TREND MICRO™

3.2 TREND MICRO™ Smart Protection Server

Installations- und Upgrade-Handbuch

Security Made Smarter

Endpoint Security

Messaging Security

Protected Cloud

Web Security

Dokument-Nr.: APGM37783/170406

Release-Datum: April 2017

Geschützt durch U.S. Patent-Nr.: Zum Patent angemeldet.

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

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

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

Bewerten Sie diese Dokumentation auf der folgenden Website:

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

Inhaltsverzeichnis

Anhang A: Migrationseinstellungen

Stichwortverzeichnis

Vorwort

Vorwort

Willkommen beim Installations- und Upgrade-Handbuch zu Smart Protection Server™. Dieses Dokument enthält Informationen über die Produkteinstellungen.

Es werden folgende Themen behandelt:

Info über Trend Micro™

Trend Micro bietet Sicherheitssoftware und -services für Virenschutz, Anti-Spam und Content-Filtering. Trend Micro hilft Kunden weltweit beim Schutz ihrer Computer vor bösartigem Code.

Produktdokumentation

Die Dokumentation zum Smart Protection Server besteht aus den folgenden Komponenten:

Dokumentation	Beschreibung
Installations- und Upgrade-Handbuch	Unterstützt Sie bei der Planung der Installation, Upgrades und Verteilung.
Administratorhandbuch	Unterstützt Sie bei der Konfiguration aller Produkteinstellungen.
Online-Hilfe	Bietet detaillierte Anweisungen zu jedem Feld und dazu, wie Sie alle Funktionen mit Hilfe der Benutzeroberfläche konfigurieren.
Readme-Datei	Enthält die neuesten Informationen über ein Produkt, die möglicherweise nicht in der anderen Dokumentation zu finden sind. Zu den Themen gehören die Beschreibung von Funktionen, Tipps für die Installation, Lösungen bekannter Probleme und bereits veröffentlichte Produktversionen.

Die Dokumentation ist verfügbar unter folgender Adresse:

http://downloadcenter.trendmicro.com/?regs=DE

Zielgruppe

Die Dokumentation zum Smart Protection Server wurde für IT-Manager und Administratoren geschrieben. In dieser Dokumentation wird davon ausgegangen, dass der Leser fundierte Kenntnisse über Computernetzwerke besitzt.

Kenntnisse über Viren-/Malware-Schutz oder Spam-Abwehr-Technologien werden nicht vorausgesetzt.

Dokumentationskonventionen

Im Smart Protection Server Benutzerhandbuch gelten die folgenden Konventionen.

TABELLE 1. Dokumentationskonventionen

KONVENTION	BESCHREIBUNG
NUR GROSSBUCHSTABEN	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Schaltflächen, Registerkarten und Optionen
Navigation > **Pfad**	Der Navigationspfad zu einem bestimmten Fenster **Datei** > **Speichern** bedeutet beispielsweise, dass Sie in der Benutzeroberfläche im Menü **Datei** auf **Speichern** klicken
 **Hinweis**	Konfigurationshinweise
 **Tipp**	Empfehlungen oder Vorschläge
 **Warnung!**	Wichtige Aktionen und Konfigurationsoptionen

Kapitel 1

Installation und Upgrade von Smart Protection Servern planen

Dieses Kapitel enthält Informationen über die Planung einer Erstinstallation oder eines Upgrades von Smart Protection Server.

Es werden folgende Themen behandelt:

Systemvoraussetzungen

In der folgenden Tabelle werden die Systemvoraussetzungen aufgeführt:

TABELLE 1-1. Systemvoraussetzungen

HARDWARE / SOFTWARE	VORAUSSETZUNGEN
Hardware	• 2.0 GHz Intel™ Core2 Duo™ 64-Bit-Prozessor mit Unterstützung von Intel™ Virtualisierungstechnik™ oder gleichwertig • 2 GB RAM (Trend Micro empfiehlt 4 GB) • 50 GB Festplattenspeicher bei Installation auf einer virtuellen Maschine **Hinweis** Der Smart Protection Server partitioniert den erkannten Festplattenspeicher nach Bedarf automatisch. **Hinweis** Gesperrte URLs stoppen die Datenerfassung, wenn Smart Protection Server einen verfügbaren Speicherplatz von weniger als 1 GB erkennt. Smart Protection Server beginnt erneut mit der Datenerfassung, sobald der Administrator mindestens 1,5 GB Speicherplatz zur Verfügung stellt. • Monitor mit einer Mindestauflösung von 1024 x 768 bei 256 Farben oder mehr

