TREND MICRO

3.3 TREND MICRO™ Smart Protection Server

Patch 4

Administratorhandbuch

Security Made Smarter

Endpoint Security

Messaging Security

Protected Cloud

Web Security

Dokument-Nr.: APGM38866/191126

Release-Datum: Dezember 2019

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

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

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

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

Bewerten Sie diese Dokumentation auf der folgenden Website:

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

Datenschutz und Offenlegung persönlicher Daten

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

Über den folgenden Link erhalten Sie Informationen zu den Daten, die Smart Protection Server erfasst, sowie detaillierte Anweisungen zur Deaktivierung der speziellen Funktionen, die Auswirkungen auf die Informationen haben.

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

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

https://www.trendmicro.com/privacy

Inhaltsverzeichnis

Vorwort

Kapitel 1: Einführung

Kapitel 2: Smart Protection Server verwenden

Kapitel 3: Smart Protection Server überwachen

Kapitel 4: Einbindung von Trend Micro Apex Central/ Control Manager

Kapitel 5: Technischer Support

Anhang A: CLI-Befehle

Stichwortverzeichnis

Vorwort

Willkommen beim Smart Protection Server™-Administratorhandbuch. 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

Einführung

Dieses Kapitel enthält eine Einführung in die Funktionen von Trend Micro™ Smart Protection Server™.

Es werden folgende Themen behandelt:

Wie funktioniert der Smart Protection Server?

Smart Protection Server ist eine webbasierte und leistungsfähige Schutzlösung der nächsten Generation. Der wesentliche Bestandteil dieser Lösung stellt die erweiterte Sucharchitektur dar, die Malware-Signaturen verwendet, die im Internet gespeichert sind.

Diese Lösung nutzt die File-Reputation- und die Web-Reputation-Technologie, um Sicherheitsrisiken zu erkennen. Diese Technologie basiert darauf, dass eine Vielzahl von zuvor auf den Endpunkten gespeicherten Malware-Signaturen und Listen auf Smart Protection Server ausgelagert werden.

Mit dieser Methode werden sowohl das System als auch das Netzwerk von der stetig zunehmenden Anzahl an Signatur-Updates auf den Endpunkten entlastet.

Die Notwendigkeit einer neuen Lösung

Bei der aktuellen Vorgehensweise gegen dateibasierte Bedrohungen werden die zum Schutz eines Endpunkts erforderlichen Pattern (auch "Definitionen" genannt) zeitgesteuert an die Endpunkte ausgeliefert. Pattern werden von Trend Micro in Paketen an die Endpunkte übertragen. Nachdem ein neues Update eingegangen ist, lädt die Viren-/Malware-Schutz-Software auf dem Endpunkt dieses Definitionspaket für neue Viren/Malware in den Arbeitsspeicher. Wenn ein neues Risiko durch neue Viren/Malware entsteht, muss dieses Pattern auf dem Endpunkt erneut vollständig oder teilweise aktualisiert und in den Arbeitsspeicher geladen werden, damit der Schutz aufrechterhalten wird.

Mit der Zeit nimmt der Umfang neu aufkommender Bedrohungen erheblich zu. Man schätzt, dass die Zahl der Bedrohungen in den nächsten Jahren fast exponentiell zunimmt. Dies führt zu einer Wachstumsrate, die die Anzahl der derzeit bekannten Bedrohungen um ein Vielfaches übersteigt. In Zukunft ist allein die immense Anzahl von Sicherheitsrisiken eine neue Art von Sicherheitsrisiko. Die Anzahl von Sicherheitsrisiken kann die Leistung von Servern und Workstations sowie die Netzwerkbandbreite beeinträchtigen. Auch die Dauer bis zur Bereitstellung eines wirksamen Schutzes - auch "Zeit bis zum Schutz" genannt - wird sich verlängern.

Trend Micro ist Vorreiter bei einem neuen Ansatz zur Bewältigung einer hohen Anzahl von Bedrohungen, durch den Trend Micro Kunden immun gegen die starke Zunahme von Viren/Malware werden. Hierzu wird eine Technologie genutzt, bei der Viren-/

Malware-Signaturen und -Pattern in die "Cloud", also das Internet, ausgelagert werden. Durch das Auslagern der Viren-/Malware-Signaturen in das Internet ist Trend Micro in der Lage, seine Kunden besser vor den neuen Risiken aufgrund der zukünftigen Anzahl von Bedrohungen zu schützen.

Lösungen auf Basis des Smart Protection Network

Der webbasierte Abfrageprozess verwendet zwei neue, netzwerkbasierte Technologien:

- Trend Micro Smart Protection Network™: Eine globale, Internet-basierte Infrastruktur, die Dienste für Clients bereitstellt, die keinen direkten Zugriff auf ihr Unternehmensnetzwerk haben.
- Smart Protection Server: Smart Protection Server befindet sich im lokalen Netzwerk. Sie sind für Benutzer vorgesehen, die Zugriff auf ihr Unternehmensnetzwerk haben. Diese Server führen ihre Tätigkeiten lokal im Unternehmensnetzwerk durch, um die Effizienz zu optimieren.

Hinweis

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.

Auf diesen beiden netzwerkbasierten Produkten sind die meisten der Viren-/Malware-Pattern-Definitionen und Web-Reputation-Bewertungen gespeichert. Das Trend Micro Smart Protection Network und Smart Protection Server stellen diese Definitionen anderen Endpunkten im Netzwerk zu Verfügung, damit diese potenzielle Bedrohungen verifizieren können. Abfragen werden nur dann an die Smart Protection Server gesendet, wenn das Risiko einer Datei oder eines URLs nicht auf dem Endpunkt ermittelt werden kann.

Die Endpunkte nutzen die File- und Web-Reputation-Technologie, um während ihrer normalen Systemschutzaktivitäten Abfragen an Smart Protection Server-Computer zu senden. Bei dieser Lösung werden Identifikationsdaten, die mithilfe der Trend Micro-Technologie ermittelt wurden, von den Agents an Smart Protection Server-Computer übertragen, um Abfragen durchzuführen. Die Agents senden niemals vollständige

Dateien, wenn sie die File-Reputation-Technologie nutzen. Das Risiko einer Datei wird immer mit Hilfe der Identifikationsdaten ermittelt.

Pattern-Dateien

Smart Protection Pattern-Dateien werden für File-Reputation-Dienste und Web-Reputation-Dienste verwendet. Trend Micro veröffentlicht diese Pattern-Dateien über den Trend Micro ActiveUpdate Server.

Folgende Dateien sind die Pattern-Dateien:

TABELLE 1-1. Pattern-Dateien für Smart Protection Server

REPUTATION-DIENST	PATTERN	DETAILS
File-Reputation-Dienste	**Pattern der intelligenten Suche**	Der Cloud-basierte Abfrageprozess nutzt die Pattern-Datei der intelligenten Suche in Kombination mit einem System für Cloud-Abfragen in Echtzeit. Das Cloud-Abfragesystem verifiziert Dateien, URLs und andere Komponenten während des Verifizierungsprozesses mithilfe eines Smart Protection Servers. Smart Protection Server Computer nutzen verschiedene Algorithmen für eine effiziente Verarbeitung, bei der möglichst wenig Bandbreite benötigt wird. Das Pattern der intelligenten Suche wird stündlich aktualisiert.

Reputation-Dienst	Pattern	Details
Web-Reputation-Dienste	**Websperr-Pattern**	Produkte, die die Web-Reputation-Dienste verwenden (beispielsweise Apex One und Deep Security), verifizieren die Reputation einer Website anhand eines Websperr-Patterns, indem Web-Reputation-Abfragen an Smart Protection Server gesendet werden. Diese Produkte gleichen die von der Smart Protection Quelle zurückgegebenen Reputationsdaten mit der Web-Reputation-Richtlinie ab, die auf dem Endpunkt festgelegt wurde. Die jeweilige Richtlinie bestimmt, ob die Produkte den Zugriff auf eine Website zulassen oder sperren. **Hinweis** Eine Liste der Produkte, die die Web-Reputation-Dienste verwenden, finden Sie unter: *Einbindung in Trend Micro-Produkte und -Dienste auf Seite 2-31*

Pattern-Update-Prozess

Pattern-Updates erfolgen als Reaktion auf Sicherheitsbedrohungen. Smart Protection Network und Smart Protection Server-Computer laden die Pattern-Datei der intelligenten Suche von den ActiveUpdate Servern herunter. Trend Micro-Produkte, die Smart Protection Server-Computer unterstützen, laden die Agent-Pattern der intelligenten Suche von ActiveUpdate Servern herunter.

Endpunkte innerhalb Ihres Intranets laden die Agent-Pattern der intelligenten Suche von Trend Micro-Produkten herunter, die Smart Protection Server-Computer unterstützen. Externe Endpunkte sind Endpunkte außerhalb des Intranets, die keine

Verbindung zu Smart Protection Server-Computern oder Trend Micro-Produkten haben, die Smart Protection Server-Computer unterstützen.

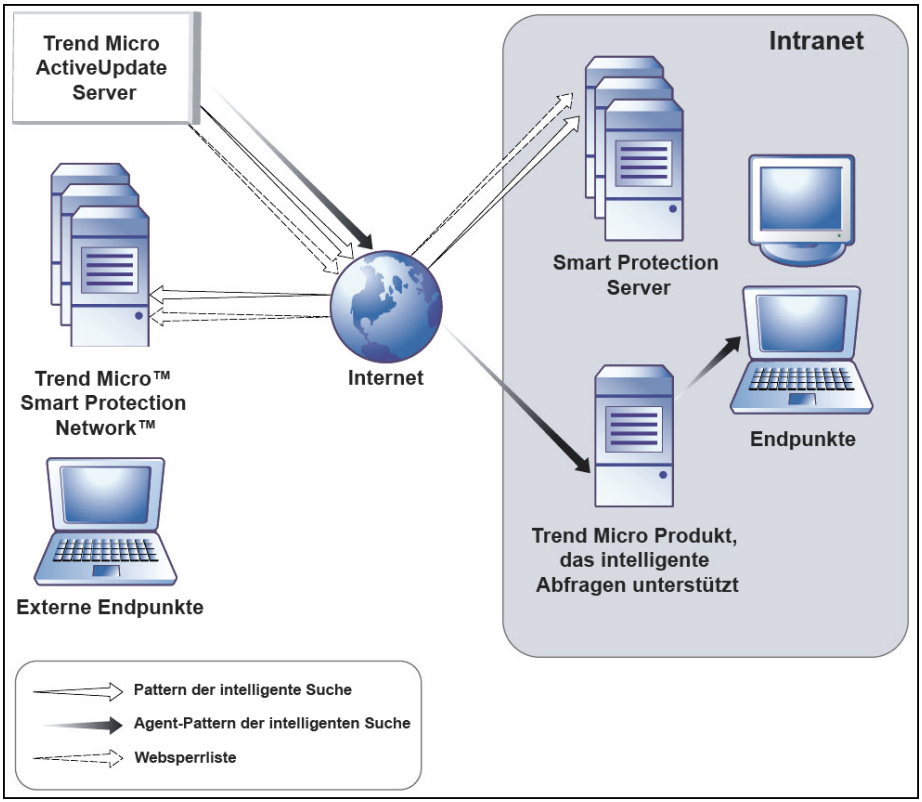


ABBILDUNG 1-1. Pattern-Update-Prozess

Der Abfrageprozess

Endpunkte, die sich zurzeit in Ihrem Intranet befinden, nutzen für Abfragen die Smart Protection Server-Computer. Endpunkte, die sich zurzeit nicht in Ihrem Intranet befinden, können für Abfragen eine Verbindung zum Trend Micro Smart Protection Network herstellen.

Obwohl eine Netzwerkverbindung erforderlich ist, um Smart Protection Server-Computer zu verwenden, können auch Endpunkte ohne Netzwerkverbindung von der Trend Micro Technologie profitieren. Agent-Pattern der intelligenten Suche und die entsprechende Suchtechnologie befinden sich auf den Endpunkten und schützen diese, wenn sie keine Verbindung zum Netzwerk haben.

Auf den Endpunkten installierte Agents führen die Suchvorgänge auf dem jeweiligen Endpunkt durch. Wenn der Agent das Risiko einer Datei oder eines URLs während der Suche nicht ermitteln kann, überprüft er dies, indem er eine Abfrage an den Smart Protection Server sendet.

TABELLE 1-2. Arbeitsweise der Schutzfunktionen in Abhängigkeit vom Zugriff auf das Internet

SPEICHERORT	ARBEITSWEISE DER PATTERN-DATEI UND DER ABFRAGEN
Zugriff auf das Internet	• **Pattern-Dateien**: Endpunkte laden die Agent-Pattern-Datei der intelligenten Suche von Trend Micro Produkte herunter, die Smart Protection Server-Computer unterstützen. • **Abfragen**: Endpunkte stellen für Abfragen eine Verbindung zum Smart Protection Server her.
Ohne Zugriff auf das Internet	• **Pattern-Dateien**: Endpunkte laden so lange nicht die neuesten Agent-Pattern-Dateien der intelligenten Suche herunter, bis ein Trend Micro Produkt verfügbar ist, das Smart Protection Server-Computer unterstützt. • **Abfragen**: Endpunkte durchsuchen Dateien mit Hilfe lokaler Ressourcen wie beispielsweise der Agent-Pattern-Datei der intelligenten Suche.

Mit der erweiterten Filtertechnologie legt der Agent die Abfrageergebnisse in einem "Zwischenspeicher" ab. Dadurch wird die Suchleistung verbessert, da die gleiche Abfrage nicht mehrfach an die Smart Protection Server-Computer gesendet werden muss.

Ein Agent, der das Risiko einer Datei nicht lokal ermitteln und auch nach mehreren Versuchen keine Verbindung zu einem Smart Protection Server-Computer herstellen kann, markiert die Datei zur weiteren Prüfung und gewährt vorübergehend Zugriff auf die Datei. Wenn die Verbindung zu einem Smart Protection Server wiederhergestellt ist, werden alle markierten Dateien erneut durchsucht. Anschließend werden die

entsprechenden Suchaktionen für alle Dateien ausgeführt, die als Bedrohung für Ihr Netzwerk bestätigt wurden.

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.

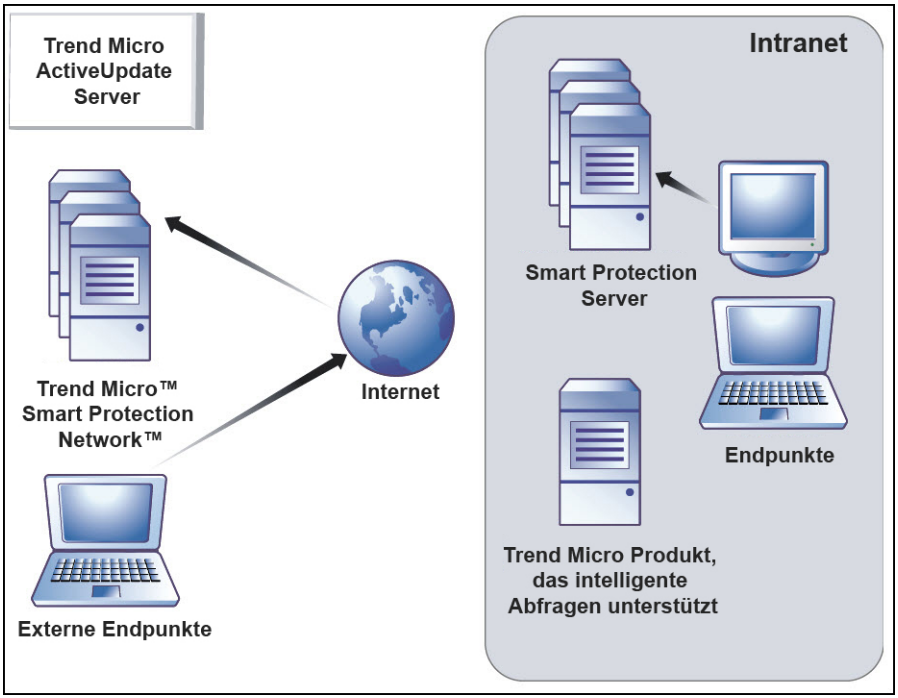


ABBILDUNG 1-2. Abfrageprozess

Neues

Smart Protection Server umfasst die folgenden neuen Funktionen und Verbesserungen:

TABELLE 1-3. Neu in Version 3.3 Patch 2

FUNKTION	BESCHREIBUNG
Integration von Trend Micro Apex Central	Smart Protection Server wird über die folgenden Funktionen in Apex Central integriert: • Einzelanmeldung (Single Sign-On, SSO) bei Smart Protection Server über die Apex Central-Konsole • Automatische Synchronisierung der Liste der verdächtigen Objekte • Smart Protection Server-Statusinformationen wie Pattern-Version, Dienstausführungsstatus und Server-Build-Versionen werden in der Apex Central-Konsole angezeigt Weitere Informationen finden Sie unter *Unterstützte Versionen von Apex Central/Control Manager auf Seite 4-2*.

