TREND MICRO™

3.0

TREND MICRO™ Smart Protection Server

Administratorhandbuch

Security Made Smarter

Dokument-Nr.: APEM36294/140116

Release-Datum: März 2014

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

Diese Dokumentation enthält eine Beschreibung der wesentlichen Funktionen des Produkts/Services und/oder Installationsanweisungen für eine Produktionsumgebung. Lesen Sie die Dokumentation vor der Installation oder Verwendung des Produkts/Services aufmerksam durch.

Ausführliche Informationen über die Verwendung bestimmter Funktionen des Produkts/Services finden Sie im Trend Micro Online Help Center und/oder der Knowledge Base von Trend Micro.

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

Bewerten Sie diese Dokumentation auf der folgenden Website:

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

Inhaltsverzeichnis

Vorwort

Vorwort v

Info über Trend Micro vi

Produktdokumentation vi

Zielgruppe vi

Dokumentationskonventionen vii

Kapitel 1: Einführung

Wie funktioniert der Trend Micro Smart Protection Server? 1-2

- Die Notwendigkeit einer neuen Lösung 1-2
- Lösungen auf Basis des Smart Protection Network 1-3

Was ist neu in dieser Version? 1-8

Wichtigste Funktionen und Vorteile 1-10

Trend Micro Smart Protection Network 1-11

- File-Reputation-Dienste 1-12
- Web-Reputation-Dienste 1-12
- Smart Feedback 1-13

Kapitel 2: Smart Protection Server verwenden

Produktkonsole verwenden 2-2

- Auf die Produktkonsole zugreifen 2-3

Smart Protection verwenden 2-3

- Reputation-Dienste verwenden 2-3
- Liste "Zulässige/Gesperrte URL" konfigurieren 2-6
- C&C-Kontaktalarmdienste konfigurieren 2-7
- Smart Feedback aktivieren 2-9

Updates 2-10

- Manuelle Updates konfigurieren 2-10
- Zeitgesteuerte Updates konfigurieren 2-11

Updates der Pattern-Dateien 2-11
Updates der Programmdateien 2-12
Eine Update-Adresse konfigurieren 2-15

Administrative Aufgaben 2-16
SNMP-Dienst 2-16
Proxy-Einstellungen 2-21
Support 2-23

Kennwort der Produktkonsole ändern 2-23

Kapitel 3: Smart Protection Server überwachen

Fenster "Zusammenfassung" verwenden 3-2
Registerkarten 3-3
Widgets 3-6

Protokolle 3-15
Protokoll 'Gesperrter Internet-Zugriff' 3-15
Update-Protokoll 3-17
Protokoll 'Reputation-Dienst' 3-17
Protokollwartung 3-18

Benachrichtigungen 3-19
E-Mail-Benachrichtigungen 3-19
SNMP-Trap-Benachrichtigungen 3-22

Kapitel 4: Hilfe anfordern

Support-Portal verwenden 4-2
Bekannte Probleme 4-2
Hotfixes, Patches und Service Packs 4-3

Bedrohungsenzyklopädie 4-3

Kontaktaufnahme mit Trend Micro 4-4
Problemlösung beschleunigen 4-5

TrendLabs 4-5

Anhang A: CLI-Befehle

Anhang B: Glossar

Stichwortverzeichnis

Stichwortverzeichnis IN-1

Vorwort

Vorwort

Willkommen beim Smart Protection Server™ Administratorhandbuch. Dieses Dokument enthält Informationen über die Produkteinstellungen.

Es werden folgende Themen behandelt:

- *Info über Trend Micro auf Seite vi*
- *Produktdokumentation auf Seite vi*
- *Zielgruppe auf Seite vi*
- *Dokumentationskonventionen auf Seite vii*

Info über Trend Micro

Trend Micro Incorporated 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 den Trend Micro™ Smart Protection Server™.

Es werden folgende Themen behandelt:

- *Wie funktioniert der Trend Micro Smart Protection Server? auf Seite 1-2*
- *Was ist neu in dieser Version? auf Seite 1-8*
- *Wichtigste Funktionen und Vorteile auf Seite 1-10*
- *Trend Micro Smart Protection Network auf Seite 1-11*

Wie funktioniert der Trend Micro Smart Protection Server?

Trend Micro™ 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 Trend Micro 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 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 der 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 den Smart Protection Server zu senden. Bei dieser Lösung werden Identifikationsdaten, die mit Hilfe der Trend Micro Technologie ermittelt wurden, von den Agents an Smart Protection Server 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

Der webbasierte Abfrageprozess nutzt kleine, lokale Pattern-Dateien in Kombination mit einem System für Internet-Abfragen in Echtzeit. Das Internet-Abfragesystem verifiziert Dateien, URLs und andere Komponenten während des Verifizierungsprozesses mit Hilfe eines Smart Protection Servers. Smart Protection Server nutzen verschiedene Algorithmen für eine effiziente Verarbeitung, bei der möglichst wenig Bandbreite benötigt wird.

Es stehen drei Pattern-Dateien zur Verfügung:

- **Pattern der intelligenten Suche**: Dieses Pattern wird auf Smart Protection Server heruntergeladen und steht dort und im Trend Micro Smart Protection Network zur Verfügung. Diese Datei wird stündlich aktualisiert.
- **Smart Scan Agent-Pattern**: Dieses Pattern wird lokal auf den Endpunkten gespeichert und für Suchvorgänge verwendet, bei denen Smart Protection Server nicht erforderlich sind. Diese Datei wird täglich aktualisiert.
- **Websperrliste**: Smart Protection Server laden dieses Pattern von Trend Micro ActiveUpdate Servern herunter. Dieses Pattern wird für Web-Reputation-Abfragen verwendet.

Pattern-Update-Prozess

Pattern-Updates erfolgen als Reaktion auf Sicherheitsbedrohungen. Das Smart Protection Network und die Smart Protection Server laden die Pattern-Datei der intelligenten Suche von den ActiveUpdate Servern herunter. Trend Micro Produkte, die Smart Protection Server 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 unterstützen. Externe Endpunkte sind Endpunkte außerhalb des Intranets, die keine Verbindung zu

Smart Protection Servern oder Trend Micro Produkten haben, die Smart Protection Server unterstützen.

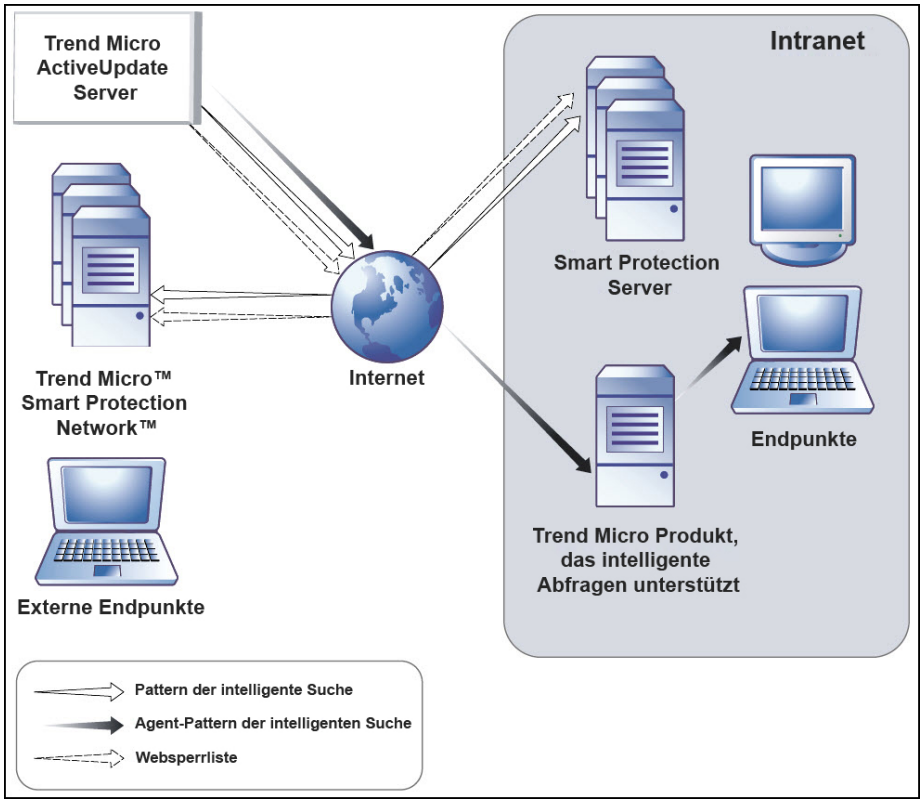


ABBILDUNG 1-1. Pattern-Update-Prozess

Der Abfrageprozess

Endpunkte, die sich zurzeit in Ihrem Intranet befinden, nutzen für Abfragen die Smart Protection Server. 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 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 1-1. 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 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 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 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 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 installieren, um die Kontinuität des Schutzes sicherzustellen, falls die Verbindung zu einem Smart Protection Server nicht verfügbar ist.