Hardware / Software	Voraussetzungen
Virtualisierung	• Microsoft™ Windows Server™ 2008 R2 Hyper-V™ • Microsoft™ Windows Server™ 2012 Hyper-V™ • Microsoft™ Windows Server™ 2012 R2 Hyper-V™ • Microsoft™ Windows Server™ 2016 Hyper-V™ • VMware™ ESXi™ Server 6.5, 6.0 Update 2, 5.5 Update 3b • Citrix™ XenServer™ 7.1, 7.0, 6.5 **Hinweis** Wenn Sie einen Citrix™ XenServer verwenden, erstellen Sie anhand der Vorlage **Anderen Datenträger installieren** eine neue virtuelle Maschine. **Hinweis** Ein speziell entwickeltes, gesichertes und leistungsoptimiertes 64-Bit-Linux-Betriebssystem ist Teil des Smart Protection Servers.

HARDWARE / SOFTWARE	VORAUSSETZUNGEN
Virtuelle Maschine	• CentOS 7 64 Bit oder CentOS 64 Bit • Weisen Sie der virtuellen Maschine mindestens 2 GB Arbeitsspeicher zu. Trend Micro empfiehlt, 4 GB zuzuweisen. • 2.0-GHz-Prozessor • Mindestens 2 virtuelle Prozessoren (4 virtuelle Prozessoren empfohlen) • 50 GB Festplattenspeicher • 1 Netzwerkgerät • Netzwerkgerät **Hinweis** Das Kernel-Modul von Smart Protection Server installiert das VMWare Tools-Modul vmxnet3. VMWare Tools müssen daher nach der Installation von Smart Protection Server nicht installiert werden. Wenn Sie während der Installation eine vmxnet3-NIC auswählen, wird möglicherweise die Meldung **Die Mindest-Hardwareanforderungen sind nicht erfüllt** angezeigt, da der vmxnet3-Treiber noch nicht installiert wurde. Diese Meldung kann ignoriert werden, und die Installation wird normal fortgesetzt.
Webkonsole	• Microsoft Edge™ • Microsoft™ Internet Explorer™ 11 • Mozilla™ Firefox™ 3.6.0 oder höher • Adobe™ Flash™ Player 8.0 oder höher ist für das Anzeigen von Diagrammen in Widgets erforderlich. • Mindestauflösung von 1024 x 768 bei 256 Farben oder mehr

Verteilung planen

Der folgende Abschnitt enthält Informationen zur Ermittlung des Typs der zu konfigurierenden Umgebung bei der Installation von lokalen Smart Protection Server-Computern.

Bewährte Methoden

- Vermeiden Sie es, gleichzeitig manuelle und zeitgesteuerte Suchvorgänge durchzuführen. Staffeln Sie die Suchvorgänge in Gruppen.
- Vermeiden Sie, dass alle Endpunkte gleichzeitig die Funktion Jetzt durchsuchen verwenden. Beispielsweise die Option **Nach dem Update 'Jetzt durchsuchen' ausführen**.
- Sie können mehrere Smart Protection Server-Computer installieren, um die Kontinuität des Schutzes sicherzustellen, falls die Verbindung zu einem Smart Protection Server nicht verfügbar ist.
- Passen Sie Smart Protection Server an langsamere Netzwerkverbindungen an, zirka 512KBit/s, indem Sie Änderungen in der `ptngrowth.ini`-Datei vornehmen.

Datei `ptngrowth.ini` konfigurieren

Prozedur

1. Öffnen Sie die Datei "ptngrowth.ini" in `/var/tmcss/conf/`.
2. Ändern Sie die `ptngrowth.ini`-Datei und verwenden Sie die unten empfohlenen Werte:

```
[COOLDOWN]
ENABLE=1
MAX_UPDATE_CONNECTION=1
UPDATE_WAIT_SECOND=360
```

3. Speichern Sie die `ptngrowth.ini`-Datei.

4. Geben Sie für den Neustart des lighttpd-Service den folgenden Befehl über die Befehlszeilenschnittstelle (CLI) ein:

```
systemctl restart lighttpd
```

Richtlinien für die Verteilung

Berücksichtigen Sie Folgendes, wenn Sie einen lokalen Smart Protection Server einrichten:

- Smart Protection Server ist eine CPU-lastige Anwendung. Dies bedeutet, dass je mehr CPU-Ressourcen zur Verfügung stehen, desto mehr gleichzeitige Anforderungen verarbeitet werden können.
- Die Netzwerkbandbreite kann zu einem Engpass werden, abhängig von der Netzwerkinfrastruktur und der Anzahl gleichzeitiger Update-Anforderungen und Verbindungen.
- Bei einer großen Anzahl gleichzeitiger Verbindungen zwischen Smart Protection Server-Computern und Endpunkten ist möglicherweise mehr Arbeitsspeicher erforderlich.

