahme

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 8-7*.

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 Security (für 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 Security (für 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 Security (für 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 Security (für 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 6-40*.

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 Trend Micro Security (für Mac) Agent die Datei säubern kann.
Kennwortgeschützte Dateien	Schließt kennwortgeschützte Dateien und komprimierte Dateien ein. **Lösung**: Heben Sie den Kennwortschutz auf, damit der Trend Micro Security (für Mac) Agent diese Dateien säubern kann.
Sicherungsdateien	Bei Dateien mit den Erweiterungen RB0~RB9 handelt es sich um Sicherungskopien infizierter Dateien. Trend Micro Security (für Mac) erstellt diese Kopien für den Fall, dass der Virus/die Malware die infizierte Datei beim Säubern beschädigt. **Lösung**: Wenn der Trend Micro Security (für Mac) Agent die infizierte Datei erfolgreich säubert, 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 in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.

3. Klicken Sie auf **Protokolle** > **Statistik zurücksetzen**.

Hinweis

Im Feld **Sicherheitsrisiken** wird die Gesamtzahl der Erkennungen für die ausgewählten Agents, alle Agents in den ausgewählten Gruppen bzw. alle Agents angezeigt.

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 Security (für 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.

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 der Agent den Zugriff auf eine Website zulässt oder sperrt.

Hinweis

Diese Funktion unterstützt die neuesten Versionen von Safari™, Mozilla™, Firefox™ und Google Chrome™ (Stand: April 2014).

Einstellungen für Web Reputation konfigurieren

Zu den Einstellungen für Web Reputation zählen Web Reputation Richtlinien, die bestimmen, ob Trend Micro Security (für Mac) den Zugriff auf eine bestimmte Website zulässt oder sperrt. Um zu ermitteln, welche Richtlinie angewendet werden soll, überprüft Trend Micro Security (für Mac) den Standort des betreffenden Agent. Der Agent-Standort gilt als "intern", wenn eine Verbindung zum Trend Micro Security (für Mac) Server hergestellt werden kann. Andernfalls gilt der Agent-Standort als "extern".

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für Web Reputation**.
4. So konfigurieren Sie eine Richtlinie für externe Agents
   a. Klicken Sie auf die Registerkarte **Externe Agents**.
   b. Wählen Sie **Web-Reputation-Richtlinie aktivieren**.

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

Hinweis

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

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

Hinweis

Die Sicherheitsstufen legen fest, ob Trend Micro Security (für Mac) den Zugriff auf eine URL zulässt oder sperrt. Wenn beispielsweise die Sicherheitsstufe auf Niedrig festgelegt ist, sperrt Trend Micro Security (für Mac) nur URLs, die bekannte Internet-Bedrohungen darstellen. Bei einer Erhöhung der Sicherheitsstufe verbessert sich die Erkennungsrate von Internet-Bedrohungen, doch steigt gleichzeitig 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. So konfigurieren Sie eine Richtlinie für interne Agents

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

b. Wählen Sie **Web-Reputation-Richtlinie aktivieren**.

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

- Smart Protection Server, wenn die Option **Abfragen an Smart Protection Server senden** aktiviert ist
- Smart Protection Network, wenn die Option **Abfragen an Smart Protection Server senden** nicht aktiviert ist

Hinweis

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

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

   - Hierfür greifen die Agents auf dieselbe Liste von Quellen für Smart Protection zurück, die auch von OfficeScan Agents genutzt wird, um den Smart Protection Server zu ermitteln, an den sie die Abfragen senden sollen.

     Wichtig

     Lesen Sie vor dem Aktivieren dieser Option die Hinweise unter *Trend Micro Smart Protection auf Seite 3-15*.

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

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

   Hinweis

   Die Sicherheitsstufen legen fest, ob Trend Micro Security (für Mac) den Zugriff auf eine URL zulässt oder sperrt. Wenn beispielsweise die Sicherheitsstufe auf Niedrig festgelegt ist, sperrt Trend Micro Security (für Mac) nur URLs, die bekannte Internet-Bedrohungen darstellen. Bei einer Erhöhung der Sicherheitsstufe verbessert sich die Erkennungsrate von Internet-Bedrohungen, doch steigt gleichzeitig auch die Wahrscheinlichkeit von Fehlalarmen.