TABELLE 1-4. Neu in Version 3.3

FUNKTION	BESCHREIBUNG
Neu gestaltetes Fenster "Zusammenfassung"	Das neu gestaltete Smart Protection Server-Dashboard bietet eine optimierte Ansicht aller Widgets und Registerkarten. Weitere Informationen finden Sie unter *Fenster "Zusammenfassung" verwenden auf Seite 3-2*.
Unterstützung für Community-Domäne/IP-Reputation-Dienst	Smart Protection Server unterstützt jetzt Community-Domäne/IP-Reputation-Dienst-Abfragen. Weitere Informationen finden Sie unter *Einbindung in Trend Micro-Produkte und -Dienste auf Seite 2-31*.

FUNKTION	BESCHREIBUNG
Einbindung von Trend Micro Control Manager	Smart Protection Server wird über die folgenden Funktionen in Control Manager integriert: • Einzelanmeldung bei Smart Protection Server über die Konsole von Control Manager • Automatische Synchronisierung der Liste der verdächtigen Objekte • Smart Protection Server-Statusinformationen wie Pattern-Version, Dienstausführungsstatus und Server-Build-Versionen werden in der Konsole von Control Manager angezeigt Weitere Informationen finden Sie unter *Unterstützte Versionen von Apex Central/Control Manager auf Seite 4-2*.
HTTPS-Unterstützung für Web Reputation	Der Web-Reputation-Dienst in dieser Version von Smart Protection Server unterstützt jetzt HTTPS-Verbindungen. Weitere Informationen finden Sie unter *CLI-Befehle auf Seite A-1*.
Neue Browserunterstützung	Smart Protection Server unterstützt jetzt Google Chrome.

Wichtigste Funktionen und Vorteile

Smart Protection Server bietet die folgenden Funktionen und Vorteile:

- File-Reputation-Technologie
  - Das Unternehmensnetzwerk wird in die Lage versetzt, besser auf die Bedrohung zu reagieren, die allein aus der Anzahl der Bedrohungen resultiert.
  - Die gesamte "Zeit bis zum Schutz" gegen aufkommende Bedrohungen wird erheblich reduziert.
  - Der Arbeitsspeicherbedarf auf den Workstations wird deutlich verringert und erhöht sich mit der Zeit auch kaum.

- Die Verwaltung wird vereinfacht. Der Hauptteil der Pattern-Definition-Updates muss nur auf einen einzigen Server übertragen werden, statt auf viele Workstations. Dadurch werden die Auswirkungen eines Pattern-Updates auf Workstations reduziert.
- Schützt vor webbasierten und kombinierten Angriffen.
- Stoppt Viren/Malware, Trojaner, Würmer sowie neue Varianten dieser Sicherheitsrisiken.
- Erkennt und entfernt Spyware/Grayware (einschließlich versteckter Rootkits).

- Web-Reputation-Technologie
  - Schützt vor webbasierten und kombinierten Angriffen.
  - Um den Datenschutz besorgte Kunden brauchen sich nicht über eine mögliche Aufdeckung vertraulicher Daten auf Grund von Web-Reputation-Abfragen beim Smart Protection Network sorgen.
  - Die Reaktionszeit auf Abfragen beim Smart Protection Server ist im Vergleich zu Abfragen beim Smart Protection Network geringer.
  - Durch die Installation eines Smart Protection Servers in Ihrem Netzwerk wird die Bandbreitenauslastung am Gateway reduziert.

Trend Micro Smart Protection Network

Das Trend Micro™ Smart Protection Network™ ist eine Content-Sicherheitsinfrastruktur mit webbasiertem Client der nächsten Generation, die zum Schutz der Kunden vor Sicherheitsrisiken und Internet-Bedrohungen entwickelt wurde. Es unterstützt sowohl lokale als auch gehostete Lösungen, um Benutzer kontinuierlich zu schützen, unabhängig davon, ob sie sich im Netzwerk, zu Hause oder unterwegs befinden. Dazu werden schlanke Agents eingesetzt, um auf eine einzigartige, webbasierte Kombination von E-Mail-, File- und Web-Reputation-Technologien und Bedrohungsdatenbanken zuzugreifen. Der Schutz der Kunden wird automatisch aktualisiert und weiter gestärkt, indem weitere Produkte, Services und Benutzer auf dieses Netzwerk zugreifen. Dadurch entsteht für die beteiligten Benutzer eine Art "Nachbarschaftsschutz" in Echtzeit.

File-Reputation-Dienste

File-Reputation-Dienste überprüft die Vertrauenswürdigkeit jeder einzelnen Datei anhand einer umfangreichen Internet-basierten Datenbank. Da Malware-Informationen im Internet gespeichert werden, sind sie sofort für alle Benutzer zugänglich. Leistungsstarke Content-Netzwerke und lokale Cache-Server gewährleisten minimale Latenzzeiten während der Überprüfung. Die webbasierte Client-Architektur bietet sofortigen Schutz, verringert den Aufwand der Pattern-Verteilung und reduziert den Speicherbedarf des Agents erheblich.

Web-Reputation-Dienste

Die Web-Reputation-Technologie von Trend Micro nutzt eine der größten Domänen-Reputationsdatenbanken der Welt und verfolgt die Glaubwürdigkeit von Webdomänen durch die Zuordnung einer Reputationsbewertung auf Grundlage von Faktoren wie beispielsweise dem Alter einer Website, historischer Änderungen des Speicherorts und Anzeichen von verdächtigen Aktivitäten, die von der Malware-Verhaltensanalyse entdeckt wurden. Anschließend werdeb Websites durchsucht und Benutzer vom Zugriff auf infizierte Websites abgehalten. Die Web-Reputation-Funktionen helfen dabei sicherzustellen, dass die Seiten, auf die die Benutzer zugreifen, sicher und frei von Internet-Bedrohungen wie beispielsweise Malware, Spyware und Phishing-Nachrichten sind, die Benutzer dazu bringen könnten, persönliche Daten preiszugeben. Um die Genauigkeit zu erhöhen und Fehlalarme zu reduzieren, weist die Web-Reputation-Technologie von Trend Micro Reputationsbewertungen bestimmten Webseiten oder Links innerhalb von Websites zu. Dabei wird nicht die gesamte Website klassifiziert oder gesperrt, da oft nur Teile einer legitimen Site gehackt wurden. Außerdem können sich Reputationen dynamisch mit der Zeit ändern.

Die Web-Reputation-Funktionen helfen dabei sicherzustellen, dass die Webseiten, auf die die Benutzer zugreifen, sicher und frei von Internet-Bedrohungen wie beispielsweise Malware, Spyware und Phishing-Nachrichten sind, die Benutzer dazu bringen könnten, persönliche Daten preiszugeben. Bei der Web Reputation werden Webseiten auf Basis der Reputationsbewertung gesperrt. Wenn Web Reputation aktiviert ist, werden Benutzer davon abgehalten, auf bösartige URLs zuzugreifen.

Smart Feedback

Trend Micro™ Smart Feedback bietet ununterbrochene Kommunikation zwischen Trend Micro-Produkten sowie Zugriff auf die Bedrohungsforschungszentren und entsprechenden Technologien des Unternehmens rund um die Uhr. Jede neue Bedrohung, die bei einem einzelnen Kunden während einer routinemäßigen Überprüfung der Reputation erkannt wird, führt zu einer automatischen Aktualisierung der Trend Micro Bedrohungsdatenbanken, wodurch diese Bedrohung für nachfolgende Kunden blockiert wird. 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 Personal- oder Geschäftsdaten eines Kunden jederzeit gewährleistet.

Kapitel 2

Smart Protection Server verwenden

Dieses Kapitel enthält Informationen zur Konfiguration des Smart Protection Server.

Es werden folgende Themen behandelt:

Erstkonfiguration

Führen Sie folgende Aufgaben nach der Installation durch.

Wichtig

Wenn Sie eine Migration von Smart Protection Server 3.1 ausführen, übertragen Sie alle Einstellungen mit dem Smart Protection Server-Migrationstool (Migration.py) auf Smart Protection Server 3.3, bevor Sie den Vorgang fortsetzen.

Weitere Informationen finden Sie im Installationshandbuch unter "Migrieren von Einstellungen aus Smart Protection Server 3.1".

Prozedur

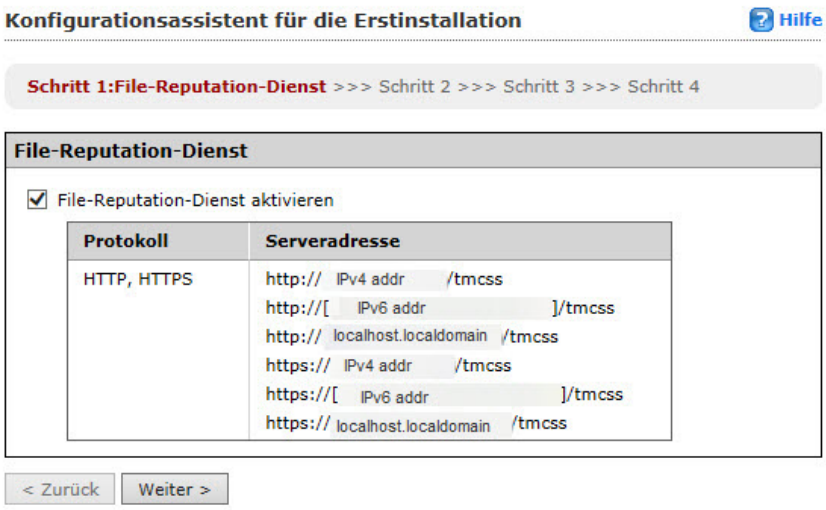
1. Melden Sie sich an der Webkonsole an.

   Das Fenster **Willkommen** wird angezeigt.

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

   Der Assistent für die Erstinstallation wird angezeigt.

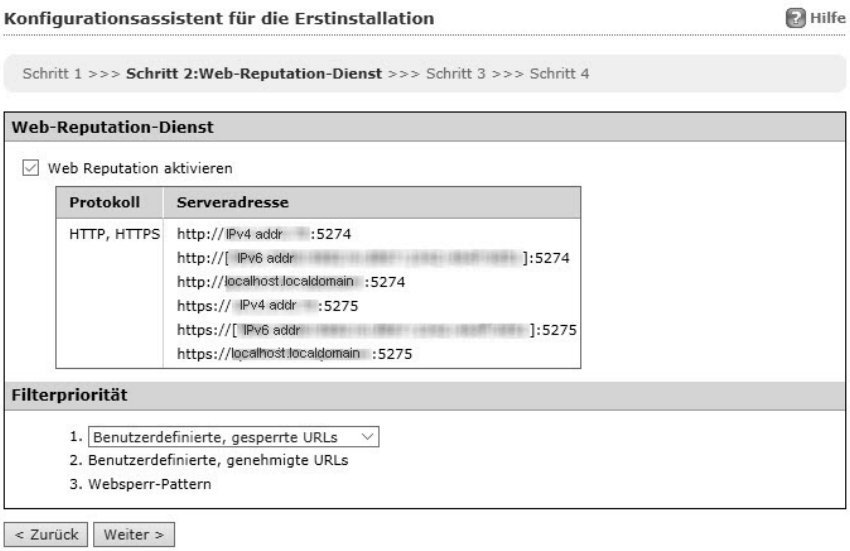
3. Aktivieren Sie das Kontrollkästchen **File-Reputation-Dienst aktivieren**.



4. Klicken Sie auf **Weiter**.

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

5. Aktivieren Sie das Kontrollkästchen **Web-Reputation-Dienst aktivieren**.



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.

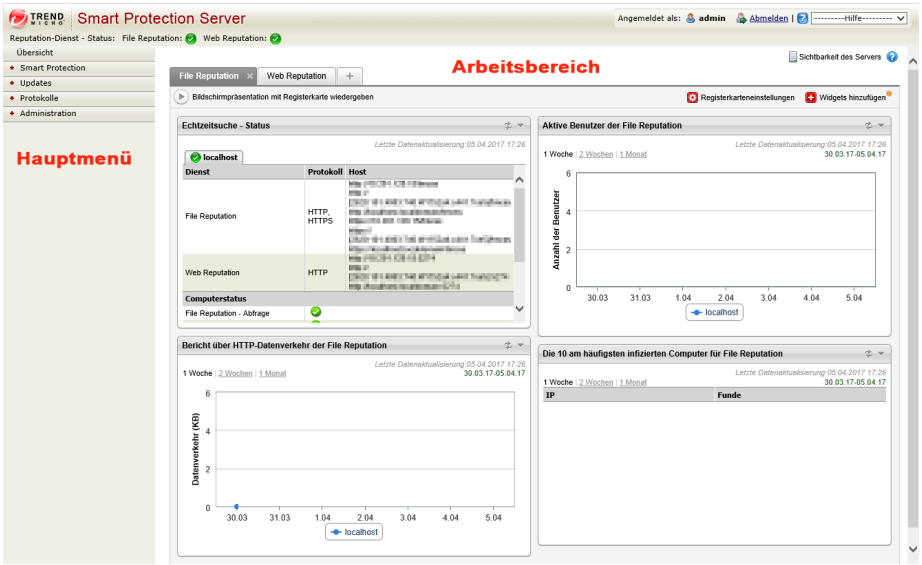
Hinweis

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

Produktkonsole verwenden

Die Produktkonsole besteht aus den folgenden Elementen:

- **Hauptmenü**: Bietet Links zu den Fenstern **Übersicht**, **Smart Protection**, **Updates**, **Protokolle** und **Administration**.
- **Arbeitsbereich**: Anzeigen von zusammenfassenden Informationen und des Komponentenstatus, Konfigurieren von Einstellungen, Aktualisieren von Komponenten und Durchführen von administrativen Aufgaben.



MENÜ	BESCHREIBUNG
Übersicht	Zeigt benutzerdefinierte Informationen über Smart Protection Server -Computer, -Datenverkehr und -Funde an, wenn Sie Widgets hinzufügen.

MENÜ	BESCHREIBUNG
Smart Protection	Bietet Optionen zum Konfigurieren der Reputation-Dienste, der benutzerdefinierten URLs, der verdächtigen Objekte sowie von Smart Feedback.
Updates	Bietet Optionen zum Konfigurieren zeitgesteuerter Updates, manueller Programm-Updates, Uploads von Programmpaketen sowie der Update-Adresse.
Protokolle	Bietet Optionen zum Abfragen von Protokollen und zur Protokollwartung.
Administration	Bietet Optionen zum Konfigurieren des SNMP-Dienstes, von Benachrichtigungen und Proxy-Einstellungen sowie zum Sammeln von diagnostischen Informationen zur Fehlerbehebung.

Auf die Produktkonsole zugreifen

Nach dem Anmelden an der Webkonsole zeigt das erste Fenster eine Statuszusammenfassung für den Smart Protection Server Computer an.

Prozedur

1. Öffnen Sie einen Webbrowser, und geben Sie den URL ein, der auf dem ersten Befehlszeilen-Banner nach der Installation angezeigt wird.
2. Geben Sie `admin` als Benutzernamen und Kennwort in den entsprechenden Feldern ein.
3. Klicken Sie auf **Anmelden**.

Smart Protection verwenden

Diese Version des Smart Protection Servers enthält File-Reputation- und Web-Reputation-Dienste.

Reputation-Dienste verwenden

Aktivieren Sie die Reputation-Dienste über die Produktkonsole, damit andere Trend Micro Produkte Smart Protection verwenden können.

File-Reputation-Dienste aktivieren

Aktivieren Sie die File-Reputation-Dienste, um Abfragen von Endpunkten zu unterstützen.