Installation vorbereiten

Bei der Installation von Smart Protection Server wird Ihr vorhandenes System für die Programminstallation formatiert. Für eine Installation von VMware oder Hyper-V ist die Erstellung einer virtuellen Maschine vor der Installation erforderlich. Nachdem Sie die Anzahl der Smart Protection Server-Computer für Ihr Netzwerk ermittelt haben, können Sie mit der Installation beginnen.

Tipp

Sie können mehrere Smart Protection Server-Computer installieren, um die Kontinuität des Schutzes sicherzustellen, falls die Verbindung zu einem Smart Protection Server nicht verfügbar ist.

Sie benötigen für die Installation die folgenden Informationen:

- Angaben zum Proxy-Server
- Ein Server für eine virtuelle Maschine, der die Anforderungen Ihres Netzwerks erfüllt

Kapitel 2

Smart Protection Server installieren

Dieses Kapitel enthält Informationen darüber, wie Sie einen Smart Protection Server installieren und Upgrades durchführen.

Es werden folgende Themen behandelt:

Eine Erstinstallation durchführen

Starten Sie das Installationsprogramm, nachdem die Voraussetzungen zur Installation erfüllt sind, um mit der Installation zu beginnen.

Smart Protection Server installieren

Auf dieser Seite wird das Verfahren zur Installation von Smart Protection Server beschrieben.

Hinweis

Für Benutzer von Smart Protection Server 3.0 oder 3.1 steht ein Migrationstool zur Übertragung von vorkonfigurierten Einstellungen auf Smart Protection Server 3.2 über eine Befehlszeile zur Verfügung.

Eine vollständige Liste der Voraussetzungen für die Migration befindet sich unter *Voraussetzungen für die Migration von Einstellungen auf Seite A-2*.

Prozedur

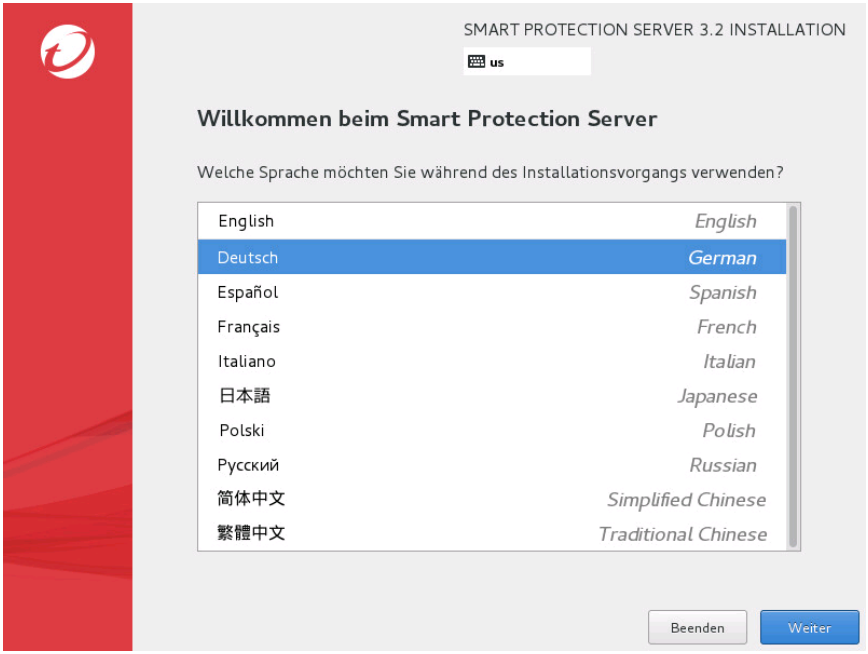
1. Erstellen Sie auf Ihrem VMware- oder Hyper-V-Server eine virtuelle Maschine, und geben Sie an, dass die virtuelle Maschine vom ISO-Image von Smart Protection Server starten soll.

   Hinweis

   Weitere Informationen finden Sie im Abschnitt über virtuelle Maschinen in den *Systemvoraussetzungen auf Seite 1-2*.