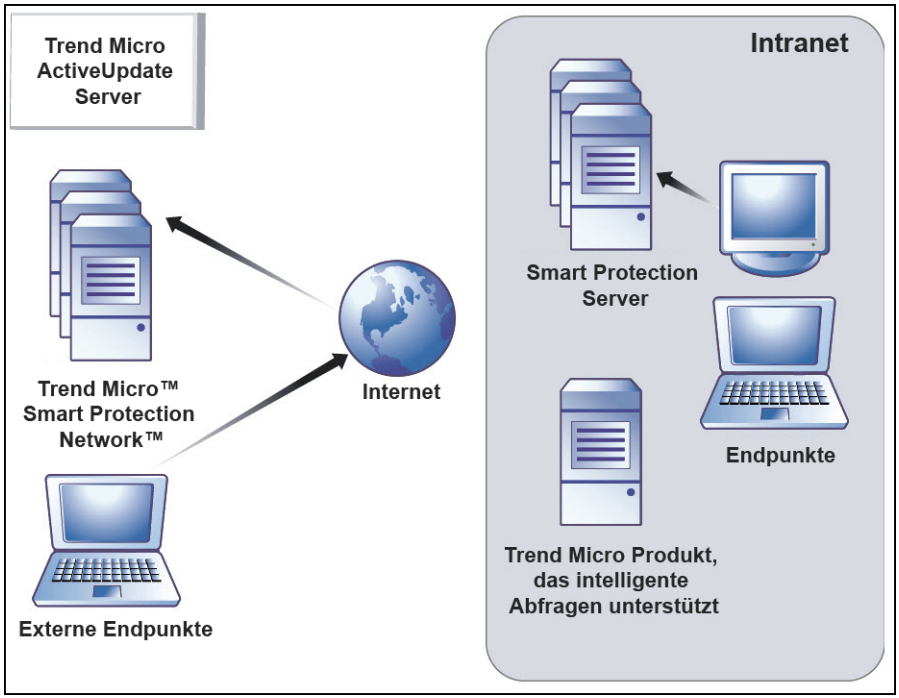


ABBILDUNG 1-2. Abfrageprozess

Was ist neu in dieser Version?

Trend Micro™ Smart Protection Server™ umfasst die folgenden neuen Funktionen und Verbesserungen:

TABELLE 1-2. Neu in Version 3.0

FUNKTION	BESCHREIBUNG
Verbesserte Pattern-Leistung	Die Leistung der File-Reputation- und Web-Reputation-Dienste wurde verbessert, um den Arbeitsspeicherbedarf beim Laden von Pattern zu reduzieren. • Web-Reputation-Dienste Web-Reputation-Dienste wurden verbessert, indem nun inkrementelle Updates für die Websperrliste zulässig sind. Dadurch wird der Bedarf an Arbeitsspeicher und Netzwerkbandbreite beim Laden der Websperrliste reduziert. • File-Reputation-Dienste Die Protokollimportfunktion für File-Reputation-Dienste wurde verbessert, um die Datenbank direkt vom Webserver aus aktualisieren zu können. Dadurch wird Folgendes sichergestellt: • Zugriffsprotokolle werden nun in Echtzeit in die Datenbank importiert, die Verarbeitungszeit für Daten wurde reduziert und die Festplatten-E/A-Leistung wurde verbessert. • Reduzierung bei der Serverauslastung und der Ressourcennutzung.
Verbesserte Kapazität	Ein eigenständiger Smart Protection Server unterstützt nun bis zu 25,000 Trend Micro™ OfficeScan™ 11 Agents.

FUNKTION	BESCHREIBUNG
Dashboard-Erweiterung	• Es gibt neue Layouts und Tabellen für Widgets. • Widgets rufen nun die Daten täglich vom Webserver ab. • Zeitüberschreitungsprobleme und einige kleinere Bugs wurden behoben.
Neue Management Information Base (MIB) für Systeminformationen	Smart Protection Server-Systeminformationen können nun direkt über ein MIB-Browsertool eines Drittanbieters abgefragt werden. Hierzu zählen: • SNMP MIB-2-System (1.3.6.1.2.1.1) • SNMP MIB-2-Schnittstellen (1.3.6.1.2.1.2) Weitere Informationen finden Sie unter *Unterstützte MIBs auf Seite 2-20*.
Neue CLI-Befehle	Es werden neue Befehle für folgende Aufgaben bereitgestellt: • Einrichten eines NTP-Servers (`configure ntp`) • Ändern des Dienstports (`configure port`) **Wichtig** Verwenden Sie diesen Befehl nur, wenn ein Konflikt mit dem aktuellen Dienstport auftritt. Weitere Informationen finden Sie unter *CLI-Befehle auf Seite A-1*.
Verbesserte Funktionen für virtuelle Maschinen	• Smart Protection Server unterstützt nun den VMware VMXNET 3-Netzwerkadapter in einer IPv6-Umgebung. • Das IPv6-Problem beim Microsoft Hyper-V-Netzwerkadapter in Kombination mit der Linux-Kernelversion 5.8 wurde behoben.

TABELLE 1-3. Neu in Version 2.6 Patch 1

FUNKTION	BESCHREIBUNG
Integration von Deep Discovery Advisor und die Virtual Analyzer Liste	Smart Protection Server können mit Deep Discovery Advisor integriert werden, um die Virtual Analyzer C&C-Serverliste zu erhalten. Deep Discovery Advisor Virtual Analyzer wertet potenzielle Risiken in einer sicheren Umgebung aus und weist den analysierten Bedrohungen mit Hilfe leistungsfähiger heuristischer Verfahren und Verhaltenstests eine Risikostufe zu. Virtual Analyzer füllt die Virtual Analyzer Liste mit allen Bedrohungen, die versuchen, eine Verbindung mit einem möglichen C&C-Server herzustellen. Die Virtual Analyzer Liste ist hochgradig firmenspezifisch und bietet eine anpassbare Verteidigungsmöglichkeit gegen gezielte Angriffe. Smart Protection Server rufen die Liste von Deep Discovery Advisor ab und bewerten alle potenziellen C&C-Bedrohungen auf Basis von Global Intelligence und der lokalen Virtual Analyzer Liste.

TABELLE 1-4. Neu in Version 2.6

FUNKTION	BESCHREIBUNG
Dashboard-Erweiterung	Das Dashboard kann jetzt auf Geräten angezeigt werden, die Adobe™ Flash™ Player nicht unterstützen.
Kleine Probleme behoben	Trend Micro hat einige kleinere Probleme behoben.

Wichtigste Funktionen und Vorteile

Trend Micro 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 Trend Micro™ Smart Protection Server™.

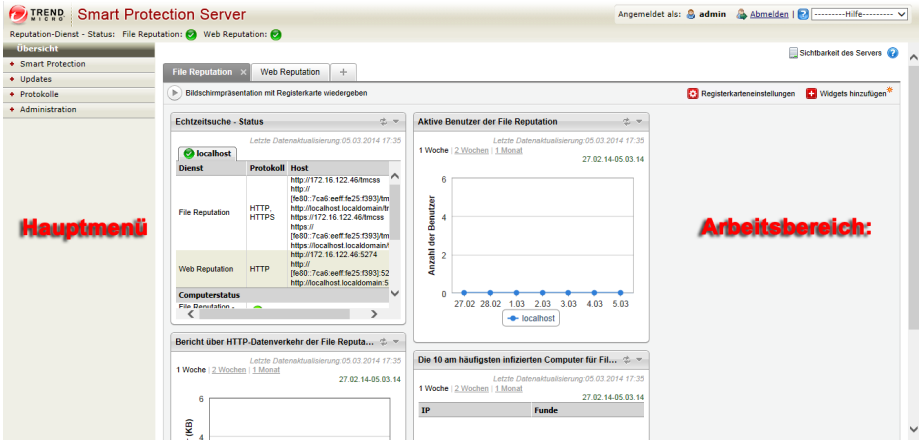
Es werden folgende Themen behandelt:

- *Produktkonsole verwenden auf Seite 2-2*
- *Smart Protection verwenden auf Seite 2-3*
- *Updates auf Seite 2-10*
- *Administrative Aufgaben auf Seite 2-16*
- *Proxy-Einstellungen auf Seite 2-21*
- *Kennwort der Produktkonsole ändern auf Seite 2-23*

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, Datenverkehr und Funde an, wenn Sie Widgets hinzufügen.
Smart Protection	Bietet Optionen zum Konfigurieren der Reputation-Dienste, eine Liste zulässiger/gesperrter URLs sowie Smart Feedback.
Updates	Bietet Optionen zum Konfigurieren zeitgesteuerter Updates, manueller Programm-Updates, Uploads von Programmpaketen sowie der Update-Adresse.

MENÜ	BESCHREIBUNG
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 wird im ersten Fenster eine Statusübersicht für Smart Protection Server angezeigt.

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

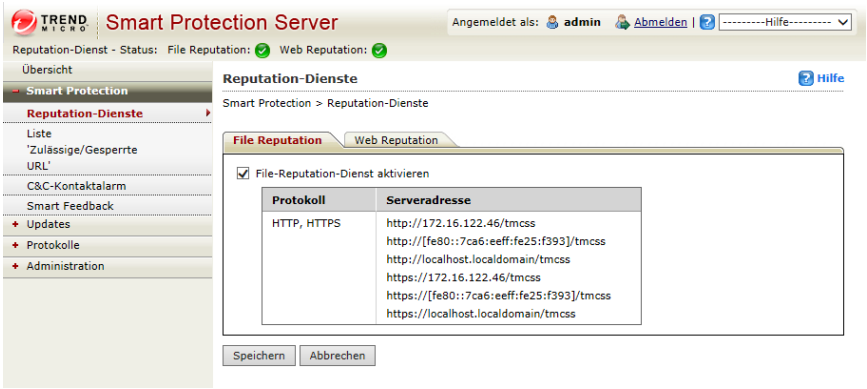
Aktivieren Sie die Reputation-Dienste über die Produktkonsole, damit andere Trend Micro Produkte Smart Protection verwenden können.

File-Reputation-Dienste aktivieren

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

Prozedur

1. Navigieren Sie zu **Smart Protection** > **Reputation-Dienste**, und klicken Sie dann auf die 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 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 dann auf die Registerkarte **Web Reputation**.

2. Aktivieren Sie das Kontrollkästchen **Web-Reputation-Dienst aktivieren**.
3. (Optional) Geben Sie die Priorität der Liste "Zulässige/Gesperrte URL" beim Filtern von URLs an.
4. Klicken Sie auf **Speichern**.