Prozedur

1. Wechseln Sie zu **Smart Protection** > **Reputation-Dienste** und anschließend zur Registerkarte **File Reputation**.

2. Aktivieren Sie das Kontrollkästchen **File-Reputation-Dienst aktivieren**.

3. Klicken Sie auf **Speichern**.

   Die Serveradresse kann jetzt von anderen Trend Micro-Produkten, die Smart Protection Server-Computer unterstützen, für File-Reputation-Abfragen verwendet werden.

Web-Reputation-Dienste aktivieren

Aktivieren Sie die Web-Reputation-Dienste, um URL-Abfragen von Endpunkten zu unterstützen. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **Web-Reputation-Dienst aktivieren:** Wählen Sie diese Option, um Web-Reputation-Abfragen von Endpunkten zu unterstützen.
- **Serveradresse**: Wird von anderen Trend Micro Produkten verwendet, die Web-Reputation-Abfragen unterstützen.
- **Filterpriorität**: Wählen Sie die Priorität zum Filtern von URLs aus.

Prozedur

1. Navigieren Sie zu **Smart Protection** > **Reputation-Dienste** und klicken Sie anschließend auf die Registerkarte **Web Reputation**.
2. Aktivieren Sie das Kontrollkästchen **Web-Reputation-Dienst aktivieren**.
3. (Optional) Geben Sie die Priorität der benutzerdefinierten zulässigen und gesperrten URLs beim Filtern der URLs an. Wenn beispielsweise **benutzerdefinierte gesperrte URLs** die höchste Priorität haben, haben **benutzerdefinierte zulässige URLs** die zweite Priorität.

4. Klicken Sie auf **Speichern**.

Die Serveradresse kann jetzt von anderen Trend Micro Produkten, die Smart Protection Server unterstützen, für Web-Reputation-Abfragen verwendet werden.

Benutzerdefinierte URLs konfigurieren

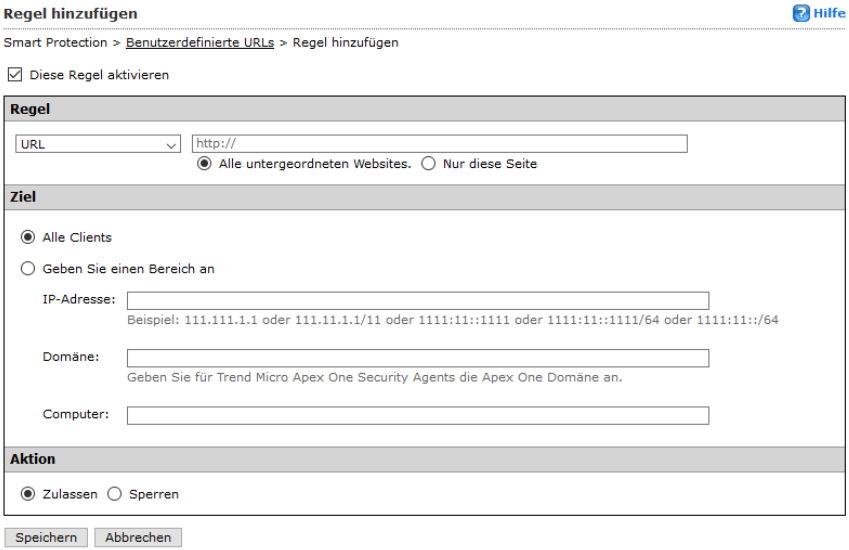
Benutzerdefinierte URLs ermöglichen Ihnen, eigene zulässige oder gesperrte URLs anzugeben. Diese werden für die Web Reputation verwendet. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **Regel suchen**: Wählen Sie diese Option, um nach einer Zeichenfolge in der Liste mit Regeln zu suchen.
- **URL testen**: Wählen Sie diese Option, um die Regeln zu suchen, die von dem URL ausgelöst werden. Der URL muss mit `http://` oder `https://` beginnen.

Prozedur

1. Navigieren Sie zu **Smart Protection** > **Benutzerdefinierte URLs**.
2. Klicken Sie unter **Suchkriterien** auf **Hinzufügen**.

Das Fenster **Regel hinzufügen** wird angezeigt.



3. Aktivieren Sie das Kontrollkästchen **Diese Regel aktivieren**.

4. Wählen Sie eine der folgenden Optionen:

   - **URL**: Zur Angabe eines URLs, der für alle untergeordneten Websites oder nur eine einzelne Seite gilt.

   - **URL mit Schlüsselwort**: Zur Angabe einer Zeichenfolge mit Hilfe regulärer Ausdrücke.

   Klicken Sie auf **Testen**, um die Regel auf die 20 häufigsten URLs und die Top-100-URLs des vorherigen Tages gemäß dem Internet-Zugriffsprotokoll anzuwenden.

5. Wählen Sie eine der folgenden Optionen:

   - **Alle Clients**: Zur Übernahme auf alle Clients.

   - **Geben Sie einen Bereich an**: Zum Anwenden auf einen Bereich von IP-Adressen, Domänen- und Computernamen.

Hinweis

Es werden IPv4- und IPv6-Adressen unterstützt.

6. Wählen Sie **Zulassen** oder **Sperren**.
7. Klicken Sie auf **Speichern**.

Benutzerdefinierte URLs importieren

Verwenden Sie dieses Fenster, um benutzerdefinierte URLs von einem anderen Smart Protection Server zu importieren. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **Durchsuchen**: Klicken Sie hierauf, um eine `.csv`-Datei von Ihrem Computer auszuwählen.
- **Upload**: Klicken Sie hier, um die ausgewählte `.csv`-Datei hochzuladen.
- **Abbrechen**: Klicken Sie hierauf, um zum vorherigen Fenster zurückzukehren.

Verdächtige Objekte konfigurieren

Ein verdächtiges Objekt ist eine IP-Adresse, Domäne oder URL oder ein SHA-1-Wert in einer übermittelten Probe, die bzw. der als bösartig bekannt oder potenziell bösartig ist.

Smart Protection Server kann folgende Quellen abonnieren, um verdächtige Objekte zu synchronisieren:

TABELLE 2-1. Quellen verdächtiger Objekte für Smart Protection Server

ADRESSE	TYP DES VERDÄCHTIGEN OBJEKTS	BESCHREIBUNG
Deep Discovery Analyzer • **Virtual Analyzer**	URL	Virtual Analyzer ist eine Cloud-basierte, virtuelle Umgebung zur Analyse verdächtiger Dateien. Mithilfe so genannter Sandbox-Images kann das Verhalten von Dateien in einer Umgebung beobachtet werden, die die Endpunkte Ihres Netzwerks simuliert, ohne dass das Netzwerk gefährdet wird. Virtual Analyzer in verwalteten Produkten verfolgt und analysiert übermittelte Proben. Virtual Analyzer kennzeichnet verdächtige Objekte auf der Grundlage ihres Potenzials zur Gefährdung oder Zerstörung Ihrer Systeme.
Apex Central/Control Manager • Konsolidierte verdächtige Objekte • **Benutzerdefinierte verdächtige Objekte** • **Virtual Analyzer – verdächtige Objekte**	URL	Deep Discovery Analyzer sendet eine Liste der verdächtigen Objekte an Apex Central/Control Manager. Apex Central/Control Manager Administratoren können Objekte hinzufügen, die sie als verdächtig ansehen, sich aber derzeit nicht in der Liste der verdächtigen Objekte von Virtual Analyzer befinden. Benutzerdefinierte verdächtige Objekte haben eine höhere Priorität als verdächtige Objekte von Virtual Analyzer. Apex Central/Control Manager konsolidiert verdächtige Objekte und dazugehörige Suchaktionen und verteilt sie an Smart Protection Server.

Sofern Abonnements bestehen, leitet der Smart Protection Server Folgendes weiter:

- Informationen zu verdächtigen URLs für Trend Micro Produkte (z. B. Apex Central, ScanMail und Deep Security), die Web-Reputation-Abfragen senden
- Aktionen gegen verdächtige URLs für Security Agents, die Web-Reputation-Abfragen senden.

Hinweis

- Weitere Informationen zur Verwaltung verdächtiger Objekte mit Apex Central finden Sie im *Apex Central-Administratorhandbuch*.

  Sie können eine PDF-Version des Handbuchs herunterladen oder das Handbuch online mithilfe des folgenden Links anzeigen:

  http://docs.trendmicro.com/de-de/enterprise/apex-central.aspx

- Weitere Informationen dazu, wie Control Manager verdächtige Objekte behandelt, finden Sie im *Leitfaden zur verbundenen Bedrohungsabwehr* für Ihre Version von Control Manager unter dem folgenden Link:

  http://docs.trendmicro.com/de-de/enterprise/control-manager.aspx

Prozedur

1. Navigieren Sie zu **Smart Protection** > **Verdächtige Objekte**.
2. Geben Sie den FQDN oder die IP-Adresse der **Quelle** der verdächtigen Objekte ein.
3. Geben Sie den **API-Schlüssel** ein, den Sie von der Quelle für verdächtige Objekte erhalten haben.
4. Optional: Klicken Sie auf **Verbindung testen**, um sicherzustellen, dass der Servername, die IP-Adresse und der API-Schlüssel gültig sind und dass die Quelle verfügbar ist.
5. Klicken Sie auf **Abonnieren**.
6. Um verdächtige Objekte sofort zu synchronisieren, wählen Sie **Verdächtige Objekte synchronisieren und aktivieren** und klicken Sie anschließend auf **Jetzt synchronisieren**.

Hinweis

Die Option ist nur verfügbar, wenn die Verbindung von Smart Protection Server zu der Quelle erfolgreich hergestellt wurde.

7. Klicken Sie auf **Speichern**.

Smart Feedback aktivieren

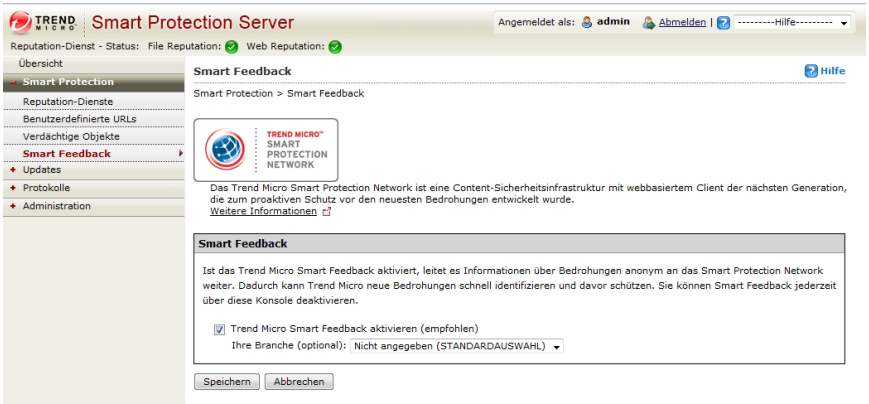
Trend Micro Smart Feedback leitet anonyme Informationen über Bedrohungen an das Trend Micro Smart Protection Network weiter, damit Trend Micro neue Bedrohungen schnell identifizieren und angehen kann. Sie können Smart Feedback jederzeit über diese Konsole deaktivieren.

Prozedur

1. Wechseln Sie zu **Smart Protection** > **Smart Feedback**.

> **Hinweis**
>
> Vergewissern Sie sich, dass der Smart Protection Server mit dem Internet verbunden ist, bevor Sie Smart Feedback aktivieren.

2. Wählen Sie **Trend Micro Smart Feedback aktivieren** aus.



3. Wählen Sie Ihre Branche.

4. Klicken Sie auf **Speichern**.

Updates

Die Wirksamkeit von Smart Protection Server hängt davon ab, ob die aktuellen Pattern-Dateien und Komponenten verwendet werden. Trend Micro veröffentlicht stündlich neue Versionen der Pattern-Dateien der intelligenten Suche.

Tipp

Trend Micro empfiehlt, die Komponenten unmittelbar nach der Installation zu aktualisieren.

Manuelle Updates konfigurieren

Pattern manuell aktualisieren:

Prozedur

1. Navigieren Sie zu **Updates**.
2. Klicken Sie im Menü auf **Pattern** oder **Programm**.
3. Klicken Sie auf **Jetzt aktualisieren** oder **Jetzt speichern und aktualisieren**, um Updates sofort durchzuführen.

Zeitgesteuerte Updates konfigurieren

Zeitgesteuerte Updates durchführen:

Prozedur

1. Navigieren Sie zu **Updates**.

2. Klicken Sie im Menü auf **Pattern** oder **Programm**.
3. Geben Sie den Update-Zeitplan an.
4. Klicken Sie auf **Speichern**.

Updates der Pattern-Dateien

Aktualisieren Sie Pattern-Dateien, damit sichergestellt ist, dass die neuesten Daten für die Abfragen zur Verfügung stehen. Diese Optionen stehen auf dem Bildschirm zur Verfügung:

- **Zeitgesteuerte Updates aktivieren**: Wählen Sie diese Option, um automatische Updates zu konfigurieren, die stündlich oder alle 15 Minuten durchgeführt werden.
- **Jetzt aktualisieren**: Klicken Sie hierauf, um alle Pattern-Dateien sofort zu aktualisieren.

Updates der Programmdateien

Führen Sie ein Update auf die neueste Version des Programms durch, um von Produktverbesserungen zu profitieren. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **Betriebssystem**: Wählen Sie diese Option, um Betriebssystemkomponenten zu aktualisieren.
- **Smart Protection Server**: Wählen Sie diese Option, um die Programmdatei des Servers zu aktualisieren.
- **Widget-Komponenten**: Wählen Sie diese Option, um Widgets zu aktualisieren.
- **Zeitgesteuerte Updates aktivieren**: Wählen Sie diese Option, um Programmdateien täglich zu einer bestimmten Uhrzeit oder wöchentlich zu aktualisieren.
- **Nur Download**: Wählen Sie diese Option, um Updates herunterzuladen und eine Abfrage, ob Sie die Programmdateien aktualisieren möchten, zu erhalten.

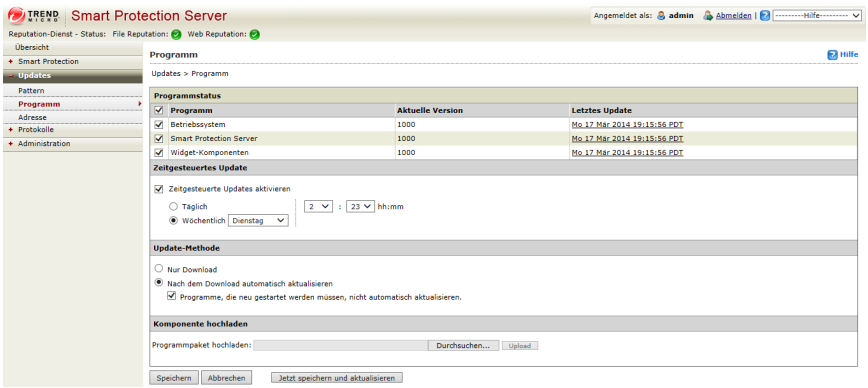
- **Nach dem Download automatisch aktualisieren**: Wählen Sie diese Option, um alle Produkt-Updates nach dem Download automatisch zu übernehmen, unabhängig davon, ob ein Neustart erforderlich ist.
- **Programme, die neu gestartet werden müssen, nicht automatisch aktualisieren**: Wählen Sie diese Option, um alle Updates herunterzuladen und nur solche Programme zu installieren, für die kein Neustart erforderlich ist.
- **Upload**: Klicken Sie hierauf, um eine Programmdatei auf den Smart Protection Server hochzuladen und zu aktualisieren.
- **Durchsuchen**: Klicken Sie hierauf, um ein Programmpaket zu suchen.
- **Jetzt speichern und aktualisieren**: Klicken Sie hierauf, um die Einstellungen zu übernehmen und sofort ein Update durchzuführen.

Es gibt drei Möglichkeiten, die Programmdatei zu aktualisieren: zeitgesteuerte Updates, manuelle Updates und Hochladen der Komponente.

Zeitgesteuerte Updates aktivieren

Prozedur

1. Wechseln Sie zu **Updates** > **Programm**.
2. Wählen Sie **Zeitgesteuerte Updates aktivieren** und dann den Update-Zeitplan aus.