   Unabhängig von der Sicherheitsstufe sperren die Agents keine nicht getesteten Websites.

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. Bestimmen Sie, ob die Agents Web Reputation-Protokolle an den Server senden sollen. Dies ist sinnvoll, wenn Sie die von Trend Micro Security (für

Mac) gesperrten URLs analysieren und entsprechende Aktionen für Websites durchführen möchten, die Sie als sicher einstufen.

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

   - **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.

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 Security (für 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** > **Globale Agent-Einstellungen** > **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 zulässigen Liste hinzufügen** oder **Zur gesperrten Liste 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 **Speichern**.

Web Reputation-Protokolle anzeigen

Vorbereitungen

Sie können interne Agents so konfigurieren, dass sie Web Reputation-Protokolle an den Server senden. Dadurch können Sie die von Trend Micro Security (für 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 in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
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 Security (für 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 Maßnahme

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 8-7*.

Kapitel 8

Server und Agents verwalten

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

Agent-Eigenschutz

Die Agent-Eigenschutzfunktion von Trend Micro Security (für Mac) hindert andere Programme und auch den Benutzer daran, die vom Trend Micro Security (für Mac) Agent verwendeten Dateien zu ändern und zu löschen.

Wenn Sie **Von Agent verwendete Dateien schützen** aktivieren und der Trend Micro Security (für Mac) Agent auf einem Endpunkt ausgeführt wird, sperrt Trend Micro Security (für Mac) die folgenden Dateien und Ordner:

- /Library/Application Support/TrendMicro/common
- /Library/Application Support/TrendMicro/Kext
- /Library/Application Support/TrendMicro/TmccMac
- /Library/Application Support/TrendMicro/TmccUpdate
- /Library/Application Support/TrendMicro/Plug-in
- /Library/Application Support/TrendMicro/Tools
- /Library/LaunchDaemons/com.trendmicro.icore.*
- /Library/LaunchDaemons/com.trendmicro.tmsm.plugin.plist
- /Library/LaunchDaemons/com.trendmicro.tmsm.launcher.plist
- /Application/TrendMicroSecurity.app

Hinweis

Trend Micro Security (für Mac) lässt zu, dass Dateien zum Ordner `/Library/Application Support/TrendMicro/Tools` hinzugefügt werden. Die darin enthaltenen Dateien können jedoch nicht gelöscht werden.

Agent-Eigenschutz konfigurieren

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Agent-Eigenschutz**.
4. Wählen Sie **Von Agent verwendete Dateien schützen**.
5. Wenn Sie Gruppen oder Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die ausgewählten Gruppen oder Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:
   - **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.

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** > **Globale Agent-Einstellungen** > **Certified Safe Software Service**.
2. Wählen Sie **Certified Safe Software Service**.
3. Wählen Sie **Certified Safe Software Service für Antiviren-Suche aktivieren**.
4. Klicken Sie auf **Speichern**.

Server und Agents aktualisieren

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

Führen Sie das Upgrade von Server und Agents immer umgehend durch, wenn ein neuer Build oder eine neue Version verfügbar ist.

Stellen Sie vor dem Upgrade sicher, dass Server und 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

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:\Programme\Trend Micro\OfficeScan\Addon\TMSM`

    oder

```
C:\Programme (x86)\Trend Micro\OfficeScan\Addon\TMSM
```

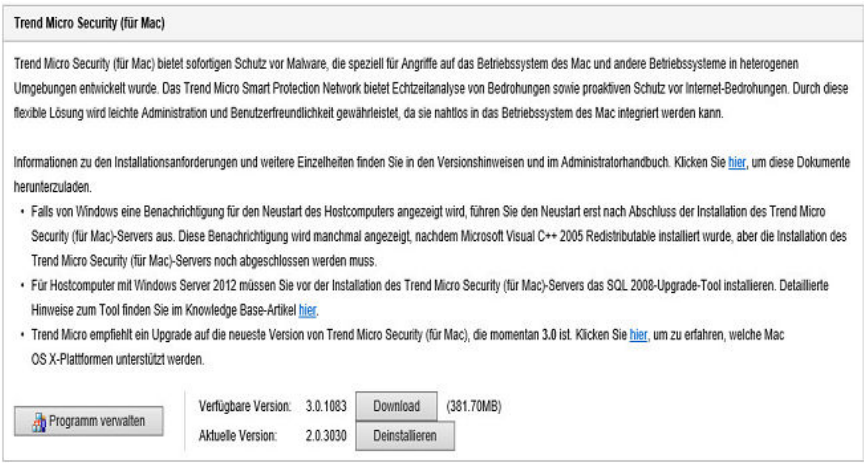
- Zu sichernde Dateien:
  - `..\apache-activemq\conf\.*`
  - `..\apache-activemq\bin\wrapper.conf`
  - `.\ServerInfo.plist`