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

Liste "Zulässige/Gesperrte URL" konfigurieren

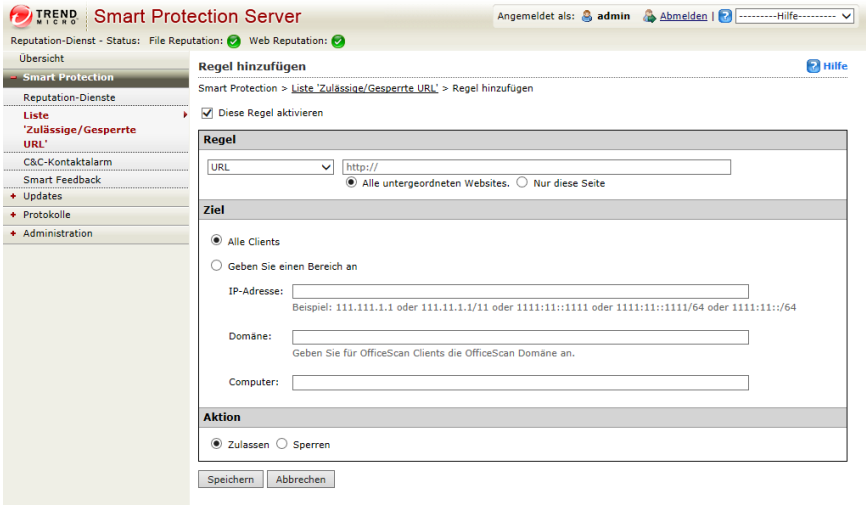
Die Liste "Zulässige/Gesperrte URL" ermöglicht Ihnen, eine benutzerdefinierte Liste von zulässigen und/oder gesperrten URLs anzugeben. Diese Liste wird für die Web Reputation verwendet. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **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** > **Liste 'Zulässige/Gesperrte URL'**.
2. Klicken Sie 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 Endpunkte**: Zur Übernahme auf alle Endpunkte.
   - **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**.

C&C-Kontaktalarmdienste konfigurieren

Trend Micro Command & Control (C&C)-Kontaktalarmdienste bieten verbesserte Erkennungs- und Warnungsfunktionen zur Minderung des Schadens infolge von erweiterten permanenten Bedrohungen und gezielten Angriffen. C&C-Kontaktalarmdienste sind in die Web-Reputation-Dienste integriert, wodurch die durchzuführende Aktion der erkannten Callback-Adresse basierend auf der Sicherheitsstufe der Web Reputation ermittelt wird.

Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **Server**: Der Servername oder die IP-Adresse des Deep Discovery Advisor Servers, der die Virtual Analyzer C&C-Liste bereitstellt.

- **API-Schlüssel**: Der API-Schlüssel von Deep Discovery Advisor. Der API-Schlüssel befindet sich auf der Seite **Info** der Webkonsole von Deep Discovery Advisor.
- **Verbindung testen**: Mit dieser Schaltfläche können Sie verifizieren, ob der Servername bzw. die IP-Adresse und der API-Schlüssel von Deep Discovery Advisor korrekt sind.
- **Registrieren**: Mit dieser Schaltfläche registrieren Sie den Smart Protection Server bei Deep Discovery Advisor.
- **Registrierung aufheben**: Mit dieser Schaltfläche heben Sie die Registrierung des Smart Protection Server bei Deep Discovery Advisor auf.
- **Virtual Analyzer C&C-Liste aktivieren**: Aktivieren Sie diese Option, um dem Smart Protection Server zu erlauben, die benutzerdefinierte C&C-Liste zu verwenden, die vom Deep Discovery Advisor Server analysiert wurde.
- **Jetzt synchronisieren**: Mit dieser Schaltfläche rufen Sie eine aktualisierte Virtual Analyzer C&C-Liste von Deep Discovery Advisor ab.

Prozedur

1. Geben Sie den Servernamen oder die IP-Adresse des Deep Discovery Advisor Server ein.

   Hinweis

   Der Servername muss im FQDN-Format und die IP-Adresse im IPv4-Format angegeben werden.

2. Geben Sie den API-Schlüssel ein.
3. Klicken Sie auf **Registrieren**, um eine Verbindung zum Deep Discovery Advisor Server herzustellen.

   Hinweis

   Administratoren können die Verbindung zum Server testen, bevor sie sich beim Server registrieren.

4. Wählen Sie **Virtual Analyzer C&C-Liste aktivieren**, um unterstützten Servern zu erlauben, die benutzerdefinierte C&C-Liste zu verwenden, die vom lokalen Deep Discovery Advisor Server analysiert wurde.

   Hinweis

   Die Option **Virtual Analyzer C&C-Liste aktivieren** ist erst verfügbar, nachdem eine Verbindung zum Deep Discovery Advisor Server hergestellt wurde.

5. 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 davor schützen kann. Sie können Smart Feedback jederzeit über diese Konsole deaktivieren.

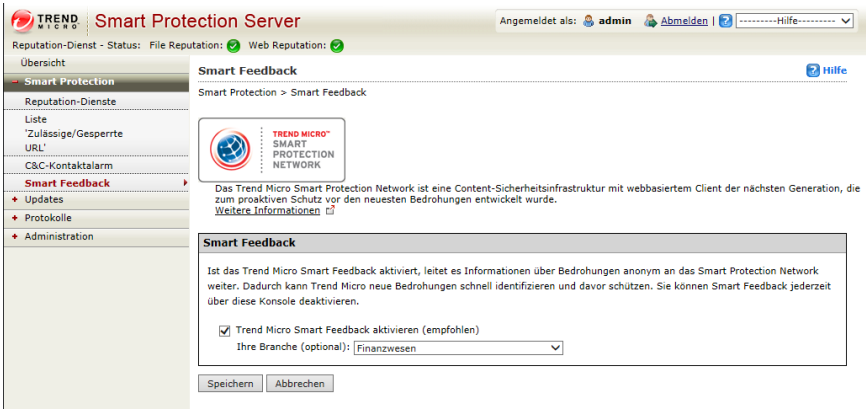
Prozedur

1. Navigieren 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**.



3. Wählen Sie Ihre Branche.

4. Klicken Sie auf **Speichern**.

Updates

Die Wirksamkeit des Smart Protection Servers hängt davon ab, ob die aktuellen Pattern-Dateien und Komponenten verwendet werden. Trend Micro veröffentlicht stündlich neue Versionen der Smart Scan Pattern-Dateien.

Tipp

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

Manuelle Updates konfigurieren

Sie können auch manuelle Updates für das Pattern der intelligenten Suche und die Websperrliste durchführen.

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

Der Smart Protection Server kann zeitgesteuerte Updates für das Pattern der intelligenten Suche und die Websperrliste 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.

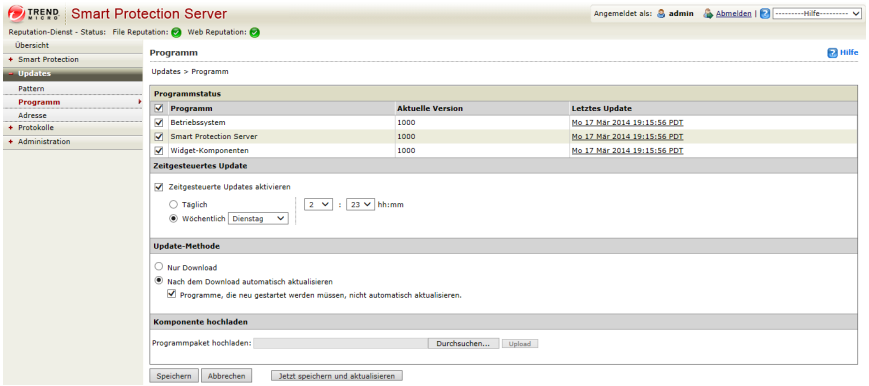
- **Betriebssystem**: Wählen Sie diese Option, um Betriebssystemkomponenten zu aktualisieren.
- **Smart Protection Server**: Wählen Sie diese Option, um die Programmdatei des Servers zu aktualisieren.
- **Widget-Komponenten**: Wählen Sie diese Option, um Widgets zu aktualisieren.
- **Zeitgesteuerte Updates 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. Navigieren Sie zu **Updates** > **Programm**.
2. Wählen Sie **Zeitgesteuerte Updates aktivieren**, und legen Sie dann den Zeitplan fest.



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.

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 den Trend Micro 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. Navigieren 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.

OBJEKTNAME	OBJEKTBEZEICHNER (OID)	BESCHREIBUNG
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.
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 der aktuellen Websperrliste zurück.
Trend-MIB:: WCSLastSuccessfulUpdate	1.3.6.1.4.1.6101.1.2.1.6	Gibt Datum und Uhrzeit des letzten erfolgreichen Updates der Websperrliste zurück.
Trend-MIB:: WCSLastUpdateError	1.3.6.1.4.1.6101.1.2.1.7	Gibt den Status des letzten Updates der Websperrliste zurück. • 0: Letztes Pattern-Update war erfolgreich. • <Fehlercode>: Letztes Pattern-Update war nicht erfolgreich.

OBJEKTNAME	OBJEKTBEZEICHNER (OID)	BESCHREIBUNG
Trend-MIB:: WCSLastUpdateErrorMessage	1.3.6.1.4.1.6101.1.2.1.8	Gibt eine Fehlermeldung zurück, wenn das letzte Update der Websperrliste 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.
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. Navigieren 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.