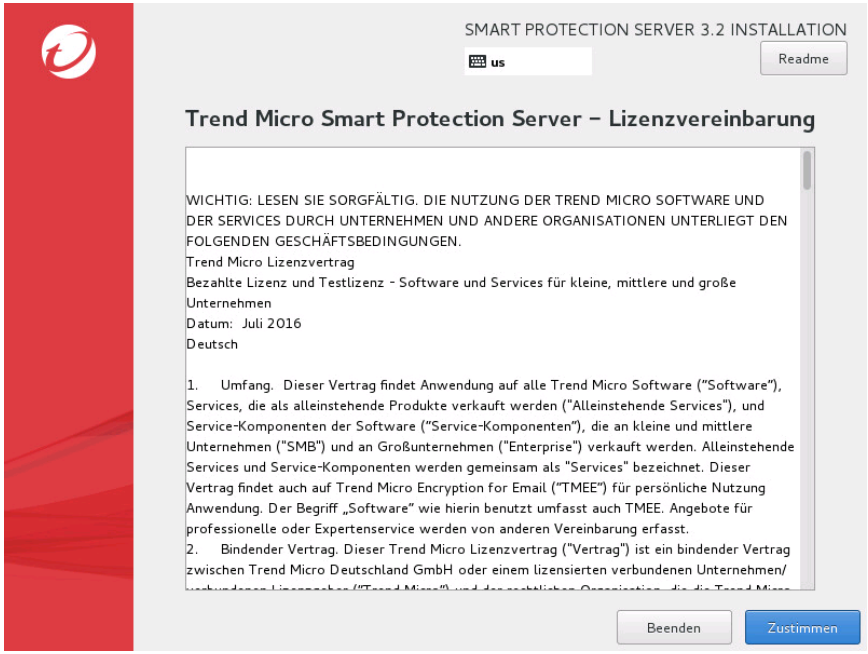
2. Schalten Sie die virtuelle Maschine ein.

Daraufhin wird der Bildschirm **Willkommen beim Smart Protection Server** angezeigt.



3. Wählen Sie die Sprache für diese Installation von Smart Protection Server aus.
4. Klicken Sie auf **Weiter**.

Der Bildschirm mit der **Lizenzvereinbarung für Trend Micro Smart Protection Server** wird angezeigt.



5. Klicken Sie zur Annahme der Lizenzbedingungen auf **Zustimmen**.

Das Fenster **INSTALLATIONSZUSAMMENFASSUNG** wird angezeigt.

6. Klicken Sie auf **DATUM & UHRZEIT**, um die Einstellungen für Datum und Uhrzeit zu überprüfen.

   a. Aktivieren Sie zur Synchronisierung der Datums- und Uhrzeiteinstellungen mit Ihrem Netzwerk die Option **Netzwerkzeit**.

   b. Um Datum und Uhrzeit anzupassen, wählen Sie in den entsprechenden Dropdown-Listen Ihre **Region** und Ihren **Ort** aus. Sie können stattdessen auch auf die Karte klicken.

   c. Klicken Sie auf **Fertig**.

7. Klicken Sie auf **NETZWERK- & HOSTNAME**, um die Netzwerkadaptereinstellungen zu überprüfen.

Hinweis

Um nach der Installation zu ändern, welches Gerät bei einem Neustart aktiv ist, melden Sie sich an der Befehlszeilenschnittstelle (CLI) an.

Falls mehrere Netzwerkgeräte vorhanden sind, konfigurieren Sie die Einstellungen für alle Geräte.

a. Wenn für Ihre Umgebung erweiterte Netzwerkeinstellungen erforderlich sind, klicken Sie auf **Konfigurieren...**.

Hinweis

Mit der Schaltfläche **Konfigurieren...** können Sie IPv4- und IPv6-Einstellungen konfigurieren. Die Standardeinstellung für IPv4 ist **Dynamische IP-Konfiguration (DHCP)**. Die Standardeinstellung für IPv6 ist **Automatische Nachbarermittlung**.

b. Klicken Sie auf **Fertig**.

8. Klicken Sie auf **INSTALLATIONSZIEL**, um den Installationsdatenträger auszuwählen.

   a. Wählen Sie im Bereich **Lokale Standarddatenträger** einen virtuellen Datenträger aus.

   b. Klicken Sie auf **Fertig**.

9. Klicken Sie auf **ROOT-KENNWORT**, um die folgenden Kennwörter einzurichten:

   - **Root-Kennwort**: Dient zur Erstellung eines Kennworts für das Root-Konto.

     Das Root-Konto gewährt Zugriff auf die Betriebssystem-Shell und verfügt über alle Rechte für den Server. Dieses Konto umfasst die meisten Berechtigungen.

   - **Admin-Kennwort**: Dient zur Erstellung eines Kennworts für das Admin-Konto.