3. Wählen Sie eine der folgenden Update-Methoden:

    - **Nur Download**: Aktivieren Sie dieses Kontrollkästchen, um Programmdateien herunterzuladen, ohne sie zu aktualisieren. Auf der Webkonsole wird eine Nachricht angezeigt, wenn Updates von Programmdateien zur Installation bereitstehen.
    - **Nach dem Download automatisch aktualisieren**: Aktivieren Sie dieses Kontrollkästchen, um Programm-Updates nach dem Herunterladen automatisch zu aktualisieren.
        - **Programme, die neu gestartet werden müssen, nicht automatisch aktualisieren**: Aktivieren Sie dieses Kontrollkästchen, um eine Abfrage auf der Webkonsole zu erhalten, wenn ein Update einen Neustart erfordert. Programm-Updates, die keinen Neustart erfordern, werden automatisch installiert.

4. Klicken Sie auf **Speichern**.

Manuelle Updates durchführen

Prozedur

1. Navigieren Sie zu **Updates** > **Programm**.
2. Wählen Sie eine der folgenden Update-Methoden:

    - **Nur Download**: Aktivieren Sie dieses Kontrollkästchen, um Programmdateien herunterzuladen, ohne sie zu aktualisieren. Auf der Webkonsole wird eine Nachricht angezeigt, wenn Updates von Programmdateien zur Installation bereitstehen.
    - **Nach dem Download automatisch aktualisieren**: Aktivieren Sie dieses Kontrollkästchen, um Programm-Updates nach dem Herunterladen automatisch zu aktualisieren.
        - **Programme, die neu gestartet werden müssen, nicht automatisch aktualisieren**: Aktivieren Sie dieses Kontrollkästchen, um eine Abfrage auf der Webkonsole zu erhalten, wenn ein Update einen Neustart

erfordert. Programm-Updates, die keinen Neustart erfordern, werden automatisch installiert.

3. Klicken Sie auf **Jetzt speichern und aktualisieren**.

Dateien für manuelle Updates hochladen

Prozedur

1. Navigieren Sie zu **Updates** > **Programm**.

   Wichtig

   Vergewissern Sie sich, dass der Smart Protection Server kein Update durchführt, bevor Sie fortfahren. Wenn Sie ein Programm oder eine Komponente aktualisieren müssen, deaktivieren Sie zunächst zeitgesteuerte Komponenten-Updates, bevor Sie fortfahren.

2. Klicken Sie unter **Komponente hochladen** auf **Durchsuchen...**, um die Programmdatei für manuelle Programm-Updates zu suchen.

   Hinweis

   Suchen Sie die Programmdatei, die Sie von der Website von Trend Micro heruntergeladen oder von Trend Micro erhalten haben.

3. Suchen Sie die Datei, und klicken Sie auf **Öffnen**.

4. Klicken Sie auf **Upload**.

   Hinweis

   Wenn Sie die zeitgesteuerte Suche deaktiviert haben, um ein Programm oder eine Komponente zu aktualisieren, aktivieren Sie die Funktion nach dem Hochladen und Aktualisieren wieder.

Verfügbare Programmdateien

Verwenden Sie dieses Fenster, um die verfügbaren Programmdateien zu aktualisieren. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- <Kontrollkästchen>: Aktivieren Sie das Kontrollkästchen des verfügbaren Programms, das aktualisiert werden sollen.
- **Jetzt aktualisieren**: Klicken Sie hierauf, um die ausgewählten Programmdateien zu aktualisieren.

Eine Update-Adresse konfigurieren

Verwenden Sie dieses Fenster, um die Update-Adresse für File Reputation und Web Reputation anzugeben. Die Standard-Update-Adresse ist der Trend Micro ActiveUpdate Server. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **Trend Micro ActiveUpdate Server**: Wählen Sie diese Option, um Updates vom Trend Micro ActiveUpdate Server herunterzuladen.
- **Andere Update-Adresse**: Wählen Sie diese Option, um eine Update-Adresse wie beispielsweise Trend Micro Apex Central/Control Manager anzugeben.

Prozedur

1. Navigieren Sie zu **Updates** > **Quelle**, und wählen Sie die Registerkarte **File Reputation** oder **Web Reputation** aus.
2. Wählen Sie **Trend Micro ActiveUpdate Server**, oder wählen Sie **Andere Update-Adresse**, und geben Sie einen URL ein.
3. Klicken Sie auf **Speichern**.

Administrative Aufgaben

Administrative Aufgaben ermöglichen Ihnen, SNMP-Dienst-Einstellungen, Benachrichtigungen und Proxy-Server-Einstellungen zu konfigurieren oder diagnostische Informationen herunterzuladen.

SNMP-Dienst

Smart Protection Server unterstützt SNMP, um eine größere Flexibilität bei der Überwachung des Produkts zu bieten. Sie können Einstellungen konfigurieren und die MIB-Datei (Management Information Base) im Fenster **SNMP-Dienst** herunterladen. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **SNMP-Dienst aktivieren**: Wählen Sie diese Option, um SNMP zu verwenden.
- **Community-Name**: Geben Sie einen SNMP-Community-Namen an.
- **IP-Einschränkung aktivieren**: Wählen Sie diese Option, um die IP-Einschränkung zu aktivieren.

Hinweis

Klassenloses Inter-Domänen-Routing (CIDR) wird für die IP-Einschränkung nicht unterstützt. Durch Aktivieren die IP-Adresseinschränkung verhindern Sie einen unbefugten Zugriff auf den SNMP-Dienst.

- **IP-Adresse**: Geben Sie eine IP-Adresse an, um den SNMP-Dienst zum Überwachen des Systemstatus zu verwenden.
- **Subnetzmaske**: Geben Sie eine Netzmaske an, um den IP-Adressbereich zur Verwendung des SNMP-Dienstes für die Überwachung des Computerstatus zu verwenden.
- **Smart Protection Server MIB**: Klicken Sie auf "Smart Protection Server MIB", um die MIB-Datei herunterzuladen.
- **Speichern**: Klicken Sie hierauf, um die Einstellungen zu speichern.
- **Abbrechen**: Klicken Sie hierauf, um die Änderungen zu verwerfen.

SNMP-Dienst konfigurieren

Konfigurieren Sie die Einstellungen für den SNMP-Dienst, um SNMP-Verwaltungssystemen zu ermöglichen, den Status des Smart Protection Servers zu überwachen.

Prozedur

1. Wechseln Sie zu **Administration** > **SNMP-Dienst**.

2. Aktivieren Sie das Kontrollkästchen **SNMP-Dienst aktivieren**.
3. Geben Sie einen **Community-Namen** an.
4. Aktivieren Sie das Kontrollkästchen **IP-Einschränkung aktivieren**, um unbefugten Zugriff auf den SNMP-Dienst zu verhindern.

> **Hinweis**
>
> Klassenloses Inter-Domänen-Routing (CIDR) wird für die IP-Einschränkung nicht unterstützt.

5. Geben Sie eine IP-Adresse an.
6. Geben Sie eine Subnetzmaske an.
7. Klicken Sie auf **Speichern**.

MIB-Datei herunterladen

Laden Sie die MIB-Datei von der Webkonsole herunter, um den SNMP-Dienst zu nutzen.

Prozedur

1. Navigieren Sie zu **Administration** > **SNMP-Dienst**.
2. Klicken Sie auf **Smart Protection Server MIB**, um die MIB-Datei herunterzuladen. Eine Bestätigungsabfrage wird angezeigt.
3. Klicken Sie auf **Speichern**.

   Das Fenster **Speichern unter** wird angezeigt.
4. Geben Sie den Speicherort an.
5. Klicken Sie auf **Speichern**.

Smart Protection Server MIB

In der folgenden Tabelle wird die Smart Protection Server MIB beschreiben.

OBJEKTNAME	OBJEKTBEZEICHNER (OID)	BESCHREIBUNG
Trend-MIB:: TBLVersion	1.3.6.1.4.1.6101.1.2.1.1	Gibt die Version des aktuellen Patterns der intelligenten Suche zurück.
Trend-MIB:: TBLLastSuccessfulUpdate	1.3.6.1.4.1.6101.1.2.1.2	Gibt Datum und Uhrzeit des letzten erfolgreichen Updates des Patterns der intelligenten Suche zurück.
Trend-MIB:: LastUpdateError	1.3.6.1.4.1.6101.1.2.1.3	Gibt den Status des letzten Updates des Patterns der intelligenten Suche zurück. • 0: Letztes Pattern-Update war erfolgreich. • <Fehlercode>: Letztes Pattern-Update war nicht erfolgreich.

Objektname	Objektbezeichner (OID)	Beschreibung
Trend-MIB:: LastUpdateErrorMessage	1.3.6.1.4.1.6101.1.2.1.4	Gibt eine Fehlermeldung zurück, wenn das letzte Update des Patterns der intelligenten Suche nicht erfolgreich war.
Trend-MIB:: WCSVersion	1.3.6.1.4.1.6101.1.2.1.5	Gibt die Version des aktuellen Websperr-Patterns zurück.
Trend-MIB:: WCSLastSuccessfulUpdate	1.3.6.1.4.1.6101.1.2.1.6	Gibt Datum und Uhrzeit des letzten erfolgreichen Updates des Websperr-Patterns zurück.
Trend-MIB:: WCSLastUpdateError	1.3.6.1.4.1.6101.1.2.1.7	Gibt den Status des letzten Updates des Websperr-Patterns zurück. • 0: Letztes Pattern-Update war erfolgreich. • <Fehlercode>: Letztes Pattern-Update war nicht erfolgreich.
Trend-MIB:: WCSLastUpdateErrorMessage	1.3.6.1.4.1.6101.1.2.1.8	Gibt eine Fehlermeldung zurück, wenn das letzte Update des Websperr-Patterns nicht erfolgreich war.
Trend-MIB:: LastVerifyError	1.3.6.1.4.1.6101.1.2.2.2	Gibt den Status der File-Reputation-Abfrage zurück. • 0: File-Reputation-Abfrage verhält sich erwartungsgemäß. • <Fehlercode>: File-Reputation-Abfrage verhält sich nicht erwartungsgemäß.
Trend-MIB:: WCSLastVerifyError	1.3.6.1.4.1.6101.1.2.2.3	Gibt den Status der Web-Reputation-Abfrage zurück. • 0: Web-Reputation-Abfrage verhält sich erwartungsgemäß. • <Fehlercode>: Web-Reputation-Abfrage verhält sich nicht erwartungsgemäß.

OBJEKTNAME	OBJEKTBEZEICHNER (OID)	BESCHREIBUNG
Trend-MIB:: LastVerifyErrorMessage	1.3.6.1.4.1.6101.1.2.2.4	Gibt eine Fehlermeldung zurück, wenn der letzte Systemstatus einer File-Reputation-Abfrage nicht erfolgreich war.
Trend-MIB:: WCSLastVerifyErrorMessage	1.3.6.1.4.1.6101.1.2.2.5	Gibt eine Fehlermeldung zurück, wenn der letzte Systemstatus einer Web-Reputation-Abfrage nicht erfolgreich war.

Unterstützte MIBs

Die folgende Tabelle enthält eine Beschreibung der unterstützten MIBs.

OBJEKTNAME	OBJEKTBEZEICHNER (OID)	BESCHREIBUNG
SNMP MIB-2-System	1.3.6.1.2.1.1	Die Systemgruppe enthält Informationen zum System, auf dem sich das Element befindet. Die Objekte in dieser Gruppe sind hilfreich für die Fehler- und Konfigurationsverwaltung. Weitere Informationen finden Sie unter IETF RFC 1213.
SNMP MIB-2-Schnittstellen	1.3.6.1.2.1.2	Die Schnittstellen-Objektgruppe enthält Informationen zu jeder Schnittstelle auf einem Netzwerkgerät. Die Informationen in dieser Gruppe sind hilfreich für die Fehler-, Konfigurations-, Leistungs- und Kontenverwaltung. Weitere Informationen finden Sie unter IETF RFC 2863.

Proxy-Einstellungen

Wenn Sie einen Proxy-Server im Netzwerk verwenden, konfigurieren Sie die Proxy-Einstellungen. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **Proxy-Server verwenden**: Wählen Sie diese Option, wenn in Ihrem Netzwerk ein Proxy-Server verwendet wird.
- **HTTP**: Wählen Sie diese Option, wenn Ihr Proxy-Server HTTP als Proxy-Protokoll verwendet.

- **SOCKS5**: Wählen Sie diese Option, wenn Ihr Proxy-Server SOCKS5 als Proxy-Protokoll verwendet.
- **Name oder IP-Adresse des Servers**: Geben Sie den Namen oder die IP-Adresse des Proxy-Servers ein.
- **Port**: Geben Sie die Portnummer ein.
- **Benutzer-ID**: Geben Sie die Benutzer-ID für den Proxy-Server ein, falls der Proxy-Server eine Authentifizierung verlangt.
- **Kennwort**: Geben Sie das Kennwort für den Proxy-Server ein, falls der Proxy-Server eine Authentifizierung verlangt.

Proxy-Einstellungen konfigurieren

Prozedur

1. Wechseln Sie zu **Administration** > **Proxy-Einstellungen**.

2. Aktivieren Sie das Kontrollkästchen **Proxy-Server für Updates verwenden**.
3. Wählen Sie **HTTP** oder **SOCKS5** als Proxy-Protokoll aus.

Hinweis

SOCKS4-Proxy-Konfigurationen werden von Smart Protection Server nicht mehr unterstützt.

4. Geben Sie den Namen oder die IP-Adresse des Servers ein.
5. Geben Sie die Portnummer ein.
6. Falls der Proxy-Server Anmeldedaten verlangt, geben Sie die **Benutzer-ID** und das **Kennwort** ein.
7. Klicken Sie auf **Speichern**.

Support

Verwenden Sie die Webkonsole, um diagnostische Informationen für die Fehlerbehebung und den Support herunterzuladen.

Klicken Sie auf **Start**, um mit dem Sammeln von Diagnoseinformationen zu beginnen.

Systeminformationen für den Support herunterladen

Prozedur

1. Navigieren Sie zu **Administration** > **Support**.
2. Klicken Sie auf **Start**.

   Ein Fenster mit dem Download-Fortschritt wird angezeigt.
3. Klicken Sie auf **Speichern**, wenn die Abfrage für die heruntergeladene Datei angezeigt wird.
4. Geben Sie den Speicherort und den Dateinamen an.
5. Klicken Sie auf **Speichern**.

Kennwort der Produktkonsole ändern

Das Kennwort der Produktkonsole ist die wichtigste Maßnahme, um den Smart Protection Server vor unbefugten Änderungen zu schützen. Ändern Sie das Kennwort aus Sicherheitsgründen regelmäßig, und verwenden Sie ein Kennwort, das nicht leicht zu erraten ist. Das Kennwort des Admin-Kontos kann über die Befehlszeilenschnittstelle (CLI) geändert werden. Verwenden Sie in der Befehlszeilenschnittstelle den Befehl "configure password", um Änderungen vorzunehmen.

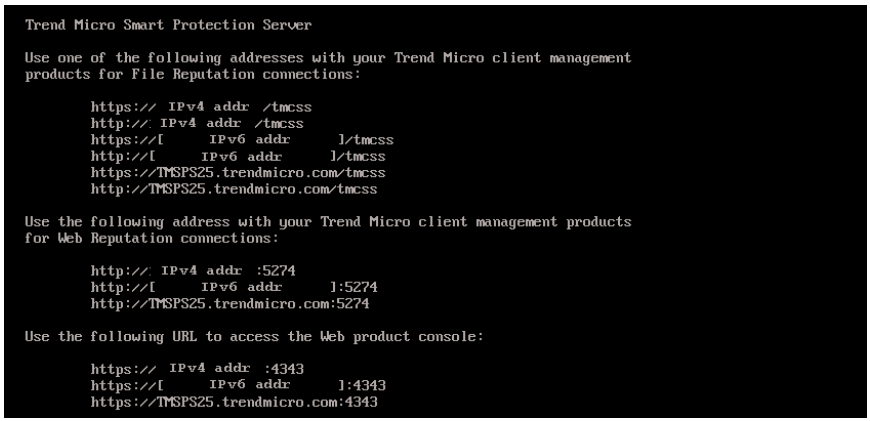
Tipp

Beachten Sie Folgendes, wenn Sie ein sicheres Kennwort 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.