- Datenbankdateien. Weitere Informationen erhalten Sie unter *Server-Datenbank sichern auf Seite 8-10*.

Prozedur

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

2. Klicken Sie im Abschnitt **Trend Micro Security (für Mac)** auf **Download**.

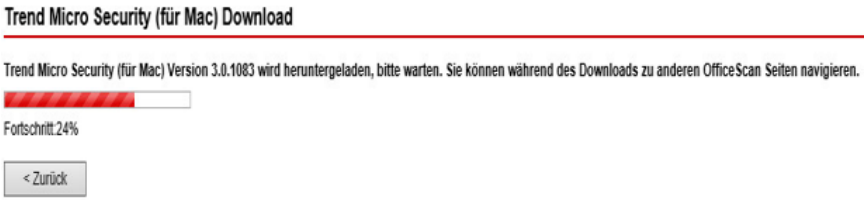


Die Größe der herunterzuladenden Datei wird neben der Schaltfläche **Download** angezeigt.

Plug-in Manager lädt das Paket nach `<OfficeScan Server-Installationsordner>\PCCSRV\Download` herunter.

`<OfficeScan Server-Installationsordner>` ist meistens `C:\Programme\Trend Micro\OfficeScan`.

3. Verfolgen Sie den Download-Fortschritt.



Sie können während des Downloads zu anderen Fenstern navigieren.

Falls beim Herunterladen des Pakets Probleme auftreten, überprüfen Sie in der OfficeScan Webkonsole die Server-Update-Protokolle. Klicken Sie im Hauptmenü auf **Protokolle** > **Server-Update**.

4. Um das Upgrade für Trend Micro Security (für Mac) sofort durchzuführen, klicken Sie auf **Jetzt upgraden**. Wenn Sie die Installation zu einem späteren Zeitpunkt nachholen möchten, gehen Sie wie folgt vor:

   a. Klicken Sie auf **Später upgraden**.

   b. Öffnen Sie das Fenster Plug-in Manager.

   c. Klicken Sie im Abschnitt **Trend Micro Security (für Mac)** auf **Upgrade**.

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

Agents aktualisieren

Achtung

Um das Aktualisieren von Agents zuzulassen, stellen Sie sicher, dass das Kontrollkästchen **Agents können Komponenten aktualisieren, aber nicht das Agent-Programm aktualisieren** im Fenster **Agent-Verwaltung** > **Einstellungen** > **Einstellungen für Updates** nicht aktiviert ist.

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 Security (für Mac) Agent** auswählen.
   - Wählen Sie in der Agent-Struktur die zu aktualisierenden Agents aus und klicken Sie auf **Tasks** > **Update**.
   - Wenn das zeitgesteuerte Update aktiviert wurde, stellen Sie sicher, dass **Trend Micro Security (für Mac) Agent** ausgewählt wurde.
   - Weisen Sie die Benutzer an, in der Agent-Konsole auf **Aktualisieren** zu klicken.

   Das Upgrade wird auf allen Agents durchgeführt, die die Benachrichtigung erhalten. Auf dem Endpunkt zeigt das Symbol für Trend Micro Security (für Mac) in der Menüleiste den laufenden Aktualisierungsvorgang an. Bis zum Abschluss des Upgrades können keine Tasks über die Konsole gestartet werden.

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 Agents angezeigt, für die das Upgrade nicht durchgeführt wurde.

   c. Um das Upgrade auch auf diesen durchzuführen, klicken Sie auf **Tasks** > **Update**.