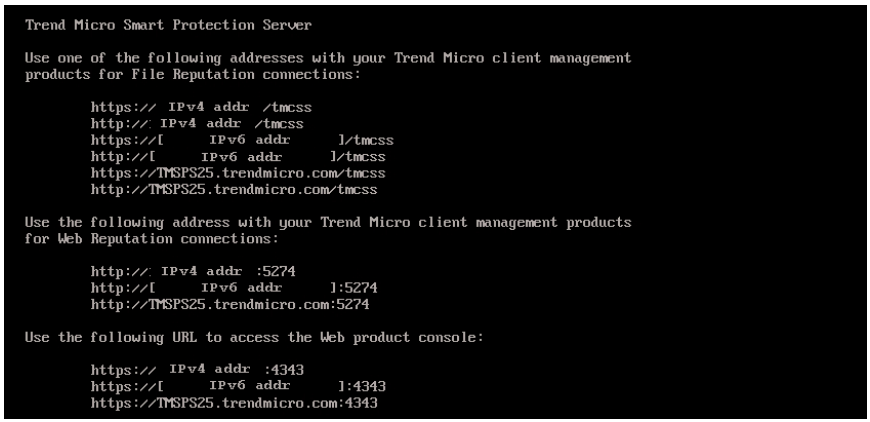
Tipp

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.

Kapitel 3

Smart Protection Server™ überwachen

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

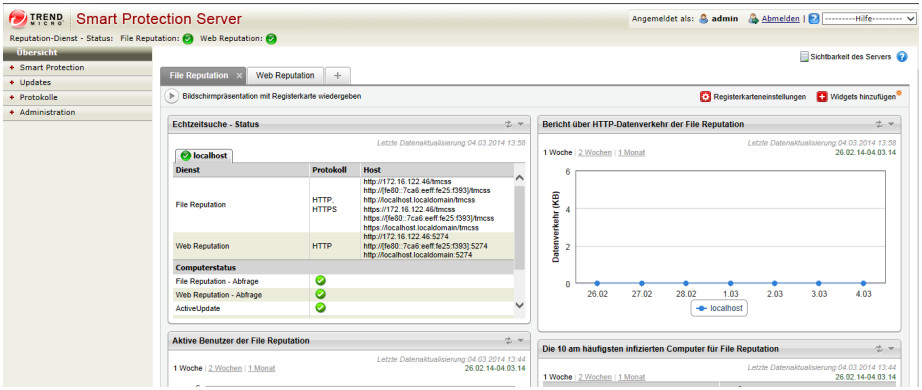
Es werden folgende Themen behandelt:

- *Fenster "Zusammenfassung" verwenden auf Seite 3-2*
- *Protokolle auf Seite 3-15*
- *Benachrichtigungen auf Seite 3-19*

Fenster "Zusammenfassung" verwenden

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

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



Das Fenster **Übersicht** besteht aus den folgenden Benutzeroberflächenelementen:

- **Sichtbarkeit des Servers**: Klicken Sie hierauf, um Server zur Liste "Sichtbarkeit des Servers" hinzuzufügen oder Proxy-Server-Einstellungen für Server zu konfigurieren, die sich auf 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 Servern zu konfigurieren.

- Registerkarten stellen einen Container für Widgets zur Verfügung. Weitere Informationen finden Sie unter *Registerkarten auf Seite 3-3*.
- Widgets sind die Hauptkomponenten des Dashboards. Weitere Informationen finden Sie unter *Widgets auf Seite 3-6*.

Registerkarten

Registerkarten stellen einen Container für Widgets zur Verfügung. Jede Registerkarte im Fenster **Übersicht** kann bis zu 20 Widgets aufweisen. Das Fenster **Übersicht** selbst unterstützt bis zu 30 Registerkarten.

Aufgaben zu Registerkarten

In der folgenden Tabelle werden alle Aufgaben im Zusammenhang mit Registerkarten aufgeführt:

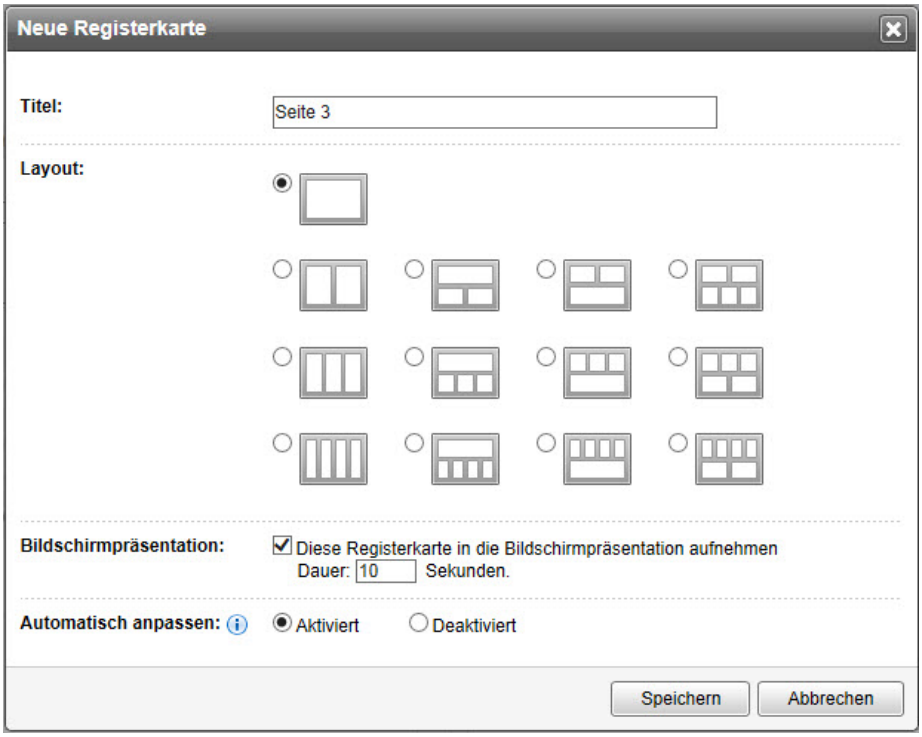
AUFGABE	SCHRITTE
Registerkarte hinzufügen	Klicken Sie auf das Pluszeichen (+) oben im Fenster **Übersicht**. Das Fenster **Neue Registerkarte** wird angezeigt. Weitere Informationen zu diesem Fenster finden Sie unter *Fenster "Neue Registerkarte" auf Seite 3-4*.
Einstellungen von Registerkarten bearbeiten	Klicken Sie auf **Registerkarteneinstellungen**. Ein Fenster, das dem Fenster **Neue Registerkarte** ähnelt, wird geöffnet, in dem Sie Einstellungen bearbeiten können.
Bildschirmpräsentation mit Registerkarte wiedergeben	Klicken Sie auf **Bildschirmpräsentation mit Registerkarte wiedergeben**. Die Informationen auf den ausgewählten Registerkarten ändern sich ähnlich wie dies bei einer Bildschirmpräsentation der Fall ist.

AUFGABE	SCHRITTE
Registerkarte verschieben	Verwenden Sie die Drag & Drop-Funktion, um die Position einer Registerkarte zu verändern.
Registerkarte löschen	Klicken Sie auf das Symbol "Löschen" ( ) neben dem Registerkartentitel. Wird eine Registerkarte gelöscht, werden auch alle Widgets auf der Registerkarte gelöscht.

Fenster "Neue Registerkarte"

Das Fenster **Neue Registerkarte** wird geöffnet, wenn Sie im Fenster **Übersicht** eine neue Registerkarte hinzufügen.

Dieses Fenster enthält die folgenden Optionen:



Optionen	Schritte
Titel	Geben Sie den Namen der Registerkarte ein.
Layout	Wählen Sie aus den verfügbaren Layouttypen aus.
Bildschirmpräsentation	Die Informationen auf den ausgewählten Registerkarten ändern sich ähnlich wie dies bei einer Bildschirmpräsentation der Fall ist. Wenn Sie diese Option aktivieren, können Sie die gewünschten Registerkarten für die Bildschirmpräsentation auswählen sowie die Wiedergabegeschwindigkeit der Bildschirmpräsentation steuern.

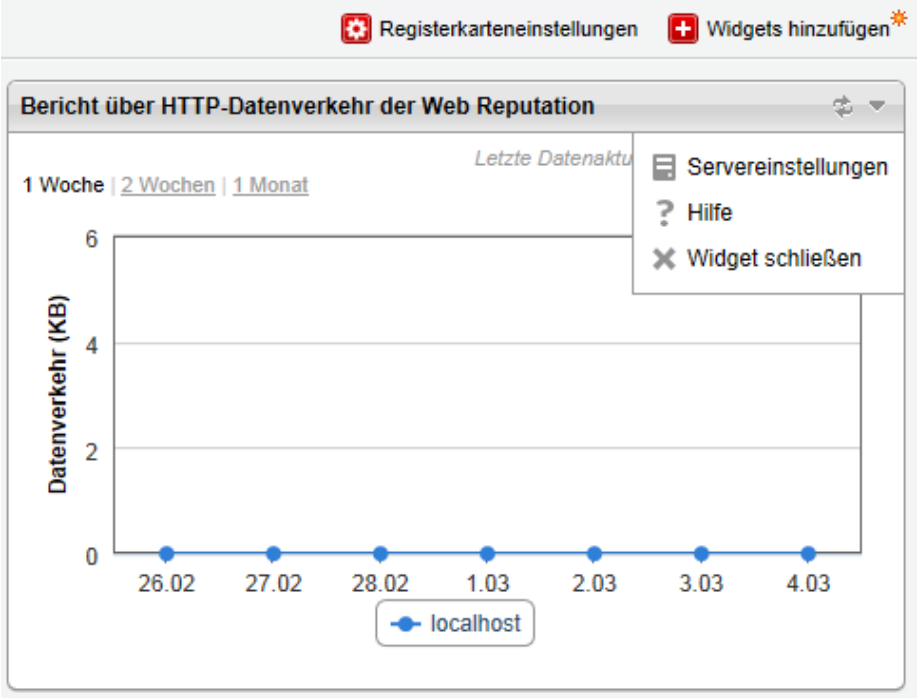
OPTIONEN	SCHRITTE
Automatisch anpassen	Beim automatischen Anpassen wird ein Widget an die Größe eines Kästchens angepasst.