Prozedur

1. Melden Sie sich mit dem Admin-Konto an der CLI-Konsole an.



2. Geben Sie Folgendes ein, um administrative Befehle zu aktivieren:

   ```
   enable
   ```

3. Geben Sie folgenden Befehl ein:

   ```
   configure password admin
   ```

4. Geben Sie das neue Kennwort ein.

5. Geben Sie das neue Kennwort ein zweites Mal ein, um es zu bestätigen.

Zertifikate importieren

Diese Version von Smart Protection Server ermöglicht Administratoren, das Serverzertifikat sicherheitshalber neu zu generieren oder zu importieren.

Prozedur

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

   Die aktuellen "Informationen zum Serverzertifikat" werden angezeigt.

2. Klicken Sie auf **Aktuelles Zertifikat ersetzen**.

3. Klicken Sie auf **Durchsuchen...** zum Auswählen eines gültigen Zertifikats zum Hochladen. Das Zertifikat muss eine PEM-Datei sein.

4. Klicken Sie auf **Weiter**.

5. Prüfen Sie die Details für das neue Zertifikat, und klicken Sie auf **Fertig stellen**. Warten Sie einige Sekunden, bis das Zertifikat importiert ist.

Einbindung in Trend Micro-Produkte und -Dienste

Smart Protection Server ist in die in den folgenden Tabellen aufgeführten Produkte und Dienste von Trend Micro eingebunden. Ausführliche Informationen zu den

Einbindungsdetails finden Sie in den relevanten Abschnitten der Online-Hilfe der entsprechenden Produkte.

TABELLE 2-2. File-Reputation-Dienste

VERWENDETE KOMPONENTEN	KOMPONENTENQUELLE	EINBINDENDE PRODUKTE UND UNTERSTÜTZTE MINDESTVERSIONEN	ERSTE VERSION VON SMART PROTECTION SERVER
Pattern der intelligenten Suche **Hinweis** Pattern der intelligenten Suche funktioniert in Verbindung mit dem auf dem einbindenden Produkt installierten Agent-Pattern der intelligenten Suche.	• Trend Micro ActiveUpdate Server (Standard) • HTTP oder HTTPS werden für alternative Update-Adressen unterstützt	• Apex One 2019 • OfficeScan 10 • Core Protection Module 10.5 • Deep Security 7.5 • InterScan Messaging Security Virtual Appliance 9.1 • InterScan Web Security Virtual Appliance 6.5 SP1 • ScanMail for Microsoft Exchange 10 SP1 • PortalProtect 2.1 for SharePoint 2.1 • Threat Mitigator 2.5 • Worry-Free Business Security 6.0	1.0

Verwendete Komponenten	Komponentenquelle	Einbindende Produkte und unterstützte Mindestversionen	Erste Version von Smart Protection Server
Smart Protection Service Proxy (für Community File Reputation verwendet)	n. z. (integriert)	• Apex One 2019 • Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1 • OfficeScan XG	3.0 Patch 2

TABELLE 2-3. Web-Reputation-Dienste

VERWENDETE KOMPONENTEN	KOMPONENTENQUELLE	EINBINDENDE PRODUKTE UND UNTERSTÜTZTE MINDESTVERSIONEN	ERSTE VERSION VON SMART PROTECTION SERVER
Websperr-Pattern	• Trend Micro ActiveUpdate Server (Standard) • Andere unterstützte Update-Adresse	• Apex One 2019 • OfficeScan 10.5 • Core Protection Module 10.5 • Deep Discovery Inspector 2.6 • Deep Security 7.5 • ScanMail for Microsoft Exchange 10.0 SP1 • ScanMail for Lotus Domino 5.6 • PortalProtect 2.1 • Trend Micro Security (für Mac) 2.0	2.0
Zulässige/ Gesperrte URLs	n. z. (Liste direkt auf der Konsole von Smart Protection Server konfiguriert)		2.0
Verdächtige URLs	• Apex Central 2019 • Control Manager 6.0 SP2 • Deep Discovery Analyzer 5.0		2.6 Patch 1
Verbesserungen bei verdächtigen URLs	• Apex Central 2019 • Control Manager 6.0 SP3	• Apex One 2019 • OfficeScan 11 SP1	3.0 Patch 1

Verwendete Komponenten	Komponentenquelle	Einbindende Produkte und unterstützte Mindestversionen	Erste Version von Smart Protection Server
Smart Protection Service Proxy (für Web Inspection Service verwendet)	n. z. (integriert)	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1	3.0 Patch 2
Proxy für den Smart Protection Dienst (für Community-Domäne/IP-Reputation-Dienst verwendet)	n. z. (integriert)	• Deep Discovery Inspector 5.0 • Deep Discovery Analyzer 6.0	3.3

Tabelle 2-4. Reputation-Dienste für mobile Apps

Verwendete Komponenten	Komponentenquelle	Einbindende Produkte und unterstützte Mindestversionen	Erste Version von Smart Protection Server
Smart Protection Service Proxy	n. z. (integriert)	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1	3.0 Patch 2

TABELLE 2-5. Certified Safe Software Service

VERWENDETE KOMPONENTEN	KOMPONENTENQUELLE	EINBINDENDE PRODUKTE UND UNTERSTÜTZTE MINDESTVERSIONEN	ERSTE VERSION VON SMART PROTECTION SERVER
Smart Protection Service Proxy	n. z. (integriert)	• Apex One 2019 • OfficeScan XG • Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1	3.0 Patch 2

TABELLE 2-6. Predictive Machine Learning

VERWENDETE KOMPONENTEN	KOMPONENTENQUELLE	EINBINDENDE PRODUKTE UND UNTERSTÜTZTE MINDESTVERSIONEN	ERSTE VERSION VON SMART PROTECTION SERVER
Smart Protection Service Proxy	n. z. (integriert)	• Apex One 2019 • OfficeScan XG • Deep Discovery Inspector 5.0 • Deep Discovery Email Inspector 3.0 • Deep Discovery Analyzer 6.0	3.1

Hinweis

Der Smart Protection Service Proxy leitet Abfrageanforderungen aus integrierten Produkten zur weiteren Analyse an Smart Protection Network.

Kapitel 3

Smart Protection Server überwachen

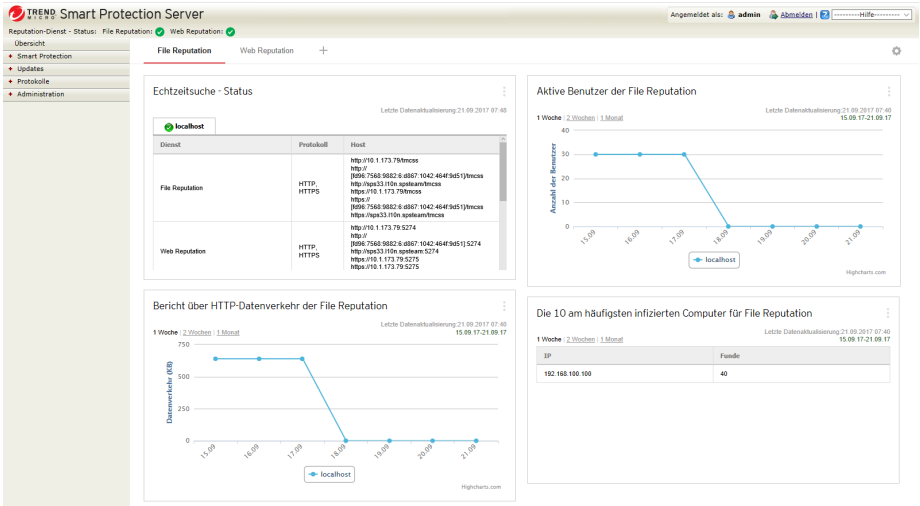
Sie können den Smart Protection Server mit Protokollen und vom Fenster "Übersicht" aus mit Widgets überwachen.

Es werden folgende Themen behandelt:

Fenster "Zusammenfassung" verwenden

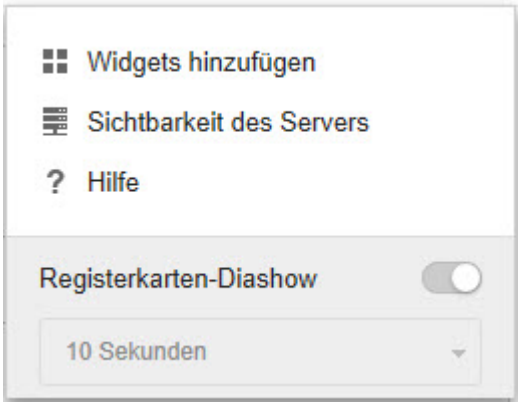
Im Fenster **Übersicht** können benutzerdefinierte Informationen über Smart Protection Server-Computer, -Datenverkehr und -Funde angezeigt werden.

File-Reputation-Dienst und Web-Reputation-Dienst unterstützen die Protokolle HTTP und HTTPS. HTTPS stellt eine sicherere Verbindung zur Verfügung, während HTTP weniger Bandbreite verwendet. Adressen von Smart Protection Server werden auf dem Konsolenbanner der Befehlszeilenschnittstelle (CLI) angezeigt.



Klicken Sie auf das Zahnradsymbol (⚙), um auf die Liste **Sichtbarkeit des Servers** im Bildschirm **Zusammenfassung** zuzugreifen.

ABBILDUNG 3-1. Sichtbarkeit des Servers



Verwenden Sie die Liste **Sichtbarkeit des Servers**, um Server zur Liste "Sichtbarkeit des Servers" hinzuzufügen oder Proxy-Server-Einstellungen für Server zu konfigurieren, die sich in der Liste befinden. Das Ändern der Serverinformationen ist bei allen Widgets gleich.

Hinweis

Smart Protection Server Adressen werden bei Trend Micro Produkten verwendet, die Endpunkte verwalten. Serveradressen werden verwendet, um die Verbindungen der Endpunkte mit den Smart Protection Server-Computern zu konfigurieren.

Arbeiten mit Registerkarten

Verwalten Sie Registerkarten durch Hinzufügen, Umbenennen und Löschen von Registerkarten, durch Ändern des Layouts und durch automatischen Wechsel zwischen Registerkartenansichten.

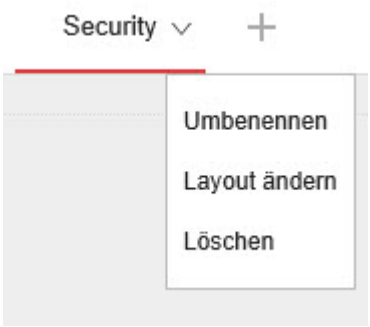
Prozedur

1. Gehen Sie zum **Fenster "Zusammenfassung"**.
2. So fügen Sie eine neue Registerkarte hinzu:
   a. Klicken Sie auf das Symbol zum Hinzufügen.

b. Geben Sie einen Namen für die neue Registerkarte ein.

3. So benennen Sie eine Registerkarte um:

a. Zeigen Sie mit der Maus auf den Registerkartennamen und klicken Sie auf den Pfeil nach unten.



b. Klicken Sie auf **Umbenennen** und geben Sie den neuen Registerkartennamen ein.

4. So ändern Sie das Layout der Widgets für eine Registerkarte:

a. Zeigen Sie mit der Maus auf den Registerkartennamen und klicken Sie auf den Pfeil nach unten.

b. Klicken Sie auf **Layout ändern**.

c. Wählen Sie das neue Layout aus dem daraufhin angezeigten Bildschirm aus.

d. Klicken Sie auf **Speichern**.

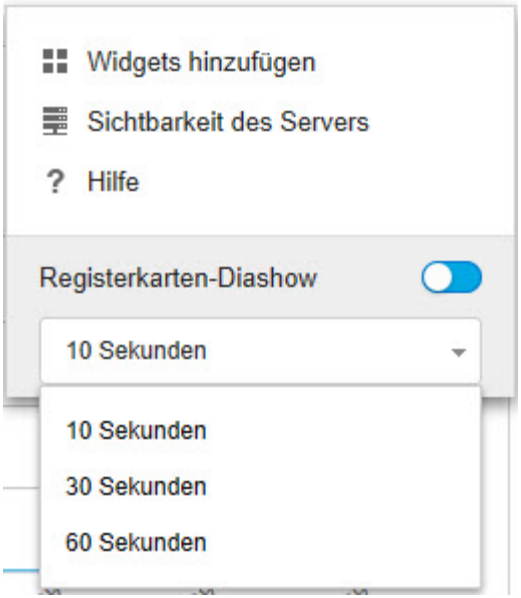
5. So löschen Sie eine Registerkarte:

a. Zeigen Sie mit der Maus auf den Registerkartennamen und klicken Sie auf den Pfeil nach unten.

b. Klicken Sie auf **Löschen** und bestätigen Sie den Vorgang.

6. So geben Sie eine Bildschirmpräsentation mit Registerkarte wieder:

a. Klicken Sie auf das Symbol **Einstellungen** rechts der Registerkartenanzeige.



b. Aktivieren Sie das Steuerelement **Registerkarten-Diashow**.

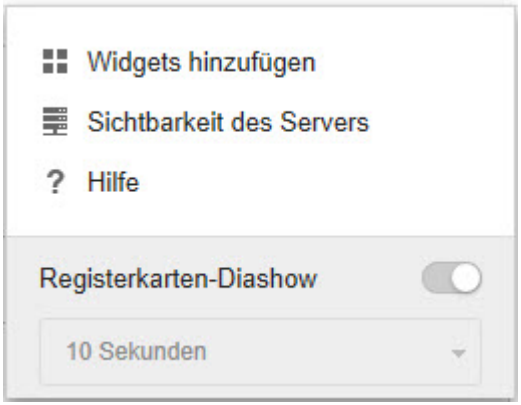
c. Wählen Sie vor dem Wechsel zur nächsten Registerkarte aus, wie lange jede Registerkarte angezeigt werden soll.

Arbeiten mit Widgets

Verwalten Sie Widgets durch Hinzufügen, Verschieben, Umbenennen und Löschen von Elementen sowie durch Größenänderung von Elementen.

Prozedur

1. Gehen Sie zum **Fenster "Zusammenfassung"**.
2. Klicken Sie auf eine Registerkarte.
3. So fügen Sie ein Widget hinzu:
   a. Klicken Sie auf das Symbol **Einstellungen** rechts der Registerkartenanzeige.



   b. Klicken Sie auf **Widgets hinzufügen**.
   c. Wählen Sie die hinzuzufügenden Widgets aus.
      - Wählen Sie in der Dropdown-Liste über den Widgets eine Kategorie aus, um die Auswahl einzugrenzen.
      - Suchen Sie mit dem Suchfeld im oberen Bereich des Bildschirms nach einem bestimmten Widget.
   d. Klicken Sie auf **Hinzufügen**.
4. Um ein Widget an eine andere Stelle in der gleichen Registerkarte zu verschieben, verschieben Sie es per Drag & Drop an die neue Stelle.
5. Ändern Sie die Größe von Widgets in einer mehrspaltigen Registerkarte, indem Sie mit dem Cursor auf den rechten Rand des Widgets zeigen und ihn dann nach links oder rechts bewegen.

6. So benennen Sie ein Widget um:

   a. Klicken Sie auf das Symbol "Einstellungen" (>).

   b. Geben Sie den neuen Titel ein.

   c. Klicken Sie auf **Speichern**.

7. Um ein Widget zu löschen, klicken Sie auf das Symbol zum Löschen (>).

Verfügbare Widgets

Folgende Widgets sind in dieser Version verfügbar.

Echtzeitsuche - Status

Mit dem Echtzeit-Status-Widget können Sie den Status des Smart Protection Servers überwachen.

Hinweis

Wenn dieses Widget in der Zusammenfassung angezeigt wird, läuft die Sitzung der Produktkonsole nicht ab. Der Computerstatus wird einmal pro Minute aktualisiert, was bedeutet, dass die Sitzung aufgrund der an den Server gesendeten Abfragen nicht abläuft. Die Sitzung läuft allerdings dennoch ab, wenn die Registerkarte ohne das Widget angezeigt wird.