     Das Admin-Konto ist das Standard-Administrationskonto für den Zugriff auf die Web- und CLI-Produktkonsolen von Smart Protection Server. Dieses

Konto umfasst alle Rechte für den Smart Protection Server, aber keine Rechte für die Betriebssystem-Shell.

Hinweis

Kennwörter müssen zwischen 6 und 32 Zeichen lang sein. Beachten Sie Folgendes, um ein sicheres Kennwort zu erstellen:

- Verwenden Sie sowohl Buchstaben als auch Ziffern.
- Vermeiden Sie Wörter, die in Wörterbüchern irgendeiner Sprache zu finden sind.
- Schreiben Sie Wörter absichtlich falsch.
- Verwenden Sie Phrasen oder kombinieren Sie Wörter.
- Verwenden Sie eine Kombination aus Groß- und Kleinschreibung.
- Verwenden Sie Sonderzeichen.

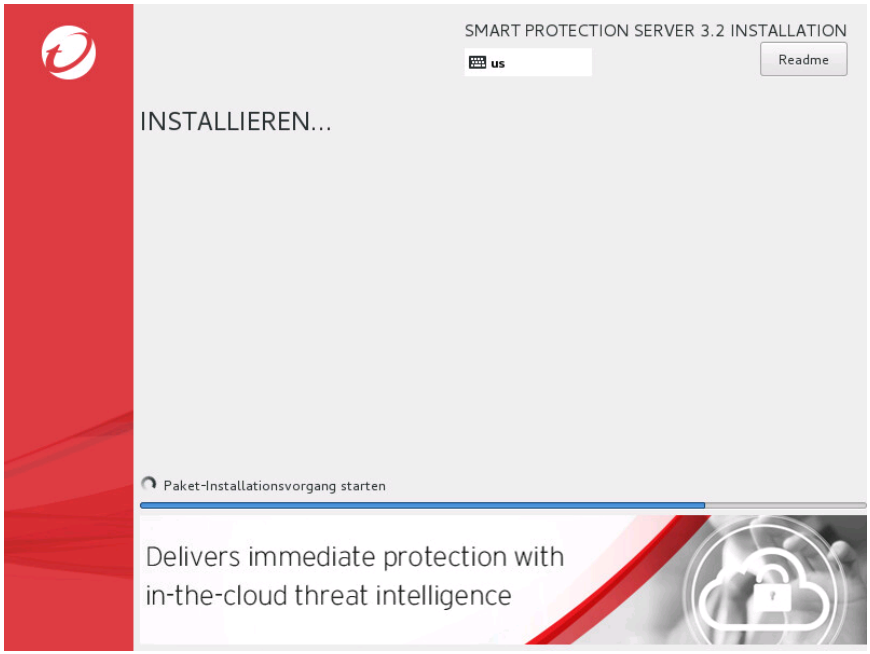
a. Klicken Sie auf **Fertig**.

10. Klicken Sie auf **Installation starten**.

Warnung!

Wenn Sie mit der Installation fortfahren, wird der erforderliche Speicherplatz partitioniert und formatiert und das Betriebssystem und die Anwendung installiert. Wenn es Daten auf der Festplatte gibt, die nicht gelöscht werden sollen, brechen Sie die Installation ab, und erstellen Sie eine Sicherung, bevor Sie fortfahren.

Der Installationsvorgang wird gestartet. Nach Abschluss der Installation wird das System neu gestartet.



Hinweis

Die Installationsprotokolldatei befindet sich unter folgendem Pfad:

```
/root/install.log
```

11. Verwenden Sie für Benutzer von Smart Protection Server 3.0 oder 3.1 das Migrationstool, um über dessen Befehlszeile vorkonfigurierte Einstellungen zu Smart Protection Server 3.2 zu übertragen.

Hinweis

Weitere Informationen finden Sie unter*Migrieren von Einstellungen aus Smart Protection Server 3.x auf Seite A-3*

12. Melden Sie sich bei der Webkonsole von Smart Protection Server an, um die Tasks durchzuführen, die nach der Installation erforderlich sind, wie beispielsweise das Konfigurieren der Proxy-Einstellungen. Melden Sie sich bei der CLI-Shell von Smart Protection Server an, wenn Sie weitere Konfigurationsschritte, Fehlerbehebungen oder Wartungstasks durchführen möchten.

Hinweis

Sie können sich mit dem Konto **`root`** mit uneingeschränkten Berechtigungen bei der Betriebssystem-Shell anmelden.