Widgets

Widgets ermöglichen Ihnen, die im Fenster **Übersicht** angezeigten Informationen anzupassen. Neue Widgets können zur Webkonsole hinzugefügt werden. Die Widgets können an eine andere Position gezogen werden, um die Anzeigereihenfolge anzupassen. Verfügbare Widget-Pakete können über das Fenster "Programm-Update" heruntergeladen und aktualisiert werden. Nach dem Aktualisieren des Widget-Pakets kann das neue Widget vom Fenster **Übersicht** aus hinzugefügt werden.

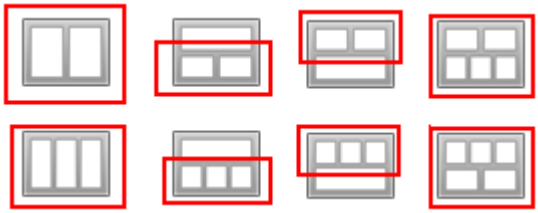
Aufgaben zu Widgets

In der folgenden Tabelle werden Aufgaben im Zusammenhang mit Widgets aufgeführt:



Aufgabe	Schritte
Widget hinzufügen	Öffnen Sie eine Registerkarte, und klicken Sie dann auf **Widgets hinzufügen** in der oberen rechten Ecke der Registerkarte. Das Fenster **Widgets hinzufügen** wird angezeigt.
Widgetdaten aktualisieren	Klicken Sie auf das Symbol "Aktualisieren" ( ).

AUFGABE	SCHRITTE
Servereinstellungen konfigurieren	Klicken Sie auf das Dreieckssymbol ( ), und klicken Sie dann auf **Servereinstellungen** ( ), um das Abrufen von Informationen vom Server für das Widget zu aktivieren bzw. zu deaktivieren. Sie können auch auf **Sichtbarkeit des Servers prüfen** klicken, um Server zur Liste "Sichtbarkeit des Servers" hinzuzufügen oder Proxy-Server-Einstellungen zum Einrichten einer Verbindung mit Servern zu konfigurieren, die sich in der Liste "Sichtbarkeit des Servers" befinden.
Hilfe anzeigen	Klicken Sie auf das Dreieckssymbol ( ), und klicken Sie dann auf **Hilfe** ( ).
Ein Widget löschen	Klicken Sie auf das Dreieckssymbol ( ), und klicken Sie dann auf **Widget schließen** ( ). Hiermit wird das Widget aus der Registerkarte entfernt, auf der es vorhanden ist, jedoch nicht aus den anderen Registerkarten oder aus der Widget-Liste im Fenster **Widgets hinzufügen**.
Verschieben eines Widgets	Verwenden Sie die Drag- & Drop-Funktion, um ein Widget an einen anderen Ort innerhalb der Registerkarte zu verschieben.

AUFGABE	SCHRITTE
Die Größe eines Widgets anpassen	Um die Größe eines Widgets zu ändern, zeigen Sie mit dem Cursor auf den rechten Rand des Widgets. Wenn eine dicke vertikale Linie mit einem Pfeil angezeigt wird (siehe Abbildung unten), halten Sie den Cursor gedrückt und ziehen ihn nach links oder rechts.  Die Größenänderung ist nur für Widgets in mehrspaltigen Registerkarten möglich. Diese Registerkarten weisen eines der folgenden Layouts auf, und die farblich hervorgehobenen Abschnitte enthalten Widgets, deren Größe geändert werden kann. 

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 unterstützt die Protokolle HTTP und HTTPS. Web Reputation unterstützt HTTP. HTTPS stellt eine sicherere Verbindung zur Verfügung, während HTTP weniger Bandbreite verwendet.
Host	Adressen des File-Reputation-Dienstes und des Web-Reputation-Dienstes. Diese Adressen werden bei solchen Trend Micro-Produkten verwendet, die Smart Protection Server unterstützen. Mit Hilfe der Adressen werden Verbindungen zu Smart Protection Servern konfiguriert.

DATEN	BESCHREIBUNG
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 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. Dieses Widget zeigt Informationen in einer 3D-Grafik an und wird stündlich aktualisiert. Sie können auch jederzeit auf das Symbol "Aktualisieren" ( ) klicken, um die Daten zu aktualisieren.

Hinweis

Mit einem Rechtsklick auf die 3D-Grafik erhalten Sie Optionen, um die Grafik zurückzusetzen oder in 2D, in 3D, in 100-%-Größe oder angepasst an die Fenstergröße anzuzeigen. Sie können auch auf den Servernamen klicken, um die Werte für die einzelnen Tage in der Grafik anzuzeigen.

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 gesperrten 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 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 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. Dieses Widget zeigt Informationen in einer 3D-Grafik an und wird stündlich aktualisiert. Sie können auch jederzeit auf das Symbol "Aktualisieren" ( ) klicken, um die Daten zu aktualisieren.

Hinweis

Mit einem Rechtsklick auf die 3D-Grafik erhalten Sie Optionen, um die Grafik zurückzusetzen oder in 2D, in 3D, in 100-%-Größe oder angepasst an die Fenstergröße anzuzeigen. Sie können auch auf den Servernamen klicken, um die Werte für die einzelnen Tage in der Grafik anzuzeigen.

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 meistgesperrten Computer der ausgewählten Smart Protection Server in der Liste an.

TABELLE 3-7. Widget-Informationen

DATEN	BESCHREIBUNG
IP	Die IP-Adresse des Computers.
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.

Protokoll 'Gesperrter Internet-Zugriff'

Im Fenster "Protokoll 'Gesperrter Internet-Zugriff'" werden Informationen über Abfragen der Web Reputation angezeigt, mit denen bösartige Ergebnisse zurückgegeben werden. Diese Optionen stehen auf dem Bildschirm zur Verfügung.

- **Schlüsselwort**: Geben Sie Schlüsselwörter an, die zum Suchen von URLs verwendet werden.

- **Datumsbereich**: Wählen Sie einen Datumsbereich.
- **Protokoll anzeigen**: Gehen Sie wie folgt vor, um Ihre Protokollabfrage zu filtern:
  - **Alle**: Zeigt Protokolle aller gesperrten Sites an.
  - **Gesperrt**: Zeigt Protokolle von Sites an, die gesperrt wurden, weil die Sites mit einem Eintrag in der benutzerdefinierten Liste der gesperrten URLs übereinstimmten.
  - **Virtual Analyzer C&C**: Zeigt Protokolle von Sites an, die gesperrt wurden, weil die Sites mit einer URL oder IP-Adresse in der Virtual Analyzer C&C-Liste übereinstimmten.
  - **Websperrliste**: Zeigt Protokolle von Sites an, die gesperrt wurden, weil die Sites mit einer URL oder IP-Adresse in der Websperrliste oder der Global Intelligence C&C-Liste übereinstimmten.
- **C&C-Listenquelle**: Zeigt Protokolle von Sites an, die gesperrt wurden, weil sie in der Global Intelligence-Liste oder Virtual Analyzer-Liste vorhanden sind.

Protokolldetails:

- **Datum und Zeit**: Zeitpunkt, an dem ein URL gesperrt wurde.
- **URL**: Der URL wurde von der Web Reputation gesperrt.
- **Filter**: Die Liste, die die Sperrung der URL oder IP-Adresse ausgelöst hat. Dabei kann es sich um eine benutzerdefinierte Liste gesperrter URLs, die Virtual Analyzer C&C-Liste oder die Trend Micro Websperrliste handeln.
- **C&C-Listenquelle**: Dabei kann es sich um die Global Intelligence-Liste oder die Virtual Analyzer-Liste handeln.
- **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 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.
- **Benutzer**: Der Benutzername des Endpunkts.
- **Domäne**: Der Domänenname des Endpunkts.
- **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.
- **Protokoll "Gesperrter Internet-Zugriff"**: 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.

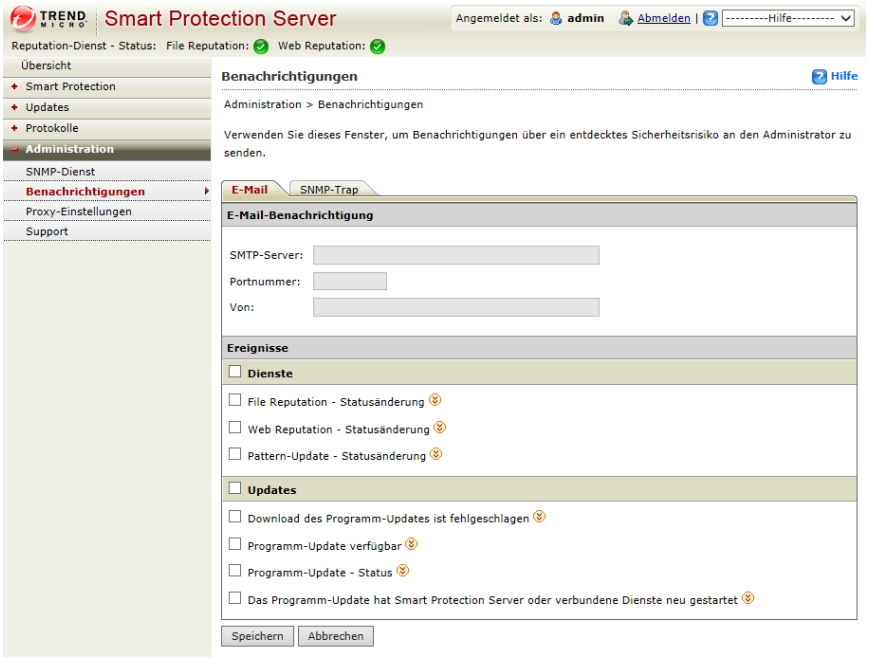
- **Nachricht**: Geben Sie eine neue Nachricht ein, oder verwenden Sie einen Standardtext für dieses Ereignis.
- **File Reputation - Statusänderung**: Wählen Sie diese Option, um eine Benachrichtigung bei einer Statusänderung zu senden, und geben Sie den Empfänger für diese Benachrichtigung an.
- **Web 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 klicken Sie dann auf die Registerkarte **E-Mail**.