TABELLE 3-1. Widget-Informationen

DATEN	BESCHREIBUNG
Dienst	Auf dem Smart Protection Server bereitgestellte Dienste.
Protokoll	Hier werden die von den Diensten unterstützten Protokolle angezeigt. File-Reputation-Dienste und Web-Reputation-Dienste unterstützen die Protokolle HTTP und HTTPS. HTTPS stellt eine sicherere Verbindung zur Verfügung, während HTTP weniger Bandbreite verwendet.

DATEN	BESCHREIBUNG
Host	Adressen des File-Reputation-Dienstes und des Web-Reputation-Dienstes. Diese Adressen werden bei solchen Trend Micro Produkten verwendet, die Smart Protection Server-Computer unterstützen. Mithilfe der Adressen werden Verbindungen zu Smart Protection Server-Computern konfiguriert.
Computerstatus	Die folgenden Punkte werden unter "Status" angezeigt: • **File-Reputation-Abfrage**: Zeigt an, ob File Reputation erwartungsgemäß funktioniert. • **Web-Reputation-Abfrage**: Zeigt an, ob Web Reputation erwartungsgemäß funktioniert. • **ActiveUpdate**: Zeigt an, ob ActiveUpdate erwartungsgemäß funktioniert. • **Durchschnittliche CPU-Auslastung**: Zeigt die durchschnittliche, vom Kernel generierte Computerauslastung während der letzten 1, 5 und 15 Minuten an. • **Freier Arbeitsspeicher**: Zeigt die verfügbare physische Speicherkapazität des Computers an. • **Belegung der Auslagerungsplatte**: Zeigt die Belegung der Auslagerungsplatte an. • **Freier Speicher**: Zeigt den verfügbaren Speicherplatz auf der Festplatte des Computers an.

Aktive Benutzer der File Reputation

Das Widget "Aktive Benutzer" zeigt die Anzahl der Benutzer an, die File-Reputation-Abfragen an Smart Protection Server gesendet haben. Jeder einzelne Client-Computer zählt als aktiver Benutzer.

Hinweis

Dieses Widget zeigt Informationen in einer 2D-Grafik an und wird stündlich aktualisiert. Sie können auch jederzeit auf das Symbol "Aktualisieren" ( ) klicken, um die Daten zu aktualisieren.

TABELLE 3-2. Widget-Informationen

DATEN	BESCHREIBUNG
Benutzer	Die Anzahl der Benutzer, die Abfragen an Smart Protection Server-Computer senden.
Datum und Uhrzeit	Datum der Abfrage.

Bericht über HTTP-Datenverkehr der File Reputation

Das Widget für den HTTP-Datenverkehrsbericht zeigt die Gesamtmenge des Datenverkehrs im Netzwerk in Kilobyte (KB) an, die aufgrund der File-Reputation-Abfragen durch Clients an den Smart Protection Server gesendet worden ist. Die Informationen in diesem Widget werden stündlich aktualisiert. Sie können auch jederzeit auf das Symbol "Aktualisieren" () klicken, um die Daten zu aktualisieren.

TABELLE 3-3. Widget-Informationen

DATEN	BESCHREIBUNG
Datenverkehr (KB)	Der durch Abfragen entstehende Datenverkehr im Netzwerk.
Datum und Uhrzeit	Datum der Abfragen.

Die 10 am häufigsten infizierten Computer für File Reputation

Dieses Widget zeigt die IP-Adressen der 10 am häufigsten als infiziert eingeordneten Computer an, nachdem der Smart Protection Server auf eine File-Reputation-Abfrage hin einen bekannten Virus erhalten hat. Die Informationen in diesem Widget werden in einer Tabelle zusammen mit der IP-Adresse des Computers und der Gesamtanzahl erkannter Bedrohungen auf jedem Computer angezeigt. Die Informationen in diesem Widget werden stündlich aktualisiert. Sie können auch jederzeit auf das Symbol "Aktualisieren" () klicken, um die Daten zu aktualisieren.

Mit diesem Widget ermitteln Sie, auf welchen Computern in Ihrem Netzwerk die meisten Virenvorfälle vorkommen.

Hinweis

Wenn Sie mehr als einen Smart Protection Server in diesem Widget aktivieren, errechnet das Widget die Gesamtanzahl erkannter Bedrohungen auf dem ausgewählten Smart Protection Server und zeigt die 10 meistinfizierten Computer der ausgewählten Smart Protection Server-Computer in der Liste an.

TABELLE 3-4. Widget-Informationen

DATEN	BESCHREIBUNG
IP	Die IP-Adresse des Computers
Erkannte Bedrohungen	Die Anzahl der von diesem Computer erkannten Sicherheitsbedrohungen

Aktive Benutzer der Web Reputation

Dieses Widget zeigt die Anzahl der Benutzer an, die Web-Reputation-Abfragen an die Smart Protection Server gesendet haben. Jeder einzelne Client-Computer zählt als aktiver Benutzer.

Hinweis

Dieses Widget zeigt Informationen in einer 2D-Grafik an und wird alle 5 Minuten aktualisiert. Sie können auch jederzeit auf das Symbol "Aktualisieren" ( ) klicken, um die Daten zu aktualisieren.

TABELLE 3-5. Widget-Informationen

DATEN	BESCHREIBUNG
Benutzer	Die Anzahl der Benutzer, die Abfragen an Smart Protection Server-Computer senden.
Datum und Uhrzeit	Datum der Abfrage.

Bericht über HTTP-Datenverkehr der Web Reputation

Das Widget für den HTTP-Datenverkehrsbericht zeigt die Gesamtmenge des Datenverkehrs im Netzwerk in Kilobyte (KB) an, die aufgrund der Web-Reputation-

Abfragen durch Clients an den Smart Protection Server gesendet worden ist. Die Informationen in diesem Widget werden stündlich aktualisiert. Sie können auch jederzeit auf das Symbol "Aktualisieren" () klicken, um die Daten zu aktualisieren.

TABELLE 3-6. Widget-Informationen

DATEN	BESCHREIBUNG
Datenverkehr (KB)	Der durch Abfragen entstehende Datenverkehr im Netzwerk.
Datum und Uhrzeit	Datum der Abfragen.

Die 10 am häufigsten gesperrten Computer für Web Reputation

Dieses Widget zeigt die IP-Adressen der 10 am häufigsten als gesperrt eingeordneten Computer an, nachdem der Smart Protection Server auf eine Web-Reputation-Abfrage hin eine URL erhalten hat. Die Informationen in diesem Widget werden in einer Tabelle zusammen mit der IP-Adresse des Computers und der Gesamtanzahl gesperrter URLs auf jedem Computer angezeigt. Die Informationen in diesem Widget werden täglich aktualisiert. Sie können auch jederzeit auf das Symbol "Aktualisieren" () klicken, um die Daten zu aktualisieren.

Mit diesem Widget ermitteln Sie, von welchen Computern in Ihrem Netzwerk aus am häufigsten auf gesperrte Websites zugegriffen wird.

Hinweis

Wenn Sie mehr als einen Smart Protection Server in diesem Widget aktivieren, errechnet das Widget die Gesamtanzahl erkannter Bedrohungen auf dem ausgewählten Smart Protection Server und zeigt die 10 meistblockierten Computer der ausgewählten Smart Protection Server-Computer in der Liste an.

TABELLE 3-7. Widget-Informationen

DATEN	BESCHREIBUNG
IP	Die IP-Adresse des Computers.

DATEN	BESCHREIBUNG
Erkannte Bedrohungen	Die Anzahl der auf diesem Computer gesperrten URLs.

Protokolle

Überwachen Sie den Status des Smart Protection Servers mit Hilfe von Protokollen. Um Protokollinformationen anzuzeigen, führen Sie eine Abfrage durch.

Gesperrte URLs

Im Fenster **Gesperrte URLs** werden Informationen über Abfragen der Web Reputation angezeigt, mit denen bösartige Ergebnisse zurückgegeben werden.

Folgende Optionen stehen auf dem Bildschirm zur Verfügung.

- **Schlüsselwort**: Geben Sie Schlüsselwörter an, die zum Suchen von URLs verwendet werden.
- **Datumsbereich**: Wählen Sie einen Datumsbereich.
- **Quelle**: Wählen Sie eine oder mehrere Quellen aus, um die entsprechenden Protokolle anzuzeigen.
    - **Benutzerdefinierte, gesperrte URLs**: Zeigt die gesperrten URLs an, die den benutzerdefinierten gesperrten URLs des Smart Protection Server entsprechen.
    - **Websperr-Pattern**: Zeigt die gesperrten URLs an, die Einträgen im Websperr-Pattern entsprechen.
    - **C&C-URLs übereinstimmend mit:** Zeigt die gesperrten URLs an, die Einträgen in den folgenden Quellen entsprechen:
        - **Apex Central – benutzerdefinierte, verdächtige Objekte**: Eine Teilmenge der benutzerdefinierten verdächtigen Objekte in Apex Central/Control Manager

- **Virtual Analyzer**: Eine Teilmenge der verdächtigen Objekte in Produkten, die mit Virtual Analyzer arbeiten, wie beispielsweise Deep Discovery Advisor, Deep Discovery Analyzer und Apex Central/Control Manager
- **Global Intelligence in Websperr-Pattern**: Trend Micro Smart Protection Network kompiliert die Global Intelligence-Liste aus weltweiten Quellen und testet und evaluiert die Risikostufe jeder C&C-Callback-Adresse. Mithilfe der Global Intelligence-Liste in Kombination mit den Reputationsbewertungen für bösartige Websites bietet Web-Reputation-Dienste mehr Sicherheit vor komplexen Bedrohungen. Die Web-Reputation-Sicherheitsstufe legt die Aktion fest, die basierend auf den zugewiesenen Risikostufen für bösartige Websites oder C&C-Server ergriffen wird.

Folgende Informationen werden auf diesem Bildschirm angezeigt:

- **Datum und Zeit**: Zeitpunkt, an dem ein URL gesperrt wurde.
- **URL**: Die gesperrte URL.
- **Protokoll anzeigen**: Zeigt Informationen zur Quelle der gesperrten URL an.
- **Client-GUID**: Die GUID des Computers, der versucht hat, auf den gesperrten URL zuzugreifen.
- **Server-GUID**: Die GUID des Trend Micro Produkts, das Smart Protection Server-Computer unterstützt.
- **Client-IP**: Die IP-Adresse des Computers, der versucht hat, auf den gesperrten URL zuzugreifen.
- **Computer**: Der Name des Computers, der versucht hat, auf den gesperrten URL zuzugreifen.
- **Produktelement**: Das Trend Micro Produkt, das den URL erkannt hat.

Update-Protokoll

Im Fenster "Update-Protokoll" werden Informationen über Pattern- oder Programmdatei-Updates angezeigt. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **Datumsbereich**: Wählen Sie den Datumsbereich, in dem das Update stattgefunden hat.
- **Typ**: Wählen Sie den Typ der Updates, die angezeigt werden sollen.

Protokolldetails:

- **Datum und Zeit**: Datum und Uhrzeit der Aktualisierung des Servers.
- **Komponentenname**: Die Komponente, die aktualisiert wurde.
- **Ergebnis**: Dies kann entweder "erfolgreich" oder "nicht erfolgreich" sein.
- **Beschreibung**: Eine Beschreibung des Update-Ereignisses.
- **Update-Methode**: Hierfür wird entweder "herkömmliche Suche" oder "intelligente Suche" angezeigt.

Protokoll 'Reputation-Dienst'

Im Fenster "Protokoll 'Reputation-Dienst'" werden Informationen zum Dienststatus von Web-Reputation und File-Reputation angezeigt. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **Dienst**: Geben Sie den Dienst an.
- **Ergebnis**: Geben Sie den Ergebnistyp an.
- **Datumsbereich**: Wählen Sie einen Datumsbereich.

Protokolldetails:

- **Datum und Zeit**: Datum und Uhrzeit der Überprüfung des Dienststatus für Web Reputation oder File Reputation.
- **Dienst**: Dies kann entweder "Web Reputation" oder "File Reputation" sein.

- **Ergebnis**: Dies kann entweder "erfolgreich" oder "nicht erfolgreich" sein.
- **Beschreibung**: Eine Beschreibung des Dienststatus für Web Reputation oder File Reputation.

Protokollwartung

Führen Sie eine Protokollwartung durch, um Protokolle zu löschen, die nicht mehr erforderlich sind. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **Pattern-Update-Protokoll**: Wählen Sie diese Option, um Protokolleinträge zu Pattern-Updates zu bereinigen.
- **Programm-Update-Protokoll**: Wählen Sie diese Option, um Protokolleinträge zu Programm-Updates zu bereinigen.
- **Gesperrte URLs** Wählen Sie diese Option, um Protokolleinträge zu URL-Abfragen zu bereinigen.
- **Protokoll "Reputation-Dienst"**: Wählen Sie diese Option, um Ereignisse des Reputation-Diensts zu bereinigen.
- **Alle Protokolle löschen**: Wählen Sie diese Option, um alle Protokolle zu löschen.
- **Protokolle bereinigen, die älter als die folgende Anzahl an Tagen sind**: Wählen Sie diese Option, um ältere Protokolle zu bereinigen.
- **Zeitgesteuerte Bereinigung aktivieren**: Wählen Sie diese Option, um eine automatische Bereinigung zu aktivieren.

Prozedur

1. Navigieren Sie zu **Protokolle** > **Protokollwartung**.
2. Wählen Sie die Protokollarten aus, die bereinigt werden sollen.
3. Wählen Sie, ob alle Protokolle oder nur Protokolle, die älter als eine bestimmte Anzahl von Tagen sind, gelöscht werden sollen.
4. Wählen Sie einen Bereinigungszeitplan, oder klicken Sie auf **Jetzt bereinigen**.

5. Klicken Sie auf **Speichern**.

Benachrichtigungen

Sie können den Smart Protection Server so konfigurieren, dass an bestimmte Personen E-Mails oder SNMP-Trap-Benachrichtigungen (Simple Network Management Protocol) gesendet werden, wenn sich der Status von Diensten oder Updates ändert.

E-Mail-Benachrichtigungen

Konfigurieren Sie die Einstellungen der E-Mail-Benachrichtigung, um Administratoren zu benachrichtigen, wenn es Statusänderungen im Zusammenhang mit Diensten oder Updates gibt. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **SMTP-Server**: Geben Sie die IP-Adresse des SMTP-Servers ein.
- **Portnummer**: Geben Sie die Portnummer des SMTP-Servers ein.
- **Von**: Geben Sie eine E-Mail-Adresse für das Absenderfeld von E-Mail-Benachrichtigungen ein.
- **Dienste**: Wählen Sie aus, ob Benachrichtigungen bei Statusänderungen in den Diensten File Reputation und Web Reputation und bei Pattern-Updates gesendet werden sollen.
- **An**: Geben Sie eine oder mehrere E-Mail-Adressen ein, an die Benachrichtigungen für dieses Ereignis gesendet werden sollen.
- **Betreff**: Geben Sie einen neuen Betreff ein, oder verwenden Sie einen Standardtext für dieses Ereignis.
- **Nachricht**: Geben Sie eine neue Nachricht ein, oder verwenden Sie einen Standardtext für dieses Ereignis.
- **File Reputation - Statusänderung**: Wählen Sie diese Option, um eine Benachrichtigung bei einer Statusänderung zu senden, und geben Sie den Empfänger für diese Benachrichtigung an.