Protokolle verwalten

Trend Micro Security (für Mac) führt umfangreiche Protokolle über erkannte Sicherheitsrisiken, gesperrte URLs und Suchvorgänge. Mit Hilfe dieser Protokolle können Sie die Antiviren-Richtlinien Ihres Unternehmens bewerten und 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 **Speichern**.

Lizenzen verwalten

Die Lizenz für Trend Micro Security (für 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	Deaktiviert	Deaktiviert

LIZENZTYP UND STATUS	FUNKTIONEN			
	ECHTZEITSUCHE	ZEITGESTEUERTE SUCHE	WEB REPUTATION	PATTERN-UPDATE
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-3*.

Prozedur

1. Gehen Sie zu **Administration** > **Produktlizenz** .
2. Informationen zur Produktlizenz anzeigen. Um aktuelle Lizenzinformationen zu erhalten, klicken Sie auf **Informationen aktualisieren**.

   Der Abschnitt **Lizenzinformationen** enthält 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 maximal zulässige Anzahl von Agent-Installationen, die die Lizenz unterstützt
   - **Lizenz läuft ab am**: Das Ablaufdatum der Lizenz
   - **Aktivierungscode**: Der für die Aktivierung der Lizenz verwendete Code.
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 Trend Micro Security**
   - **Trend Micro Security für (Mac)**
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 8-10*.

Prozedur

1. Halten Sie die folgenden Dienste über die Microsoft Management Console an:
   - **ActiveMQ für Trend Micro Security**
   - **Trend Micro Security für (Mac)**
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 Control Manager

Trend Micro Control Manager ist eine zentrale Management-Konsole zur Verwaltung von Produkten und Diensten von Trend Micro auf Gateway-, Mailserver-, Dateiserver- und Corporate-Desktop-Ebene. Die webbasierte Management-Konsole von Control Manager bietet einen zentralen Punkt zur Überwachung aller verwalteten Produkte im gesamten Netzwerk.

Systemadministratoren können von hier aus Infektionen, Sicherheitsverstöße, Viruseintrittspunkte und andere Aktivitäten und Elemente überwachen und Berichte darüber erstellen. Außerdem können sie Komponenten im gesamten Netzwerk herunterladen und verteilen und dadurch für stets aktuellen und durchgehenden Schutz sorgen. Um zusätzliche Flexibilität zu gewährleisten, ermöglicht Control Manager sowohl manuelle als auch im Vorhinein geplante Aktualisierungen sowie die Konfiguration und Verwaltung von Produkten in Einzelelementen oder Gruppen.

Control Manager-Integration in dieser Version

Diese Version von Trend Micro Security (für Mac) unterstützt Control Manager 6.0 SP3 und höher. In dieser Version können Sie Trend Micro Security (für Mac) Richtlinien erstellen, verwalten und verteilen und Endpunkte von Control Manager überwachen.

Die folgenden Richtlinienkonfigurationen sind in Control Manager verfügbar:

- Einstellungen für manuelle Suche
- Einstellungen für Echtzeitsuche
- Einstellungen für den Suchausschluss
- Zwischenspeicher-Einstellungen für Suchen
- Zeitgesteuerte Suche – Einstellungen
- Einstellungen für Updates
- Web-Reputation-Einstellungen
- Einstellungen des Agent-Eigenschutzes
- Einstellungen der Suchmethode

Sie können Endpunkte mit Hilfe des Widgets **Security (für Mac) Leistungsindikatoren** in Control Manager überwachen. Weitere Informationen finden Sie unter *Leistungsindikatoren-Widget auf Seite 8-13*.

Weitere Informationen hierzu finden Sie in der Dokumentation zu Control Manager.

Hinweis

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

Leistungsindikatoren-Widget

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

Informationen dazu, wie Sie ein Widget zum **Dashboard**-Fenster hinzufügen, finden Sie in der Dokumentation zu 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

Konfigurieren Sie die Servereinstellungen für das Widget, um Informationen vom Trend Micro Security (für Mac) Server abzurufen.