   Die Registerkarte für E-Mail-Benachrichtigungen wird angezeigt.



2. Aktivieren Sie das Kontrollkästchen **Dienst**, um eine E-Mail-Benachrichtigung bei Statusänderungen für alle Dienste zu erhalten, oder wählen Sie die gewünschten Dienste unter 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 klicken Sie dann auf die 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

Hilfe anfordern

In diesem Kapitel finden Sie Informationen, wie Sie beim Arbeiten mit Trend Micro™ Smart Protection Server™ zusätzliche Hilfe erhalten.

Es werden folgende Themen behandelt:

- *Support-Portal verwenden auf Seite 4-2*
- *Bedrohungsenzyklopädie auf Seite 4-3*
- *Kontaktaufnahme mit Trend Micro auf Seite 4-4*
- *TrendLabs auf Seite 4-5*

Support-Portal verwenden

Das Trend Micro Support-Portal ist täglich rund um die Uhr online verfügbar und enthält die aktuellsten Informationen zu häufig auftretenden und ungewöhnlichen Problemen.

Prozedur

1. Navigieren Sie zu http://esupport.trendmicro.com.
2. Wählen Sie in der entsprechenden Dropdown-Liste ein Produkt oder einen Dienst aus, und geben Sie sonstige entsprechende Informationen an.

   Die Seite **Technischer Support** wird angezeigt.
3. Verwenden Sie das Feld **Search Support** (Support suchen), um nach verfügbaren Lösungen zu suchen.
4. Falls keine Lösung gefunden wird, klicken Sie im linken Navigationsbereich auf **Submit a Support Case** (Support-Anfrage einreichen), und geben Sie die entsprechenden Informationen ein, oder reichen Sie eine Support-Anfrage auf der folgenden Seite ein:

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

   Ein Support-Mitarbeiter von Trend Micro analysiert Ihre Anfrage und antwortet innerhalb von maximal 24 Stunden.

Bekannte Probleme

Unter "Bekannte Probleme" werden unerwartete Eigenschaften des Produkts dokumentiert, für die möglicherweise eine vorübergehende Lösung erforderlich ist. Trend Micro empfiehlt, immer die Readme-Datei zu lesen, die Informationen über Systemvoraussetzungen und bekannte Probleme enthält, die die Installation oder die Leistung beeinflussen könnten. Readme-Dateien enthalten auch eine Beschreibung der neuen Funktionen einer Version sowie weitere, hilfreiche Informationen.

Die neuesten bekannten Probleme und mögliche Workarounds stehen auch in der Trend Micro Knowledge Base zur Verfügung:

http://esupport.trendmicro.com

Hotfixes, Patches und Service Packs

Nach der offiziellen Veröffentlichung eines Produkts erstellt Trend Micro oft Hotfixes, Patches und Service Packs zur Behebung besonderer Probleme, zur Leistungsverbesserung oder zur Funktionserweiterung.

Die folgende Übersicht zeigt, welche Komponenten möglicherweise von Trend Micro veröffentlicht werden:

- **Hot Fix**: Ein Workaround oder eine Lösung zu Problemen, über die Trend Micro von Kunden informiert wurde. Die von Trend Micro erstellten und veröffentlichten Hotfixes erhalten nur bestimmte Kunden.
- **Sicherheits-Patch**: Ein einzelner Hotfix oder eine Gruppe von Hotfixes zur Verteilung an alle Kunden.
- **Patch**: Eine Gruppe von Sicherheits-Patches zur Verteilung an alle Kunden.
- **Service Pack**: Eine erhebliche Funktionserweiterungen, die ein Upgrade des Produkts durchführt.

Ihr Händler bzw. Ihr Support-Anbieter informiert Sie ggf. bei Verfügbarkeit dieser Produkte. Weitere Informationen über neu veröffentlichte Hotfixes, Patches und Service Packs finden Sie auch auf der Trend Micro Website unter:

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

Jede Veröffentlichung enthält eine Readme-Datei mit Informationen über Installation, Verteilung und Konfiguration. Lesen Sie die Readme vor der Installation aufmerksam durch.

Bedrohungsenzyklopädie

Der Großteil der Malware besteht heutzutage aus "kombinierten Bedrohungen", also einer Kombination aus mindestens zwei Technologien zur Umgehung der Sicherheitsprotokolle des Computers. 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://www.trendmicro.com/vinfo/de/virusencyclo/default.asp 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

Trend Micro Mitarbeiter sind per Telefon, Fax oder E-Mail verfügbar:

Adresse	TREND MICRO INCORPORATED Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland
Telefon	+49 (0) 811 88990-700
Fax	+4981188990799
Website	http://www.trendmicro.com
E-Mail-Adresse	sales@trendmicro.de marketing@trendmicro.de

- Weltweite Support-Büros:

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

- Trend Micro Produktdokumentation:

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

Problemlösung beschleunigen

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

- Schritte, um das Problem nachvollziehen zu können
- Informationen zur Appliance und zum Netzwerk
- Marke und Modell des Computers sowie zusätzliche Hardware, die an den Endpunkt angeschlossen ist
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Betriebssystem- und Service Pack-Version
- Client-Version des Endpunkts
- Seriennummer oder Aktivierungscode
- Ausführliche Beschreibung der Installationsumgebung
- Genauer Wortlaut eventueller Fehlermeldungen
- Virtualisierungsplattform (VMware™ oder Hyper-V™) und Version

TrendLabs

Bei TrendLabs℠ handelt es sich um ein globales Netzwerk aus Forschungs-, Entwicklungs- und Wartungszentren, die täglich rund um die Uhr nach Sicherheitsbedrohungen suchen, Angriffe verhindern und schnell und problemlos Lösungen bereitstellen. TrendLabs dient als Backbone der Trend Micro Service-Infrastruktur und beschäftigt mehrere hundert Mitarbeiter und zertifizierte Support-Experten, die sich um die vielfältigen Anfragen zu Produkten und technischem Support kümmern.

TrendLabs überwacht die weltweite Bedrohungslage, um effektive Sicherheitsmaßnahmen anzubieten, mit denen Angriffe erkannt, vermieden und beseitigt werden können. Die Kunden profitieren von diesen täglichen Bemühungen in Form von häufigen Viren-Pattern-Updates und Erweiterungen der Scan Engine.

Weitere Informationen zu TrendLabs finden Sie unter:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

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
configure date	**configure date** <Datum> <Uhrzeit>	Daten konfigurieren und im CMOS speichern *date* DATUMSFELD [DATUMSFELD] *time* ZEITFELD [ZEITFELD]

Befehl	Syntax	Beschreibung
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 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

Befehl	Syntax	Beschreibung
`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
`configure ntp`	`configure ntp <IP oder FQDN>`	NTP-Server konfigurieren
`configure port`	`configure port <frs_http_port> <frs_https_port> <wrs_http_port>`	Dienstports der File-Reputation- und Web-Reputation-Dienste ändern.
`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]

BEFEHL	SYNTAX	BESCHREIBUNG
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]
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]

Befehl	Syntax	Beschreibung
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 service	**configure service interface** <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
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

BEFEHL	SYNTAX	BESCHREIBUNG
`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
`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

Befehl	Syntax	Beschreibung
`configure timezone America St_Johns`	`configure timezone America St_Johns`	Zeitzone für den Standort Amerika/St Johns konfigurieren
`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
`configure timezone Asia Jerusalem`	`configure timezone Asia Jerusalem`	Zeitzone für den Standort Asien/Jerusalem konfigurieren

Befehl	Syntax	Beschreibung
`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
`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

Befehl	Syntax	Beschreibung
`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
`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

Befehl	Syntax	Beschreibung
`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
`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

Befehl	Syntax	Beschreibung
`configure timezone Pacific Guam`	`configure timezone Pacific Guam`	Zeitzone für den Standort Pazifik/Guam konfigurieren
`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
`configure timezone US Pacific`	`configure timezone US Pacific`	Zeitzone für den Standort USA/Pazifik konfigurieren
`disable adhoc-query`	`disable adhoc-query`	Internet-Zugriffsprotokoll deaktivieren

Befehl	Syntax	Beschreibung
disable ssh	**disable ssh**	sshd-Daemon deaktivieren
enable	**enable**	Administrative Befehle aktivieren
enable adhoc-query	**enable adhoc-query**	Internet-Zugriffsprotokoll aktivieren
enable hyperv-ic	**enable hyperv-ic**	Linux-Integrationskomponenten für Hyper-V Linux auf dem Smart Protection Server 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

Befehl	Syntax	Beschreibung
`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
`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

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

Anhang B

Glossar

In diesem Glossar werden Begriffe im Zusammenhang mit Smart Protection Server erläutert.

BEGRIFF	DEFINITION
Aktivieren	Die Software muss nach dem Registrierungsvorgang aktiviert werden. Trend Micro Produkte sind erst nach Durchführung der Produktaktivierung betriebsbereit. Die Aktivierung kann während der Installation oder danach (in der Management-Konsole) über das Fenster "Produktlizenz" aktiviert werden.
ActiveUpdate	Die ActiveUpdate Funktion ist Bestandteil vieler Trend Micro Produkte. Über die Verbindung zur Trend Micro Update-Website stellt ActiveUpdate per Internet oder mit der Trend Micro Total Solution CD aktuelle Downloads von Viren-Pattern-Dateien, Scan Engines und andere Programmdateien bereit.
Adresse	"Adresse" bezeichnet eine Netzwerkadresse (siehe IP-Adresse) oder eine E-Mail-Adresse, d. h. die Zeichenfolge, die den Absender oder den Empfänger einer E-Mail angibt.
Administrator	Bezieht sich auf den Systemadministrator, d. h. die Person in einem Unternehmen, die für folgende Aufgaben zuständig ist: Installation neuer Hardware und Software, Zuweisung von Benutzernamen und Kennwörtern, Überwachung des Festplattenspeichers und anderer IT-Ressourcen, Erstellung von Sicherungsdateien und Verwaltung der Netzwerksicherheit.