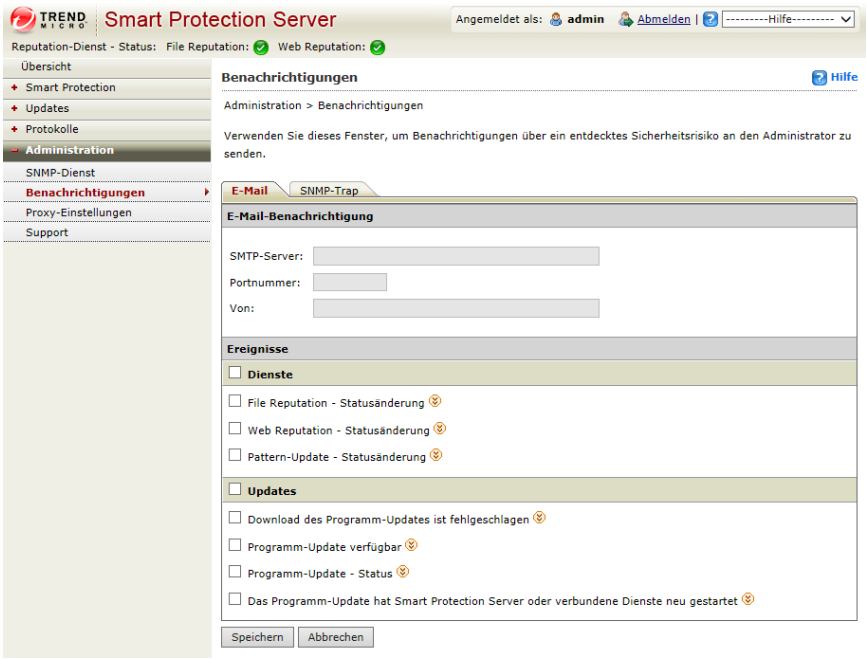
- **Web Reputation - Statusänderung**: Wählen Sie diese Option, um eine Benachrichtigung bei einer Statusänderung zu senden, und geben Sie den Empfänger für diese Benachrichtigung an.
- **Pattern-Update - Statusänderung**: Wählen Sie diese Option, um eine Benachrichtigung bei einer Statusänderung zu senden, und geben Sie den Empfänger für diese Benachrichtigung an.
- **Updates**: Wählen Sie diese Option, um Benachrichtigungen bei allen programmbezogenen Änderungen zu senden.
- **Download des Programm-Updates ist fehlgeschlagen**: Wählen Sie diese Option, um eine Benachrichtigung zu senden, wenn ein Programm-Update nicht erfolgreich heruntergeladen wurde, und geben Sie den Empfänger für diese Benachrichtigung an.
- **Programm-Update verfügbar**: Wählen Sie diese Option, um eine Benachrichtigung zu senden, wenn ein Programm-Update verfügbar und eine Bestätigung erforderlich ist, und geben Sie den Empfänger für diese Benachrichtigung an.
- **Programm-Update - Status**: Wählen Sie diese Option, um eine Benachrichtigung zu senden, wenn ein Programm aktualisiert wurde, und geben Sie den Empfänger für diese Benachrichtigung an.
- **Das Programm-Update hat Smart Protection Server oder verbundene Dienste neu gestartet**: Wählen Sie diese Option, um eine Benachrichtigung zu senden, wenn ein Programm-Update den Smart Protection Server oder dazugehörige Dienste neu gestartet hat, und geben Sie den Empfänger für diese Benachrichtigung an.
- **Standardmeldung**: Klicken Sie hierauf, um die Felder "Betreff" und "Nachricht" auf den Standardtext von Trend Micro zurückzusetzen.

E-Mail-Benachrichtigungen konfigurieren

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** und dann zur Registerkarte **E-Mail**.

   Die Registerkarte für E-Mail-Benachrichtigungen wird angezeigt.



2. Aktivieren Sie das Kontrollkästchen **Dienste**, um eine E-Mail-Benachrichtigung bei Statusänderungen für alle Dienste zu erhalten, oder wählen Sie die spezifischen Dienste aus den angezeigten Optionen aus:

   - **File Reputation - Statusänderung**: Wählen Sie diese Option, um eine Benachrichtigung bei einer Statusänderung zu senden, und geben Sie den Empfänger, den Betreff und die Nachricht an.
   - **Web Reputation - Statusänderung**: Wählen Sie diese Option, um eine Benachrichtigung bei einer Statusänderung zu senden, und geben Sie den Empfänger, den Betreff und die Nachricht an.

- **Pattern-Update - Statusänderung**: Wählen Sie diese Option, um eine Benachrichtigung bei einer Statusänderung zu senden, und geben Sie den Empfänger, den Betreff und die Nachricht an.

3. Aktivieren Sie das Kontrollkästchen **Updates** oder wählen Sie eine der folgenden Optionen aus:

   - **Download des Programm-Updates ist fehlgeschlagen**: Wählen Sie diese Option, um eine Benachrichtigung bei diesem Ereignis zu senden, und geben Sie den Empfänger, den Betreff und die Nachricht an.
   - **Programm-Update verfügbar**: Wählen Sie diese Option, um eine Benachrichtigung bei diesem Ereignis zu senden, und geben Sie den Empfänger, den Betreff und die Nachricht an.
   - **Programm-Update - Status**: Wählen Sie diese Option, um eine Benachrichtigung bei diesem Ereignis zu senden, und geben Sie den Empfänger, den Betreff und die Nachricht an.
   - **Das Programm-Update hat Smart Protection Server oder verbundene Dienste neu gestartet**: Wählen Sie diese Option, um eine Benachrichtigung bei diesem Ereignis zu senden, und geben Sie den Empfänger, den Betreff und die Nachricht an.

4. Geben Sie im Feld **SMTP-Server** die IP-Adresse des SMTP-Servers ein.
5. Geben Sie die SMTP-Portnummer ein.
6. Geben Sie eine E-Mail-Adresse in das Feld **Von** ein. Bei allen E-Mail-Benachrichtigungen wird diese Adresse im Feld 'Von' der E-Mail-Nachrichten angezeigt.
7. Klicken Sie auf **Speichern**.

SNMP-Trap-Benachrichtigungen

Konfigurieren Sie die Einstellungen der SNMP-Benachrichtigung (Simple Network Management Protocol), um Administratoren mit Hilfe von SNMP-Traps zu benachrichtigen, wenn es Statusänderungen im Zusammenhang mit Diensten gibt. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **IP-Adresse des Servers**: Geben Sie IP-Adresse des SNMP-Trap-Empfängers an.
- **Community-Name**: Geben Sie den SNMP-Community-Namen an.
- **Dienste**: Wählen Sie aus, ob eine SNMP-Benachrichtigung bei Statusänderungen in den Diensten File Reputation und Web Reputation und bei Pattern-Updates gesendet werden sollen.
- **Nachricht**: Geben Sie eine neue Nachricht ein, oder verwenden Sie einen Standardtext für dieses Ereignis.
- **File Reputation - Statusänderung**: Wählen Sie diese Option, um eine Benachrichtigung bei Statusänderungen zu senden.
- **Web Reputation - Statusänderung**: Wählen Sie diese Option, um eine Benachrichtigung bei Statusänderungen zu senden.
- **Pattern-Update - Statusänderung**: Wählen Sie diese Option, um eine Benachrichtigung bei Statusänderungen zu senden.
- **Standardmeldung**: Klicken Sie hierauf, um das Feld "Nachricht" auf den Standardtext von Trend Micro zurückzusetzen.

SNMP-Trap-Benachrichtigungen konfigurieren

Konfigurieren Sie die Einstellungen der SNMP-Benachrichtigung (Simple Network Management Protocol), um Administratoren mit Hilfe von SNMP-Traps zu benachrichtigen, wenn es Statusänderungen im Zusammenhang mit Diensten gibt.

Prozedur

1. Navigieren Sie zu **Administration** > **Benachrichtigungen** und dann zur Registerkarte **SNMP**.

Die Registerkarte für SNMP-Trap-Benachrichtigungen wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen **Dienste** oder eines der folgenden Kontrollkästchen:

   - **File Reputation - Statusänderung**: Wählen Sie diese Option, um eine Benachrichtigung bei einer Statusänderung zu senden, und geben Sie den Empfänger, den Betreff und die Nachricht an.
   - **Web Reputation - Statusänderung**: Wählen Sie diese Option, um eine Benachrichtigung bei einer Statusänderung zu senden, und geben Sie den Empfänger, den Betreff und die Nachricht an.
   - **Pattern-Update - Statusänderung**: Wählen Sie diese Option, um eine Benachrichtigung bei einer Statusänderung zu senden, und geben Sie den Empfänger, den Betreff und die Nachricht an.

3. Geben Sie die IP-Adresse des SNMP-Trap-Servers ein.

4. Geben Sie den SNMP-Community-Namen ein.

5. Klicken Sie auf **Speichern**.

Kapitel 4

Einbindung von Trend Micro Apex Central™/Control Manager™

Smart Protection Server wird in Apex Central/Control Manager integriert.

Es werden folgende Themen behandelt:

Info zu Apex Central/Control Manager

Trend MicroApex Central™/Control Manager™ ist eine zentrale Management-Konsole, mit der Produkte und Dienste von Trend Micro auf der Gateway-, Mailserver-, Dateiserver- und Unternehmensdesktopebene verwaltet werden können. Die webbasierte Management-Konsole von Apex Central/Control Manager bietet eine einzelne Überwachungsstelle für verwaltete Produkte und Dienste im ganzen Netzwerk.

Mit Apex Central/Control Manager können Systemadministratoren Aktivitäten wie z. B. Infektionen, Sicherheitsverletzungen oder Viruseintrittsstellen überwachen und Berichte dazu erstellen. Systemadministratoren können Komponenten herunterladen und im ganzen Netzwerk bereitstellen und so einen einheitlichen und aktuellen Schutz sicherstellen. Apex Central/Control Manager ermöglicht manuelle und geplante Updates sowie die Konfiguration und Verwaltung von Produkten als Gruppen oder als Einzelobjekte und bietet so eine größere Flexibilität.

Unterstützte Versionen von Apex Central/ Control Manager

Diese Version von Smart Protection Server unterstützt die folgenden Versionen von Apex Central/Control Manager.

Funktionen	Apex Central Version	Control Manager-Version		
	2019	7.0	6.0 SP3	6.0 SP2 oder früher
Verdächtige Objekte und Aktionen synchronisieren	Ja	Ja	Ja	Nein

Funktionen	Apex Central Version	Control Manager-Version		
	2019	7.0	6.0 SP3	6.0 SP2 oder früher
Apex Central/ Control Manager als alternative Update-Adresse verwenden	Ja	Ja	Ja	Ja

Hinweis

Smart Protection Server kann nur mit reinen IPv4-Netzwerken oder Dual-Stack-Netzwerken von Apex Central/Control Manager verbunden werden.

Einbindung von Apex Central/Control Manager in Smart Protection Server

Diese Version von Smart Protection Server unterstützt die folgenden Funktionen von Apex Central/Control Manager:

TABELLE 4-1. Einbindung von Apex Central/Control Manager

FUNKTION	BESCHREIBUNG
Synchronisierung verdächtiger Objekte und Aktionen	1. Apex Central/Control Manager fasst verdächtige Objekte und Suchaktionen zusammen und leitet diese Informationen dann an Smart Protection Server weiter. 2. Smart Protection Server leitet verdächtige URLs und Aktionen an Security Agents weiter. Bei Produkten, die Web-Reputation-Abfragen (wie Portal Protect und Deep Security) senden, leitet Smart Protection Server nur verdächtige URLs weiter. **Hinweis** • Weitere Informationen zur Verwaltung verdächtiger Objekte mit Apex Central finden Sie im *Apex Central-Administratorhandbuch*. Sie können eine PDF-Version des Handbuchs herunterladen oder das Handbuch online mithilfe des folgenden Links anzeigen: http://docs.trendmicro.com/de-de/enterprise/apex-central.aspx • Weitere Informationen dazu, wie Control Manager verdächtige Objekte behandelt, finden Sie im *Leitfaden zur verbundenen Bedrohungsabwehr* für Ihre Version von Control Manager unter dem folgenden Link: http://docs.trendmicro.com/de-de/enterprise/control-manager.aspx
Apex Central/ Control Manager als alternative Update-Adresse	Apex Central/Control Manager kann als Update-Adresse agieren, wenn Smart Protection Server über keine Internetverbindung verfügt.
Anmeldung über Einzelanmeldung	Apex Central/Control Manager ermöglicht Ihnen die Einzelanmeldung bei Smart Protection Server über die Konsole von Apex Central/Control Manager.

Kapitel 5

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 **Support kontaktieren** 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 Deutschland GmbH Zeppelinstraße 1 85399 Hallbergmoos Deutschland
Telefon	+49 (0) 811 88990-700
Website	http://www.trendmicro.de
E-Mail-Adresse	sales_info@trendmicro.de

- Weltweite Support-Büros:

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

- Kontaktaufnahme mit Trend Micro:

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

- Trend Micro Produktdokumentation:

  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.

Email Reputation Services

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

https://ers.trendmicro.com/

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

https://success.trendmicro.com/solution/1112106

File-Reputation-Dienste

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

https://success.trendmicro.com/solution/1059565

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

CLI-Befehle

In diesem Abschnitt werden die CLI-Befehle (Command Line Interface, Befehlszeilenschnittstelle) beschrieben, die Sie im Produkt zum Überwachen, Debuggen, Beheben von Fehlern und Konfigurieren verwenden können. Melden Sie sich mit Ihrem Admin-Konto an der CLI über die virtuelle Maschine an. Mit Hilfe von CLI-Befehlen können Administratoren Konfigurationsaufgaben, Debugging und Fehlerbehebung durchführen. Die CLI-Schnittstelle stellt auch zusätzliche Befehle zur Verfügung, um kritische Ressourcen und Funktionen zu überwachen. Um auf die CLI-Schnittstelle zuzugreifen, benötigen Sie das Administratorkonto und -kennwort.

BEFEHL	SYNTAX	BESCHREIBUNG
certificate regen self-sign	**certificate regen self-sign** <Ausgestellt_an> <Ausgestellt_von> <Gültigkeit>	Selbstsigniertes Zertifikat neu generieren. <Ausgestellt_an>: Allgemeiner Name oder CN des Empfängers des Zertifikats <Ausgestellt_von>: Allgemeiner Name oder CN des Ausstellers des Zertifikats <Gültigkeit>: Die Anzahl der Tage, die das Zertifikat gültig ist
certificate update CA	**certificate update CA**	Das neueste CA-Paket herunterladen

BEFEHL	SYNTAX	BESCHREIBUNG
configure date	**configure date** <Datum> <Uhrzeit>	Daten konfigurieren und im CMOS speichern date DATUMSFELD [DATUMSFELD] time ZEITFELD [ZEITFELD]
configure dns ipv4	**configure dns ipv4** <dns1> [dns2]	IPv4-DNS-Einstellungen konfigurieren dns1 IPv4_ADDR Primary DNS server dns2 IPv4_ADDR Secondary DNS server []
configure dns ipv6	**configure dns ipv6** <dns1> [dns2]	IPv6-DNS-Einstellungen konfigurieren dns1 IPv6_ADDR Primary DNS server dns2 IPv6_ADDR Secondary DNS server []
configure hostname	**configure hostname** <Host-Name>	Host-Namen konfigurieren hostname HOST-NAME Host-Name oder FQDN
configure ipv4 dhcp	**configure ipv4 dhcp [vlan]**	Standard-Ethernet-Schnittstelle für die Verwendung von DHCP konfigurieren vlan VLAN-ID VLan-ID [1-4094], Standard kein VLan: [0]
configure ipv4 static	**configure ipv4 static** <IP> <Maske> <Gateway> [VLan]	Standard-Ethernet-Schnittstelle für die Verwendung einer statischen IPv4-Adresse konfigurieren vlan VLAN-ID VLan-ID [1-4094], Standard kein VLan: [0]
configure ipv6 auto	**configure ipv6 auto** [vlan]	Standard-Ethernet-Schnittstelle für die Verwendung der automatischen Neighbor Discovery-IPv6-Adresse konfigurieren vlan VLAN-ID VLan-ID [1-4094], Standard kein VLan: [0]

Befehl	Syntax	Beschreibung
configure ipv6 dhcp	**configure ipv6 dhcp** [vlan]	Standard-Ethernet-Schnittstelle für die Verwendung der dynamischen IPv6-Adresse konfigurieren (DHCPv6) vlan VLAN-ID VLan-ID [1-4094], Standard kein VLan: [0]
configure ipv6 static	**configure ipv6 static** <v6ip> <v6mask> <v6gate> [vlan]	Standard-Ethernet-Schnittstelle für die Verwendung einer statischen IPv6-Adresse konfigurieren vlan VLAN-ID VLan-ID [1-4094], Standard kein VLan: [0]
configure locale de_DE	**configure locale de_DE**	Deutsch als Gebietsschema konfigurieren
configure locale en_US	**configure locale en_US**	Englisch als Gebietsschema konfigurieren
configure locale es_ES	**configure locale es_ES**	Spanisch als Gebietsschema konfigurieren
configure locale fr_FR	**configure locale fr_FR**	Französisch als Gebietsschema konfigurieren
configure locale it_IT	**configure locale it_IT**	Italienisch als Gebietsschema konfigurieren
configure locale ja_JP	**configure locale ja_JP**	Japanisch als Gebietsschema konfigurieren
configure locale ko_KR	**configure locale ko_KR**	Koreanisch als Gebietsschema konfigurieren
configure locale ru_RU	**configure locale ru_RU**	Russisch als Gebietsschema konfigurieren
configure locale zh_CN	**configure locale zh_CN**	Chinesisch (vereinfacht) als Gebietsschema konfigurieren
configure locale zh_TW	**configure locale zh_TW**	Chinesisch (traditionell) als Gebietsschema konfigurieren