1. Navigieren Sie zum **Dashboard**-Fenster auf Control Manager.
2. Klicken Sie auf die Registerkarte, auf der sich das Widget **Security (für Mac) Leistungsindikatoren** befindet.
3. Wählen Sie **Servereinstellungen** aus dem Menü ( ) im oberen rechten Bereich des Widgets aus.
4. Klicken Sie auf **Sichtbarkeit des Servers prüfen**.
5. Klicken Sie auf **Hinzufügen**.
6. Konfigurieren Sie die Servereinstellungen:
   - **Server Name**: Der FQDN oder die IP-Adresse und die Portnummer des OfficeScan Servers, auf dem Trend Micro Security (für Mac) installiert ist
   - **Servertyp**: Wählen Sie aus der Liste **Security (für Mac)** aus.

- **Konto**: Der Benutzername für die Serveranmeldung
- **Kennwort**: Das Kennwort für die Serveranmeldung

7. Klicken Sie auf **Speichern**.
8. Wenn Ihr Netzwerk einen Proxy-Server erfordert, klicken Sie auf das Symbol 'Erweitern' (), und konfigurieren Sie die Proxy-Server-Einstellungen.
9. Klicken Sie auf **Anwenden**.

Hinweis

Um weitere Trend Micro Security (für Mac) Server hinzuzufügen, klicken Sie auf **Hinzufügen**.

10. Klicken Sie auf **Schließen**.
11. Wählen Sie **Servereinstellungen** aus dem Menü () im oberen rechten Bereich des Widgets aus.
12. Wählen Sie mindestens einen Trend Micro Security (für Mac) Server aus, und klicken Sie auf **Speichern**.

Leistungsindikatoren konfigurieren

Greifen Sie in Control Manager auf das Widget **Security (für Mac) Leistungsindikatoren** auf dem **Dashboard** zu, um die folgenden indikatorbezogenen Tasks durchzuführen.

TABELLE 8-1. KPI-Widget-Indikator-Tasks

TASK	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 **Speichern**.

TASK	SCHRITTE
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 **Speichern**.
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 **Speichern**. **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. • Die Option **Enable alerts at the following threshold** ist ausgewählt.

Widget-Einstellungen konfigurieren

Wählen Sie im **Dashboard** des Control Manager **Widget-Einstellungen** im Menü im oberen rechten Bereich des Widgets, um die folgenden Tasks durchzuführen.

TABELLE 8-2. KPI-Widget-Einstellungen

TASK	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

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

Der Server kommuniziert mit Agents über den Listening-Port (Voreinstellung: 61617).

Anmerkungen und Erinnerungen:

- Wenn Sie eine andere Portnummer angeben, vergewissern Sie sich, dass diese noch nicht durch eine andere Anwendung genutzt wird, 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 OfficeScan Agent-Firewall aktiviert wurde, fügen Sie eine Richtlinienausnahme hinzu, die eingehenden und ausgehenden Datenverkehr über den Listening-Port zulässt.

- Sie können 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.
- Wenn Sie planen, alle vorhandenen Servernamen und IPv4/IPv6-Adressen zu aktualisieren oder zu ersetzen oder den Listening-Port oder Proxy-Einstellungen zu ändern, tun Sie das vor der Installation von Agents. Falls Sie Agents installiert haben und Einstellungen ändern, verlieren die Agents die Verbindung zum Server, und die einzige Möglichkeit, die Verbindung wieder aufzubauen, besteht darin, die Agents erneut zu verteilen.

Prozedur

1. Wechseln Sie zu **Administration** > **Kommunikation zwischen Agent und Server**.
2. Geben Sie den Servernamen oder die IPv4/IPv6-Adresse(n) und den Listening-Port ein.

   Hinweis

   Wenn im Feld **Name (oder IP-Adresse) des Servers** mehrere Einträge vorhanden sind, wählt der Agent nach dem Zufallsprinzip einen Eintrag aus. Stellen Sie sicher, dass die Verbindung zwischen Agent und Server über alle Einträge hergestellt werden kann.

3. Wählen Sie aus, ob sich Agents über einen Proxy-Server mit dem Server verbinden.
   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.
4. Klicken Sie auf **Speichern**.
5. Wenn Sie aufgefordert werden, die Trend Micro Security (für 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 Agents

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

- Wenn Sie das Agent-Programm mit Hilfe des Agent-Deinstallationsprogramms von den Endpunkten entfernen, den Agent aber nicht vom Server abmelden.
- Wenn Sie die Festplatte des Endpunkts neu formatiert haben, ohne den Agent vom Server abzumelden.
- Wenn Sie die Agent-Dateien manuell entfernt haben.
- Wenn ein Benutzer den Agent über einen längeren Zeitraum entlädt oder deaktiviert.