BEGRIFF	DEFINITION
Administratorkonto	Benutzername und Kennwort mit Administratorberechtigungen.
Virenschutz	Computerprogramme, die Computerviren erkennen und säubern.
Authentifizierung	Die Identitätsüberprüfung einer Person oder eines Prozesses. Die Authentifizierung stellt sicher, dass digitale Datenübertragungen an den beabsichtigten Empfänger gesendet werden. Außerdem bestätigt die Authentifizierung dem Empfänger die Integrität der Nachricht und die Quelle (von wo und von wem die Nachricht stammt). Für die einfachste Form der Authentifizierung wird ein Benutzername und ein Kennwort benötigt, um auf ein bestimmtes Konto zugreifen zu können. Authentifizierungsprotokolle können auch auf der Verschlüsselung mit einem geheimen Schlüssel basieren, wie beispielsweise dem DES-Algorithmus (Data Encryption Standard), oder auf Systemen mit öffentlichem Schlüssel unter Verwendung von digitalen Signaturen. Siehe auch "Verschlüsselung mit öffentlichem Schlüssel" und "Digitale Signatur".
Client	Ein Computer oder ein Prozess, der über ein Protokoll den Dienst eines anderen Computers oder Prozesses (eines Servers) anfordert und die Antworten dieses Servers akzeptiert. Ein Client ist Teil einer Client/Server-Software-Architektur.
Konfiguration	Die Auswahl von Optionen für die Funktionen Ihres Trend Micro Produkts. Sie können z.B. auswählen, ob eine mit einem Virus infizierte Datei in Quarantäne verschoben oder gelöscht werden soll.
Standardeinstellung	Ein Wert, der in einem Feld der Management-Konsole voreingestellt ist. Ein Standardwert wird nach logischen Aspekten und aus Gründen der Bequemlichkeit ausgewählt und eingestellt. Verwenden Sie die Standardwerte, oder ändern Sie diese.
(Administrative) Domäne	Eine Gruppe von Computern mit einer gemeinsamen Datenbank und Sicherheitsrichtlinie.
Domänenname	Der vollständige Name eines Systems, der aus dem Namen seines lokalen Hosts und dessen Domänenamen, z.B. sagtdiralles.de, besteht. Mit einem Domänennamen sollte für jeden Host im Internet eine eindeutige Internet-Adresse bestimmt werden können. Bei dieser so genannten "Namensauflösung" wird das Domain Name System (DNS) verwendet.

Begriff	Definition
Download	Daten, die z. B. per HTTP von einer Website heruntergeladen wurden.
Herunterladen	Die Daten von einem Computer zu einem anderen übertragen. Der Begriff bezeichnet häufig die Datenübertragung von einem größeren Host-System (insbesondere von einem Server oder Mainframe) zu einem kleineren Client-System.
FAQ	Häufig gestellte Fragen: Eine Liste mit Antworten zu häufig gestellten Fragen zu einem bestimmten Thema.
Datei	Ein Datenelement für Speicherzwecke, wie beispielsweise eine E-Mail oder ein HTTP-Download.
Dateityp	Die Art der in einer Datei gespeicherten Daten. Die meisten Betriebssysteme bestimmen den Dateityp über die Dateierweiterung. Der Dateityp entscheidet über die Auswahl eines entsprechenden Symbols, das in der Benutzeroberfläche für die Datei steht, und die passende Anwendung, mit der die Datei angezeigt, bearbeitet, ausgeführt oder gedruckt wird.
Spyware/ Grayware	Eine Kategorie für Software, die unberechtigt, unerwünscht oder bösartig ist. Im Gegensatz zu Bedrohungen wie Viren, Würmern oder Trojanern werden Daten durch Grayware weder infiziert noch repliziert oder vernichtet, aber sie kann Ihre Datenschutzinteressen verletzen. Beispiele für Grayware sind Spyware, Adware und Tools für den Remote-Zugriff.
Gateway	Ein Gateway ist ein Programm oder ein Spezialgerät, das IP-Datagramme von einem Netzwerk zu einem anderen überträgt, bis das Ziel erreicht wird.
GUI	Grafische Benutzeroberfläche: Die Verwendung von grafischen Elementen statt nur von Wörtern für die Ein- und Ausgabe eines Programms und dessen Bedienung. Dadurch unterscheidet sie sich von einer Befehlszeilenschnittstelle, bei der die Kommunikation über den Austausch von Textzeichenfolgen erfolgt.
Festplattenlaufwerk (oder Festplatte)	Eine oder mehrere magnetische Scheiben, die um eine zentrale Achse rotieren und über Schreib-/Leseköpfe und Elektronik verfügen. Sie werden zum Lesen, Schreiben und Speichern von Daten verwendet. Die meisten Festplatten sind permanent mit dem Laufwerk verbunden, aber es sind auch Wechselmedien erhältlich.

BEGRIFF	DEFINITION
HTTP	Hypertext Transfer Protocol: Das Client-Server-TCP/IP-Protokoll, das im World Wide Web für den Austausch von HTML-Dokumenten verwendet wird. Normalerweise verwendet es Port 80.
HTTPS	Hypertext Transfer Protocol Secure: Eine Variante von HTTP, die für sichere Transaktionen verwendet wird.
Host	Ein mit einem Netzwerk verbundener Computer.
Internet	Ein Client-Server-orientiertes Hypertext-System zum Abruf von Informationen, bestehend aus vielen Netzwerken, die via Router miteinander verbunden sind. Das Internet ist ein modernes Informationssystem und weithin anerkanntes Medium für Werbung, Online-Handel und -Dienste sowie Universitäts- und Forschungsnetzwerke. Das World Wide Web ist der bekannteste Aspekt des Internets.
Internet Protocol (IP)	Ein Internet-Standardprotokoll, das eine Basiseinheit von Daten definiert, die als Datagramm bezeichnet wird. Ein Datagramm wird in einem verbindungslosen Best-Effort-Verteilungssystem eingesetzt. Das Internet Protocol definiert, wie Informationen über das Internet zwischen Systemen übergeben werden.
Intranet	Ein Netzwerk, das innerhalb eines Unternehmens ähnliche Dienste bereitstellt wie außerhalb das Internet, das aber nicht unbedingt mit dem Internet verbunden ist.
IP	Internetprotokoll – siehe "IPv4-Adresse" oder "IPv6-Adresse".
IPv4-Adresse	Internet-Adressen für Netzwerkgeräte, die in der Regel durch Punktschreibweise dargestellt werden, wie z. B. `123.123.123.123`.
IPv6-Adresse	Internet-Adressen für Netzwerkgeräte, in der Regel im Format `1234:1234:1234:1234:1234:1234:1234:1234`.
IT	Informationstechnologie: Hardware, Software, Netzwerk, Telekommunikation und Benutzer-Support.

BEGRIFF	DEFINITION
Java-Datei	Java ist eine universelle Programmiersprache, die von Sun Microsystems entwickelt wurde. Eine Java-Datei enthält Java-Code. Java unterstützt die Programmierung für das Internet in Form von plattformunabhängigen Java-Applets. (Bei einem Applet handelt es sich um ein in der Programmiersprache Java entwickeltes Programm, das auf einer HTML-Seite enthalten sein kann. Wenn Sie mit einem Java-fähigen Browser eine Seite anzeigen, die ein Applet enthält, wird der Code des Applets auf Ihr System übertragen und von der Java Virtual Machine des Browsers ausgeführt.)
Bösartiger Java-Code	Virencode, der in Java geschrieben oder eingebettet wurde. Siehe auch "Java-Datei".
JavaScript-Virus	JavaScript ist eine einfache, von Netscape entwickelte Programmiersprache, die Webentwicklern ermöglicht, mit Hilfe von Skripts dynamische Inhalte in HTML-Seiten einzubinden. Einige Funktionen von JavaScript sind identisch mit der Programmiersprache Java von Sun Microsystems, sie wurde jedoch unabhängig davon entwickelt. Ein JavaScript-Virus ist ein Virus, der auf diese Skripts im HTML-Code abzielt. Dadurch kann sich der Virus in Webseiten befinden und über den Browser des Benutzers auf einen Benutzer-Desktop heruntergeladen werden. Siehe auch "VBScript-Virus".
KB	Kilobyte: 1024 Byte Speicher.
Lizenz	Die gesetzliche Autorisierung, ein Produkt von Trend Micro verwenden zu dürfen.
Link (auch: Hyperlink)	Ein Verweis von einer Stelle in einem Hypertext-Dokument auf eine Stelle in einem anderen bzw. demselben Dokument. Links werden in der Regel vom übrigen Text durch eine andere Farbe oder einen anderen Stil abgesetzt, wie beispielsweise unterstrichener blauer Text. Wenn Sie den Link aktivieren, indem Sie beispielsweise darauf klicken, wird im Browser das Ziel des Links angezeigt.