13. Führen Sie die nach der Installation erforderlichen Aufgaben durch.

Hinweis

Weitere Informationen finden Sie unter *Aufgaben nach der Installation auf Seite 3-1*.

Kapitel 3

Aufgaben nach der Installation

Dieses Kapitel enthält Informationen über die erforderlichen Aufgaben nach der Installation von Smart Protection Server.

Es werden folgende Themen behandelt:

Nach der Installation

Trend Micro empfiehlt, im Anschluss an die Installation folgende Aufgaben durchzuführen:

- Wenn Sie mit den Mindestvoraussetzungen installiert haben, deaktivieren Sie das Protokoll "Gesperrter Internet-Zugriff" von der Befehlszeilenschnittstelle (CLI) aus, indem Sie im Admin-Konto Folgendes eingeben:

```
enable
disable adhoc-query
```

- Führen Sie die Erstkonfiguration durch. Weitere Informationen finden Sie unter *Erstkonfiguration auf Seite 3-2*
- Konfigurieren Sie die Einstellungen für den Smart Protection Server in anderen Trend Micro Produkten, die auf der intelligenten Suche basierende Lösungen unterstützen.

Hinweis

Im Echtzeit-Status-Widget und auf der CLI-Konsole von Smart Protection Server werden die Adressen von Smart Protection Server angezeigt.

Nach der Installation von Smart Protection Server ist keine Installation von VMWare Tools mehr erforderlich. Das Kernel-Modul des Servers enthält das für den Smart Protection Server erforderliche VMWare Tools-Modul (vmxnet3).

Erstkonfiguration

Führen Sie folgende Aufgaben nach der Installation durch.

Wichtig

Wenn Sie eine Migration von Smart Protection Server 3.0 oder 3.1 ausführen, übertragen Sie alle Ihre Einstellungen mit dem Smart Protection Server Migrationstool (Migration.py) auf Smart Protection Server 3.2, bevor Sie fortfahren.

Prozedur

1. Melden Sie sich an der Webkonsole an.

   Das Fenster **Willkommen** wird angezeigt.

2. Klicken Sie auf **Erstinstallation konfigurieren**.

   Der Assistent für die Erstinstallation wird angezeigt.

3. Aktivieren Sie das Kontrollkästchen **"File-Reputation-Dienst aktivieren"**, um File Reputation zu verwenden.

4. Klicken Sie auf **Weiter**.

   Das Fenster "Web-Reputation-Dienst" wird angezeigt.

5. Aktivieren Sie das Kontrollkästchen **Web-Reputation-Dienst aktivieren**, um Web Reputation zu verwenden.

6. (Optional) Mit Hilfe der Einstellungen zur Filterpriorität können Sie die Filterreihenfolge für URL-Abfragen angeben.

7. Klicken Sie auf **Weiter**.

   Das Fenster "Smart Feedback" wird angezeigt.

8. Wählen Sie, ob Sie Smart Feedback verwenden möchten, um Trend Micro dabei zu unterstützen, schneller Lösungen für neue Bedrohungen bereitzustellen.

9. Klicken Sie auf **Weiter**.

   Das Fenster "Proxy-Einstellungen" wird angezeigt.

10. Geben Sie Proxy-Einstellungen an, falls in Ihrem Netzwerk ein Proxy-Server verwendet wird.

11. Klicken Sie auf **Fertig stellen**, um die Erstkonfiguration des Smart Protection Servers abzuschließen.

    Das Fenster "Zusammenfassung" der Webkonsole wird angezeigt.

Hinweis

Der Smart Protection Server aktualisiert die Pattern-Dateien nach der Erstkonfiguration automatisch.

Kapitel 4

Technischer Support

Erfahren Sie mehr über die folgenden Themen:

Ressourcen zur Fehlerbehebung

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

Support-Portal verwenden

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

Prozedur

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

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

Adresse	Trend Micro, Incorporated Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland
Telefon	Telefon: +49 811 88990-546 Tel.: +49(0) 811 88990-700
Website	www.trendmicro.de
E-Mail-Adresse	sales@trendmicro.de

- Weltweite Support-Büros:

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

- Trend Micro Produktdokumentation:

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

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://downloadcenter.trendmicro.com/index.php?regs=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

Migrationseinstellungen

Dieses Kapitel enthält Informationen zur Verwendung des Migrationstools für die Migration von Einstellungen aus Smart Protection Server 3.x.

Es werden folgende Themen behandelt:

Voraussetzungen für die Migration von Einstellungen

Smart Protection Server stellt ein Migrationstool zur Verfügung, über dessen Befehlszeile vorkonfigurierte Einstellungen aus Smart Protection Server 3.0 oder 3.1 auf die neueste Version übertragen werden können.