Damit in der Agent-Struktur nur aktive Agents angezeigt werden, können Sie Trend Micro Security (für Mac) so konfigurieren, dass inaktive Agents automatisch aus der Agent-Struktur entfernt werden.

Inaktive Agents automatisch entfernen

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 ein Agent von Trend Micro Security (für Mac) als inaktiv betrachtet wird.
4. Klicken Sie auf **Speichern**.

Agent-Symbole

Symbole in der Task-Leiste und der Hauptkonsole des Endpunkts zeigen den Status des Agents und die Task an, die er derzeit ausführt.

Task-Leisten-Symbol	Menüsymbol	Beschreibung
		Der Agent ist gestartet und wird ausgeführt und ist mit dem übergeordneten Server verbunden.
		Die Produktlizenz wurde aktiviert.
		Der Agent ist gestartet und wird ausgeführt, ist aber nicht mit dem übergeordneten Server verbunden.
		Eine neue Komponentenversion ist verfügbar. Aktualisieren Sie den Agent sofort.
		Der Agent hat eine Sicherheitsbedrohung erkannt, für deren Behebung ein Neustart des Computers erforderlich ist.
		Der Agent sucht gerade nach Sicherheitsrisiken und ist mit dem übergeordneten Server verbunden.
		Der Agent aktualisiert Komponenten über den übergeordneten Server.

Task-Leisten-Symbol	Menüsymbol	Beschreibung
		Bei einem Komponenten-Update müssen Sie den Agent neu starten, um die Installation abzuschließen.
		Smart Scan oder der Web-Reputation-Dienst ist nicht auf dem Agent verfügbar. Überprüfen Sie Ihre Netzwerkverbindung.
		Der Agent wurde beim übergeordneten Server registriert, aber die Produktlizenz wurde nicht aktiviert. Einige Agent-Funktionen sind nicht verfügbar, wenn die Lizenz nicht aktiviert wurde. Weitere Informationen finden Sie unter *Lizenzen verwalten auf Seite 8-8*.
		Der Agent wurde nicht beim übergeordneten Server registriert. Die Produktlizenz kann aktiviert oder nicht aktiviert sein. Wenn ein Agent nicht beim übergeordneten Server registriert wurde: • Die Echtzeitsuche ist aktiviert, aber die Aktion bei Sicherheitsrisiken ist immer "Übergehen". • Manuelle Suche, zeitgesteuerte Suche, Web Reputation und Pattern-Updates sind deaktiviert.
		Die Produktlizenz (Voll- oder Testversion) wurde aktiviert, ist aber abgelaufen. Einige Agent-Funktionen sind nicht verfügbar, wenn die Lizenz abgelaufen ist.
		Der Agent wurde auf einer nicht unterstützten Plattform installiert.
		Der Agent funktioniert nicht ordnungsgemäß. Aktualisieren Sie den Agent auf die neueste Version, oder wenden Sie sich an den technischen Support.
		Der Agent hat eine Suche abgeschlossen oder eine Sicherheitsbedrohung erkannt.

Kapitel 9

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 Security (für 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 Trend Micro Security**
   - **OfficeScan Plug-in Manager**
   - **SQL Server (TMSM)**
   - **Trend Micro Security für (Mac)**

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`
   - **OfficeScan Debug-Protokolle**: `C:\Programme\Trend Micro \OfficeScan\PCCSRV\Log\ofcdebug.log`

     a. Aktivieren Sie die Debug-Protokollierung, wenn die Datei nicht vorhanden ist. Klicken Sie im Banner der OfficeScan Webkonsole auf das erste „c" oder „O" in „OfficeScan", 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 Security (für Mac). Wechseln Sie dafür zu `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\TMSM`.