BEFEHL	SYNTAX	BESCHREIBUNG
configure ntp	**configure ntp <IP oder FQDN>**	NTP-Server konfigurieren
configure port	**configure port <frs_http_port> <frs_https_port> <wrs_http_port>> <wrs_https_port>**	Dienstports der File-Reputation- und Web-Reputation-Dienste ändern.
configure password	**configure password** <Benutzer>	Kontokennwort konfigurieren Benutzer BENUTZER Der Benutzername, dessen Kennwort Sie ändern möchten. Der Benutzer kann "admin", "root" oder ein anderer Benutzer aus der Administratorgruppe des Smart Protection Servers sein.
configure proxy-service	**configure proxy-service** <wis_url> <cfr_url> <grid_url> <mars_url>	URLs des globalen Schutzdienstes von Trend Micro ändern. <wis_url>: URL für Web Inspection Service <cfr_url>: URL für Community File Reputation <grid_url>: URL für Goodware-Ressource und Informationsdatenbank <mars_url>: URL für Reputation-Dienste für mobile Apps
configure service	**configure service inter-face** <Name der Schnittstelle>	Standardeinstellungen des Servers konfigurieren
configure timezone Africa Cairo	**configure timezone Africa Cairo**	Zeitzone für den Standort Afrika/Kairo konfigurieren
configure timezone Africa Harare	**configure timezone Africa Harare**	Zeitzone für den Standort Afrika/Harare konfigurieren

BEFEHL	SYNTAX	BESCHREIBUNG
`configure timezone Africa Nairobi`	`configure timezone Africa Nairobi`	Zeitzone für den Standort Afrika/Nairobi konfigurieren
`configure timezone America Anchorage`	`configure timezone America Anchorage`	Zeitzone für den Standort Amerika/Anchorage konfigurieren
`configure timezone America Bogota`	`configure timezone America Bogota`	Zeitzone für den Standort Amerika/Bogota konfigurieren
`configure timezone America Buenos_Aires`	`configure timezone America Buenos_Aires`	Zeitzone für den Standort Amerika/Buenos Aires konfigurieren
`configure timezone America Caracas`	`configure timezone America Caracas`	Zeitzone für den Standort Amerika/Caracas konfigurieren
`configure timezone America Chicago`	`configure timezone America Chicago`	Zeitzone für den Standort Amerika/Chicago konfigurieren
`configure timezone America Chihuahua`	`configure timezone America Chihuahua`	Zeitzone für den Standort Amerika/Chihuahua konfigurieren
`configure timezone America Denver`	`configure timezone America Denver`	Zeitzone für den Standort Amerika/Denver konfigurieren
`configure timezone America Godthab`	`configure timezone America Godthab`	Zeitzone für den Standort Amerika/Godthab konfigurieren

BEFEHL	SYNTAX	BESCHREIBUNG
`configure timezone America Lima`	`configure timezone America Lima`	Zeitzone für den Standort Amerika/Lima konfigurieren
`configure timezone America Los_Angeles`	`configure timezone America Los_Angeles`	Zeitzone für den Standort Amerika/Los Angeles konfigurieren
`configure timezone America Mexico_City`	`configure timezone America Mexico_City`	Zeitzone für den Standort Amerika/Mexiko-Stadt konfigurieren
`configure timezone America New_York`	`configure timezone America New_York`	Zeitzone für den Standort Amerika/New York konfigurieren
`configure timezone America Noronha`	`configure timezone America Noronha`	Zeitzone für den Standort Amerika/Noronha konfigurieren
`configure timezone America Phoenix`	`configure timezone America Phoenix`	Zeitzone für den Standort Amerika/Phoenix konfigurieren
`configure timezone America Santiago`	`configure timezone America Santiago`	Zeitzone für den Standort Amerika/Santiago konfigurieren
`configure timezone America St_Johns`	`configure timezone America St_Johns`	Zeitzone für den Standort Amerika/St Johns konfigurieren

Befehl	Syntax	Beschreibung
`configure timezone America Tegucigalpa`	`configure timezone America Tegucigalpa`	Zeitzone für den Standort Amerika/Tegucigalpa konfigurieren
`configure timezone Asia Almaty`	`configure timezone Asia Almaty`	Zeitzone für den Standort Asien/Almaty konfigurieren
`configure timezone Asia Baghdad`	`configure timezone Asia Baghdad`	Zeitzone für den Standort Asien/Bagdad konfigurieren
`configure timezone Asia Baku`	`configure timezone Asia Baku`	Zeitzone für den Standort Asien/Baku konfigurieren
`configure timezone Asia Bangkok`	`configure timezone Asia Bangkok`	Zeitzone für den Standort Asien/Bangkok konfigurieren
`configure timezone Asia Calcutta`	`configure timezone Asia Calcutta`	Zeitzone für den Standort Asien/Kalkutta konfigurieren
`configure timezone Asia Colombo`	`configure timezone Asia Colombo`	Zeitzone für den Standort Asien/Colombo konfigurieren
`configure timezone Asia Dhaka`	`configure timezone Asia Dhaka`	Zeitzone für den Standort Asien/Dhaka konfigurieren
`configure timezone Asia Hong_Kong`	`configure timezone Asia Hong_Kong`	Zeitzone für den Standort Asien/Hongkong konfigurieren
`configure timezone Asia Irkutsk`	`configure timezone Asia Irkutsk`	Zeitzone für den Standort Asien/Irkutsk konfigurieren

BEFEHL	SYNTAX	BESCHREIBUNG
`configure timezone Asia Jerusalem`	`configure timezone Asia Jerusalem`	Zeitzone für den Standort Asien/Jerusalem konfigurieren
`configure timezone Asia Kabul`	`configure timezone Asia Kabul`	Zeitzone für den Standort Asien/Kabul konfigurieren
`configure timezone Asia Karachi`	`configure timezone Asia Karachi`	Zeitzone für den Standort Asien/Karatschi konfigurieren
`configure timezone Asia Katmandu`	`configure timezone Asia Katmandu`	Zeitzone für den Standort Asien/Kathmandu konfigurieren
`configure timezone Asia Krasnoyarsk`	`configure timezone Asia Krasnoyarsk`	Zeitzone für den Standort Asien/Krasnojarsk konfigurieren
`configure timezone Asia Kuala_Lumpur`	`configure timezone Asia Kuala_Lumpur`	Zeitzone für den Standort Asien/Kuala Lumpur konfigurieren
`configure timezone Asia Kuwait`	`configure timezone Asia Kuwait`	Zeitzone für den Standort Asien/Kuwait konfigurieren
`configure timezone Asia Magadan`	`configure timezone Asia Magadan`	Zeitzone für den Standort Asien/Magadan konfigurieren
`configure timezone Asia Manila`	`configure timezone Asia Manila`	Zeitzone für den Standort Asien/Manila konfigurieren
`configure timezone Asia Muscat`	`configure timezone Asia Muscat`	Zeitzone für den Standort Asien/Maskat konfigurieren

Befehl	Syntax	Beschreibung
`configure timezone Asia Rangoon`	`configure timezone Asia Rangoon`	Zeitzone für den Standort Asien/Rangun konfigurieren
`configure timezone Asia Seoul`	`configure timezone Asia Seoul`	Zeitzone für den Standort Asien/Seoul konfigurieren
`configure timezone Asia Shanghai`	`configure timezone Asia Shanghai`	Zeitzone für den Standort Asien/Shanghai konfigurieren
`configure timezone Asia Singapore`	`configure timezone Asia Singapore`	Zeitzone für den Standort Asien/Singapur konfigurieren
`configure timezone Asia Taipei`	`configure timezone Asia Taipei`	Zeitzone für den Standort Asien/Taipeh konfigurieren
`configure timezone Asia Tehran`	`configure timezone Asia Tehran`	Zeitzone für den Standort Asien/Teheran konfigurieren
`configure timezone Asia Tokyo`	`configure timezone Asia Tokyo`	Zeitzone für den Standort Asien/Tokio konfigurieren
`configure timezone Asia Yakutsk`	`configure timezone Asia Yakutsk`	Zeitzone für den Standort Asien/Jakutsk konfigurieren
`configure timezone Atlantic Azores`	`configure timezone Atlantic Azores`	Zeitzone für den Standort Atlantik/Azoren konfigurieren
`configure timezone Australia Adelaide`	`configure timezone Australia Adelaide`	Zeitzone für den Standort Australien/Adelaide konfigurieren

BEFEHL	SYNTAX	BESCHREIBUNG
`configure timezone Australia Brisbane`	`configure timezone Australia Brisbane`	Zeitzone für den Standort Australien/Brisbane konfigurieren
`configure timezone Australia Darwin`	`configure timezone Australia Darwin`	Zeitzone für den Standort Australien/Darwin konfigurieren
`configure timezone Australia Hobart`	`configure timezone Australia Hobart`	Zeitzone für den Standort Australien/Hobart konfigurieren
`configure timezone Australia Melbourne`	`configure timezone Australia Melbourne`	Zeitzone für den Standort Australien/Melbourne konfigurieren
`configure timezone Australia Perth`	`configure timezone Australia Perth`	Zeitzone für den Standort Australien/Perth konfigurieren
`configure timezone Europe Amsterdam`	`configure timezone Europe Amsterdam`	Zeitzone für den Standort Europa/Amsterdam konfigurieren
`configure timezone Europe Athens`	`configure timezone Europe Athens`	Zeitzone für den Standort Europa/Athen konfigurieren
`configure timezone Europe Belgrade`	`configure timezone Europe Belgrade`	Zeitzone für den Standort Europa/Belgrad konfigurieren

Befehl	Syntax	Beschreibung
`configure timezone Europe Berlin`	`configure timezone Europe Berlin`	Zeitzone für den Standort Europa/Berlin konfigurieren
`configure timezone Europe Brussels`	`configure timezone Europe Brussels`	Zeitzone für den Standort Europa/Brüssel konfigurieren
`configure timezone Europe Bucharest`	`configure timezone Europe Bucharest`	Zeitzone für den Standort Europa/Bukarest konfigurieren
`configure timezone Europe Dublin`	`configure timezone Europe Dublin`	Zeitzone für den Standort Europa/Dublin konfigurieren
`configure timezone Europe Moscow`	`configure timezone Europe Moscow`	Zeitzone für den Standort Europa/Moskau konfigurieren
`configure timezone Europe Paris`	`configure timezone Europe Paris`	Zeitzone für den Standort Europa/Paris konfigurieren
`configure timezone Pacific Auckland`	`configure timezone Pacific Auckland`	Zeitzone für den Standort Pazifik/Auckland konfigurieren
`configure timezone Pacific Fiji`	`configure timezone Pacific Fiji`	Zeitzone für den Standort Pazifik/Fidschi konfigurieren
`configure timezone Pacific Guam`	`configure timezone Pacific Guam`	Zeitzone für den Standort Pazifik/Guam konfigurieren

BEFEHL	SYNTAX	BESCHREIBUNG
`configure timezone Pacific Honolulu`	`configure timezone Pacific Honolulu`	Zeitzone für den Standort Pazifik/Honolulu konfigurieren
`configure timezone Pacific Kwajalein`	`configure timezone Pacific Kwajalein`	Zeitzone für den Standort Pazifik/Kwajalein konfigurieren
`configure timezone Pacific Midway`	`configure timezone Pacific Midway`	Zeitzone für den Standort Pazifik/Midway konfigurieren
`configure timezone US Alaska`	`configure timezone US Alaska`	Zeitzone für den Standort USA/Alaska konfigurieren
`configure timezone US Arizona`	`configure timezone US Arizona`	Zeitzone für den Standort USA/Arizona konfigurieren
`configure timezone US Central`	`configure timezone US Central`	Zeitzone für den Standort USA/Central konfigurieren
`configure timezone US East-Indiana`	`configure timezone US East-Indiana`	Zeitzone für den Standort USA/East-Indiana konfigurieren
`configure timezone US Eastern`	`configure timezone US Eastern`	Zeitzone für den Standort USA/Ostküste konfigurieren
`configure timezone US Hawaii`	`configure timezone US Hawaii`	Zeitzone für den Standort USA/Hawaii konfigurieren
`configure timezone US Mountain`	`configure timezone US Mountain`	Zeitzone für den Standort USA/Mountain konfigurieren

BEFEHL	SYNTAX	BESCHREIBUNG
configure timezone US Pacific	**configure timezone US Pacific**	Zeitzone für den Standort USA/Pazifik konfigurieren
disable adhoc-query	**disable adhoc-query**	Internet-Zugriffsprotokoll deaktivieren
disable ssh	**disable ssh**	sshd-Daemon deaktivieren
enable	**enable**	Administrative Befehle aktivieren
enable adhoc-query	**enable adhoc-query**	Internet-Zugriffsprotokoll aktivieren
enable ssh	**enable ssh**	sshd-Daemon aktivieren
exit	**exit**	Sitzung beenden
Hilfe	**Hilfe**	Übersicht über die CLI-Syntax anzeigen.
history	**history** `[limit]`	In dieser Befehlszeilensitzung verwendete Befehle anzeigen `Limit`gibt die Anzahl der anzuzeigenden CLI-Befehle an. Beispiel: Die Angabe von „5“ für `Limit` bedeutet, dass 5 CLI-Befehle angezeigt werden.
reboot	**reboot** `[Zeit]`	Computer nach einer angegebenen Verzögerung oder sofort neu starten `Zeit` EINHEIT Zeit in Minuten, bis der Computer neu gestartet wird [0]
show date	**show date**	Aktuelles Datum und aktuelle Uhrzeit anzeigen
show hostname	**show hostname**	Netzwerk-Host-Namen anzeigen
show interfaces	**show interfaces**	Informationen zu den Netzwerkschnittstellen anzeigen
show ipv4 address	**show ipv4 address**	IPv4-Adresse des Netzwerks anzeigen

BEFEHL	SYNTAX	BESCHREIBUNG
`show ipv4 dns`	`show ipv4 dns`	IPv4-DNS-Server des Netzwerks anzeigen
`show ipv4 gateway`	`show ipv4 gateway`	IPv4-Gateway des Netzwerks anzeigen
`show ipv4 route`	`show ipv4 route`	IPv4-Routing-Tabelle des Netzwerks anzeigen
`show ipv4 type`	`show ipv4 type`	IPv4-Konfigurationstyp des Netzwerks anzeigen (dhcp / static)
`show ipv6 address`	`show ipv6 address`	IPv6-Adresse des Netzwerks anzeigen
`show ipv6 dns`	`show ipv6 dns`	IPv6-DNS-Server des Netzwerks anzeigen
`show ipv6 gateway`	`show ipv6 gateway`	IPv6-Gateway des Netzwerks anzeigen
`show ipv6 route`	`show ipv6 route`	IPv6-Routing-Tabelle des Netzwerks anzeigen
`show ipv6 type`	`show ipv6 type`	IPv6-Konfigurationstyp des Netzwerks anzeigen (auto / dhcp / static)
`show timezone`	`show timezone`	Zeitzone des Netzwerks anzeigen
`show uptime`	`show uptime`	Betriebszeit des Systems anzeigen
`show url management`	`show url management`	URL der Webverwaltungskonsole anzeigen
`show url FileReputationService`	`show url FileReputationService`	Endpunkt-Verbindungsadressen für File-Reputation-Dienste anzeigen
`show url WebReputationService`	`show url WebReputationService`	Endpunkt-Verbindungsadressen für Web-Reputation-Dienste anzeigen

BEFEHL	SYNTAX	BESCHREIBUNG
shutdown	**shutdown** [Zeit]	Computer nach einer angegebenen Verzögerung oder sofort herunterfahren Zeit EINHEIT Zeit in Minuten, bis der Computer heruntergefahren wird [0]

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: APGM38866/191126