Wichtig

Einstellungen aus Vorgängerversionen von Smart Protection Server können ausschließlich vor der Initialisierung des Computers mit Smart Protection Server 3.2 migriert werden. Nach erfolgter Initialisierung des Computers mit Smart Protection Server 3.2 lassen sich Einstellungen nur durch Deinstallation und erneute Installation des Servers migrieren.

Die folgenden Voraussetzungen müssen vor Beginn der Migration erfüllt sein:

VORAUSSETZUNG	BESCHREIBUNG
Virtuelle Maschine	• Für Smart Protection Server 3.2 ist eine virtuelle Maschineninstanz erforderlich, die mindestens die gleichen Spezifikationen wie die des Computers aufweist, aus dem Sie Einstellungen migrieren möchten. • Die Smart Protection Server 3.2-ISO muss auf der virtuellen Maschineninstanz installiert sein, bevor das Tool ausgeführt wird.
SSH	SSH muss auf dem Smart Protection Server-Computer, aus dem Sie Einstellungen migrieren möchten, aktiviert sein. Weitere Informationen finden Sie in der Online-Hilfe oder im Administratorhandbuch.
Synchronisierung verdächtiger Objekte	Wenn die Synchronisierung verdächtiger Objekte aktiviert ist, stellen Sie sicher, dass eine funktionsfähige Verbindung zwischen der neuen virtuellen Maschine und der Quelle der verdächtigen Objekte besteht.

Migrieren von Einstellungen aus Smart Protection Server 3.x

Smart Protection Server stellt ein Migrationstool zur Verfügung, über dessen Befehlszeile vorkonfigurierte Einstellungen aus Smart Protection Server 3.0 oder 3.1 auf die neueste Version übertragen werden können.

Wichtig

Einstellungen aus Vorgängerversionen von Smart Protection Server können ausschließlich vor der Initialisierung des Computers mit Smart Protection Server 3.2 migriert werden. Nach erfolgter Initialisierung des Computers mit Smart Protection Server 3.2 lassen sich Einstellungen nur durch Deinstallation und erneute Installation des Servers migrieren.

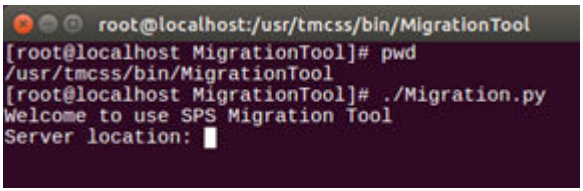
Eine vollständige Liste der Voraussetzungen für die Migration befindet sich unter *Voraussetzungen für die Migration von Einstellungen auf Seite A-2*.

Prozedur

1. Öffnen Sie anhand der Anmeldedaten für das Root-Konto eine Befehlszeile auf der virtuellen Maschine von Smart Protection Server 3.2.
2. Ändern Sie das Arbeitsverzeichnis in `/usr/tmcss/bin/MigrationTool`.
3. Führen Sie das Migrationstool mit dem folgenden Befehl aus:

   `#>./Migration.py`

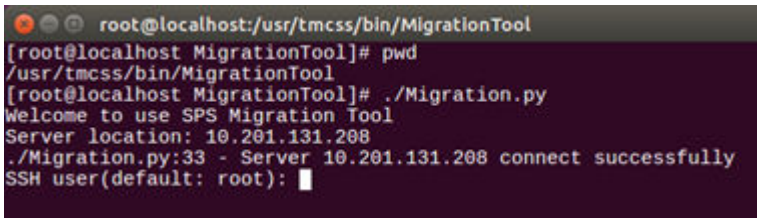
   Das Migrationstool fordert Angaben zum Server an.



4. Geben Sie den **Serverstandort** des Smart Protection Server-Computers an, aus dem Sie Einstellungen migrieren möchten.