5. Überprüfen Sie die Datenbankdateien und Registrierungsschlüssel.

   a. Überprüfen Sie, ob in `C:\Programme\Microsoft SQL Server\MSSQL.x\MSSQL\Data\` oder `C:\Programme (x86)\Microsoft SQL Server\MSSQL.x\MSSQL\Data\` die folgenden Dateien vorhanden sind:

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

   b. Überprüfen Sie, ob die Datenbankinstanz für Trend Micro Security (für 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 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 Security (für 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 Security (für Mac) sollte immer ausgeführt werden. Sollte dieser Dienst nicht aktiv sein, liegt möglicherweise ein Problem mit dem Dienst ‚ActiveMQ' vor.
   a. Erstellen Sie eine Sicherheitskopie der ActiveMQ-Daten, die sich in `C:\Programme\Trend Micro\OfficeScan\Addon\TMSM\apache-activemq\data\*.*` befinden.
   b. Löschen Sie die ActiveMQ-Daten.
   c. Versuchen Sie, den Dienst für Trend Micro Security (für 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:

```
Das Plug-in-Programm kann nicht deinstalliert werden. Der
Deinstallationsbefehl für das Plug-in-Programm fehlt im
Registrierungsschlüssel.
```

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 OfficeScan Plug-in Manager Service neu.
5. Laden Sie das Plug-in-Programm herunter, installieren Sie es, und deinstallieren Sie es anschließend.

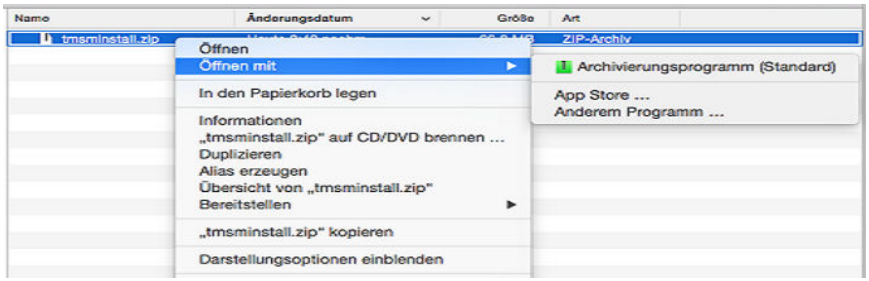
Agent-Installation

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>
  ```

  Zum 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>
  ```

  Zum Beispiel:

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

Allgemeiner Agent-Fehler

Problem:

Im Agent ist ein Fehler oder ein Problem aufgetreten.

Prozedur

1. Öffnen Sie <*Agent-Installationsordner*>`/Tools` und starten Sie 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 Trend Micro Security (für Mac) 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.

Die Knowledge Base von Trend Micro

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

http://esupport.trendmicro.com/en-us/default.aspx?locale=de_de

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

Technischer Support

Erfahren Sie mehr über die folgenden Themen:

- *Ressourcen zur Fehlerbehebung auf Seite 9-8*
- *Kontaktaufnahme mit Trend Micro auf Seite 9-9*
- *Verdächtige Inhalte an Trend Micro senden auf Seite 9-11*
- *Sonstige Ressourcen auf Seite 9-12*

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

Tipp

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

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

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

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 http://about-threats.trendmicro.com/de/threatencyclopedia#malware finden Sie weitere Informationen zu folgenden Themen:

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

Kontaktaufnahme mit Trend Micro

In Deutschland erreichen Sie unsere Trend Micro Vetriebspartner telefonisch oder per E-Mail:

Adresse	Trend Micro, Incorporated Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland Irving, Texas 75062 U.S.A.
Telefon	Telefon: +1 (817) 569-8900 Gebührenfrei in den USA: (888) 762-8736
Website	http://www.trendmicro.de/ueber-uns/kontakt/index.html
E-Mail-Adresse	sales@trendmicro.de

- Weltweite Support-Büros:

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

- Trend Micro Produktdokumentation:

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

Problemlösung beschleunigen

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

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

- Genauer Wortlaut eventueller Fehlermeldungen

Verdächtige Inhalte an Trend Micro senden

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

E-Mail-Reputation-Dienste

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

https://ers.trendmicro.com/

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

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

File-Reputation-Dienste

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

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

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

Web-Reputation-Dienste

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

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

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

Sonstige Ressourcen

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

Download Center

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

http://www.trendmicro.com/download/emea/?lng=de

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

Anregungen und Kritik

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

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

Anhang A

IPv6-Unterstützung in Trend Micro Security (für Mac)

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

IPv6-Unterstützung in Trend Micro Security (für Mac) ist ab Version 2.0 verfügbar. Frühere Versionen von Trend Micro Security (für Mac) bieten keine Unterstützung für IPv6-Adressen. Die IPv6-Unterstützung wird nach der Installation oder dem Upgrade der IPv6-kompatiblen Trend Micro Security (für Mac) Server und Agents automatisch aktiviert.

IPv6-Voraussetzungen für Trend Micro Security (für Mac) Server

Der Trend Micro Security (für Mac) Server muss mit einer Version von an OfficeScan Server installiert werden, die IPv6 unterstützt.

Die IPv6-Unterstützung in OfficeScan ist ab Version 10.6 verfügbar. Frühere Versionen von OfficeScan, die mit Trend Micro Security (für Mac) kompatibel sind (siehe *Server-Installationsvoraussetzungen auf Seite 2-2*), unterstützen die IPv6-Adressierung nicht.

Weitere Informationen zur IP6-Unterstützung finden Sie in der Dokumentation zu OfficeScan 10.6 oder höher.

IPv6-Voraussetzungen für Trend Micro Security (für Mac) Agent

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

Es empfiehlt sich, für den Agent sowohl eine IPv4- als auch eine IPv6-Adresse anzugeben, da bestimmte Entitäten, mit denen er sich verbinden soll, nur IPv4-Adressen unterstützen.

Einschränkungen eines reinen IPv6-Servers

Die folgende Tabelle enthält eine Liste der Einschränkungen für Trend Micro Security (für Mac) Server mit ausschließlich einer IPv6-Adresse.

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 • Reiner IPv4-Control Manager 6.0
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.
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 Security (für Mac) Server und die Entitäten, mit denen er zusammenarbeitet.

Einschränkungen eines reinen IPv6-Agents

Die folgende Tabelle enthält eine Liste der Einschränkungen für Agents mit ausschließlich einer IPv6-Adresse.

TABELLE A-2. Einschränkungen eines reinen IPv6-Agents

ELEMENT	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 • Reiner IPv4-Trend Micro Security (für Mac) Server
Web Reputation-Abfragen	Reine IPv6-Agents können keine Web Reputation-Abfragen an das Trend Micro Smart Protection Network senden.
Proxyverbindung	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 Security (für Mac) akzeptiert die Standarddarstellung von IPv6-Adressen.

  Zum 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 Security (für 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 Security (für 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-Struktur, 3-5
    allgemeine Tasks, 3-5
Anregungen und Kritik, 9-12

C

Control Manager-Integration, 8-12
CPU-Auslastung, 6-21

D

Damage Cleanup Services, 1-3, 1-6

F

File-Reputation-Dienste, 3-16

H

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

I

Intelligente Suche, 6-6, 6-7
    Wechsel von der herkömmlichen Suche, 6-7
IntelliScan, 6-19
Internet-Bedrohungen, 7-2

K

Knowledge Base, 9-7
Komponenten, 3-14
Kontaktaufnahme, 9-7
    Knowledge Base, 9-7
    Trend Micro, 9-7

L

Leistungssteuerung, 6-21

P

Programme, 3-14

S

Smart Feedback, 3-16
Smart Protection
    File-Reputation-Dienste, 3-16
    Web-Reputation-Dienste, 3-16
Suchkriterien
    Benutzeraktivitäten für Dateien, 6-18
    CPU-Auslastung, 6-21
    Zeitplan, 6-21
    Zu durchsuchende Dateien, 6-19
Suchmethode
    Standardeinstellung, 6-5
Suchtypen, 6-12
support
    Probleme schneller beheben, 9-10

T

Trend Micro
    Knowledge Base, 9-7
Trojaner, 1-3, 1-6

U

Unterstützung für IPv6, A-2
    Einschränkungen, A-3

V

Viren-/Malware-Suche
    Ergebnisse, 6-39

W

Webkonsole, 3-2
    Info über, 3-2
web reputation, 7-2

Web-Reputation-Dienste, 3-16
Widgets, 3-12, 3-14, 3-15

TREND MICRO INCORPORATED

Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland
Tel.: +49 (0) 811 88990-700 Fax: +4981188990799
sales@trendmicro.de marketing@trendmicro.de

www.trendmicro.com

Item Code: TSGM37575/160929