Hinweis

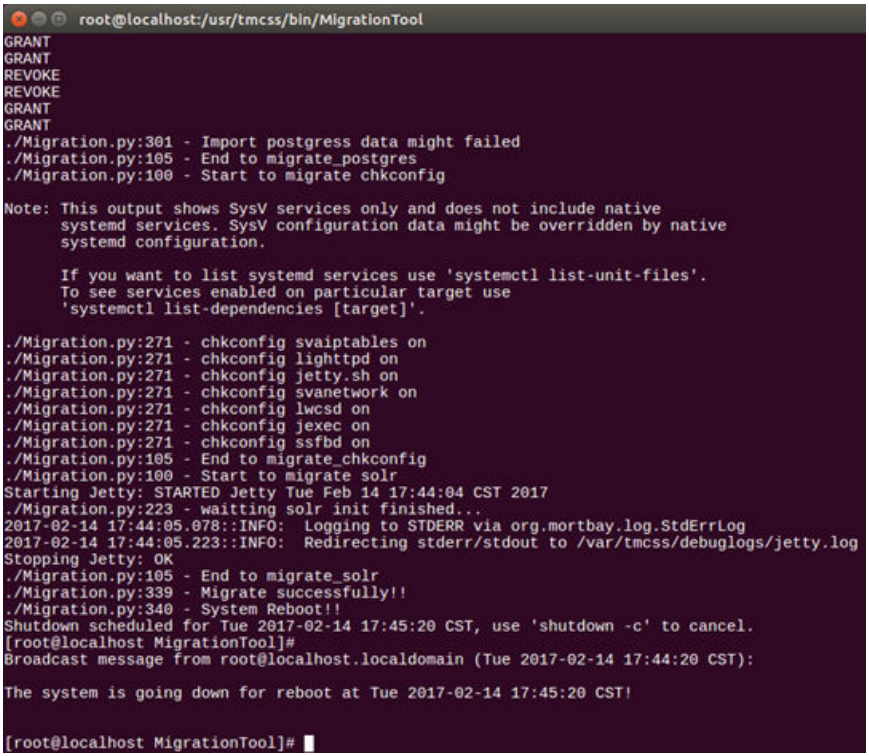
Für den **Serverstandort** kann das IP-Adress- oder das FQDN-Format verwendet werden, wobei der Standort über eine SSH-Verbindung überprüft wird.



5. Um die Einstellungen des vorherigen Servers abzurufen, geben Sie das Root-Konto und das zugehörige Kennwort ein.

   Daraufhin wird der Migrationsvorgang gestartet. Je nach Größe der Datenbank kann der Migrationsvorgang einige Zeit in Anspruch nehmen. Nach Abschluss des

Vorgangs wird der Computer mit Smart Protection Server 3.2 automatisch neu gestartet, wobei die migrierten Einstellungen angewendet werden.



Wichtig

Tritt während des Migrationsvorgangs ein Problem auf, wird Smart Protection Server nicht neu gestartet, und es wird eine Liste mit Fehlermeldungen angezeigt. Die Protokolldatei mit den Migrationsfehlern kann unter folgendem Pfad eingesehen werden:

`/var/tmcss/debuglogs/SPSMigration.log`

6. Öffnen Sie die Konsole von Smart Protection Server 3.2 mit dem Admin-Konto, um die migrierten Einstellungen zu überprüfen.

- Überprüfen Sie den Pattern-Status für den File Reputation- und den Web Reputation-Dienst:

  a. Wechseln Sie zu **Updates** > **Pattern**.

  b. Stellen Sie sicher, dass **File Reputation** und **Web Reputation** korrekt konfiguriert sind.

  c. Wurde ein Pattern fälschlicherweise deaktiviert, klicken Sie auf **Jetzt aktualisieren**, um das neueste Pattern zu erhalten.

Hinweis

Lässt sich die Aktualisierung nicht erfolgreich durchführen, überprüfen Sie, ob Sie Zugriff auf das Internet haben und die Proxy-Einstellungen korrekt sind (**Administration** > **Proxy-Einstellungen**).

- Überprüfen Sie die korrekte Konfiguration von **Verdächtige Objekte synchronisieren und aktivieren**, indem Sie zu **Smart Protection** > **Verdächtige Objekte** wechseln.

Hinweis

Ist **Verdächtige Objekte synchronisieren und aktivieren** fälschlicherweise deaktiviert, überprüfen Sie die Angaben zu **Adresse** und **API-Schlüssel** für die Virtual Analyzer-Quelle, und klicken Sie auf **Abonnieren**.

- Überprüfen Sie alle anderen Einstellungen in der Webkonsole von Smart Protection Server.

7. Sofern für den vorherigen Computer mit Smart Protection Server 3.x Zertifikate erforderlich waren, müssen diese erneut importiert werden.

Hinweis

Weitere Informationen finden Sie im Smart Protection Server-Administratorhandbuch.

8. Um dieselbe IP-Adresse der Vorgängerversion von Smart Protection Server auf der Konsole von Smart Protection Server 3.2 zu verwenden, fahren Sie die Vorgängerversion von Smart Protection Server herunter.

Stichwortverzeichnis

TREND MICRO INCORPORATED

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

www.trendmicro.com

Item Code: APGM37783/170406