BEGRIFF	DEFINITION
Lokales Netzwerk (LAN)	Eine Netzwerktechnologie, die Ressourcen innerhalb einer Büroumgebung mit einer hohen Geschwindigkeit, z. B. Ethernet, miteinander vernetzt. Ein lokales Netzwerk ist ein auf kürzere Distanzen begrenztes Netzwerk, das mehrere Computer innerhalb eines Gebäudes miteinander verbindet. 10BaseT Ethernet ist die am häufigsten verwendet Form eines LANs. Ein Hardware-Gerät, ein so genannter Hub, fungiert als allgemeiner Knotenpunkt, über den Daten von einem Computer zu einem anderen Computer im Netzwerk gesendet werden können. LANs sind in der Regel auf Entfernungen von unter 500 m begrenzt und bieten kostengünstige Netzwerkfunktionen mit hoher Bandbreite innerhalb eines kleinen geografischen Bereichs.
Malware (bösartige Software)	Programme oder Dateien, die mit dem Ziel entwickelt wurden, Schäden anzurichten, wie beispielsweise Viren, Würmer und Trojaner.
Management-Konsole	Die Benutzeroberfläche Ihres Trend Micro Produkts. Wird auch als Produktkonsole bezeichnet.
Mb/s	Millionen Bit pro Sekunde: Eine Maßeinheit für die Bandbreite bei der Datenkommunikation.
MB	Megabyte: 1024 Kilobyte Daten.
Kombinierte Bedrohungen	Komplexe Angriffe, die von mehreren Eintrittsstellen und Schwachstellen in den Unternehmensnetzwerken profitieren. Beispiele hierfür sind die Bedrohungen "Nimda" oder "Code Red".
Netzwerkadressübersetzung (Network Address Translation, NAT)	Ein Standard zur Übersetzung von sicheren IP-Adressen in temporäre, externe, registrierte IP-Adressen aus dem Adresspool. Auf diese Weise können vertrauenswürdige Netzwerke mit privat zugeordneten IP-Adressen auf das Internet zugreifen. Das bedeutet auch, dass Sie nicht für jeden Computer in Ihrem Netzwerk eine registrierte IP-Adresse benötigen.

Begriff	Definition
Netzwerkvirus	Netzwerkviren verbreiten sich grundsätzlich über Netzwerkprotokolle wie TCP, FTP, UDP, HTTP und E-Mail-Protokolle. Systemdateien und die Bootsektoren von Festplatten werden meist nicht verändert. Stattdessen infizieren Netzwerkviren den Arbeitsspeicher der Client-Computer und verursachen eine Überflutung des Netzwerks mit Daten. Dies führt zu einer Verlangsamung oder – schlimmer noch – dem vollständigen Ausfall des Netzes.
Benachrichtigung (siehe auch "Aktion" und "Ziel")	Eine Nachricht, die an eine oder mehrere der folgenden Personen weitergeleitet wird: Systemadministrator, Absender einer Nachricht, Empfänger einer Nachricht oder einer heruntergeladenen oder übertragenen Datei. Die Benachrichtigung informiert darüber, dass eine verbotene Aktion ausgeführt oder versucht wurde, wie beispielsweise ein Virus, der beim versuchten Download in einer HTTP-Datei entdeckt wird.
Betriebssystem	Die Software, die Aufgaben wie die Steuerung von Peripheriegeräten, die Aufgabenplanung und die Speicherzuordnung übernimmt. In dieser Dokumentation bezeichnet der Begriff auch die Software, die ein Windows-System und eine grafische Benutzeroberfläche darstellt.
Parameter	Eine Variable, z. B. ein Wertebereich (eine Zahl zwischen 1 und 10).
Pattern-Datei (auch: offizielles Pattern-Release)	Die Pattern-Datei, die auch als offizielles Pattern-Release (OPR) bezeichnet wird, ist die neueste Pattern-Sammlung für identifizierte Viren. Sie wird mehrfach getestet, um sicherzustellen, dass Sie optimal vor den neuesten Virenbedrohungen geschützt sind. Diese Pattern-Datei ist am wirksamsten, wenn sie in Verbindung mit der neuesten Scan Engine genutzt wird.
Port	Ein logischer Kanal oder Kanal-Endpunkt in einem Kommunikationssystem, der zur Unterscheidung zwischen verschiedenen logischen Kanälen auf derselben Netzwerkschnittstelle oder auf demselben Computer verwendet wird. Jedem Anwendungsprogramm ist eine eigene eindeutige Portnummer zugewiesen.
Proxy	Ein Prozess, der einen Cache-Speicher mit Elementen bereitstellt, die auf anderen Servern gespeichert sind, die voraussichtlich langsamer sind oder bei denen durch den Zugriff Kosten entstehen.

BEGRIFF	DEFINITION
Proxy-Server	Ein WWW-Server, der URLs mit einem speziellen Präfix akzeptiert, mit dem Dokumente entweder von einem lokalen Zwischenspeicher oder einem Remote-Server abgerufen werden, und der dann den URL an die anfordernde Instanz zurücksendet.
Suche	Schrittweise Überprüfung von Elementen in einer Datei, um Elemente zu finden, die bestimmte Kriterien erfüllen.
Scan Engine	Dieses Modul sucht und findet Viren in dem Host-Produkt, in das es integriert ist.
Sektor	Eine physische Einheit auf einer Festplatte. (Siehe auch "Partition", wobei es sich um eine logische Einheit auf der Festplatte handelt.)
Secure Socket Layer (SSL)	Secure Socket Layer (SSL) ist ein von Netscape entwickeltes Protokoll für die Datensicherheit, das im Schichtenmodell zwischen Anwendungsprotokollen (z. B. HTTP, Telnet oder FTP) und TCP/IP liegt. Dieses Sicherheitsprotokoll bietet Datenverschlüsselung, Server-Authentifizierung, Nachrichtenintegrität und optionale Client-Authentifizierung für eine TCP/IP-Verbindung.
Server	Ein Programm, das Dienste für andere (Client-) Programme bereitstellt. Die Verbindung zwischen Client und Server erfolgt in der Regel mittels Übertragung von Nachrichten und über ein Netzwerk. Dabei werden anhand eines Protokolls die Anfragen der Clients und die Antworten des Servers kodiert. Der Server kann permanent ausgeführt werden (als Daemon) und darauf warten, dass Anforderungen eingehen, oder er kann durch einen Daemon einer höheren Ebene aufgerufen werden, der mehrere bestimmte Server steuert.
Freigabelaufwerk	Das Peripheriegerät eines Computers, das von mehreren Personen genutzt wird und auf diese Weise einer erhöhten Virengefährdung ausgesetzt ist.
Signatur	Siehe "Virensignatur".
SNMP	Simple Network Management Protocol: Ein Protokoll, das die Überwachung von mit einem Netzwerk verbundenen Geräten im Hinblick auf Zustände unterstützt, die die Aufmerksamkeit eines Administrators erfordern.

BEGRIFF	DEFINITION
Verkehr	Die ein- und ausgehenden Daten zwischen dem Internet und Ihrem Netzwerk.
Transmission Control Protocol/ Internet Protocol (TCP/IP)	Ein Verbindungsprotokoll, das Computern mit unterschiedlichen Betriebssystemen ermöglicht, Daten auszutauschen. Es steuert, wie die Daten zwischen Computern im Internet übertragen werden.
Auslöser	Ein Ereignis, das eine Aktion auslöst. Beispiel: Das Trend Micro Produkt erkennt einen Virus in einer E-Mail. Dies kann der Auslöser dafür sein, dass die Nachricht in Quarantäne gestellt und eine Benachrichtigung an den Systemadministrator, den Absender oder den Empfänger der Nachricht gesendet wird.
True-File-Type	Wird von der Virenprüfungstechnologie IntelliScan zur Identifizierung der Art der Daten in einer Datei genutzt, indem sie unabhängig von der Dateinamenerweiterung (die möglicherweise irreführend ist) die Datei-Header überprüft.
URL	Universal Resource Locator: Die übliche Methode zur Angabe des Orts eines Objekts, in der Regel einer Webseite, im Internet, wie beispielsweise www.trendmicro.com. Die URL wird per DNS einer IP-Adresse zugeordnet.
Virtuelle IP-Adresse (VIP-Adresse)	Eine VIP-Adresse ordnet den bei einer IP-Adresse eingehenden Datenverkehr basierend auf der Ziel-Portnummer im Paket-Header einer anderen Adresse zu.
VLAN (Virtual Local Area Network)	Ein logischer (kein physischer) Verbund von Geräten, die eine Single-Broadcast-Domäne bilden. VLAN-Mitglieder werden nicht durch ihren Standort in einem physischen Subnetzwerk, sondern anhand von Tags in den Frame Headern der übertragenen Daten identifiziert. VLANs werden im Standard IEEE 802.1Q beschrieben.

BEGRIFF	DEFINITION
Virtual Private Network (VPN)	Ein VPN ist eine einfache, kostengünstige und sichere Möglichkeit für Unternehmen, Telearbeitern und mobile Facharbeitern per lokaler Einwahl Zugriff auf das Unternehmensnetzwerk oder andere Internetdienstanbieter (ISP) zu bieten. Sichere private Internetverbindungen sind kostengünstiger als private Leitungen. VPNs wird durch Technologien und Standards wie Tunneling und Verschlüsselung ermöglicht.
Virtueller Router	Ein virtueller Router ist die Komponente von ScreenOS, die für das Routing zuständig ist.
Virtuelles System	Ein virtuelles System ist ein Teilbereich des Hauptsystems, das der Benutzer wie eine eigenständige Einheit nutzen kann. Virtuelle Systeme befinden sich separat voneinander in derselben Trend Micro GateLock Remote-Anwendung. Jedes von ihnen kann durch einen eigenen Systemadministrator verwaltet werden.
Virus	Bei einem Computervirus handelt es sich um ein Programm (ein ausführbarer Code), das in der Lage ist, Komponenten zu infizieren. So wie biologische Viren können sich auch Computerviren schnell verbreiten und lassen sich häufig nur schwer ausmerzen. Neben der Vervielfältigung weisen einige Computerviren noch eine weitere Gemeinsamkeit auf: Sie enthalten eine Schadensroutine, welche die Nutzlast (Payload) des Virus trägt. Abgesehen von den eher harmlosen Schadensroutinen, mit denen Nachrichten oder Bilder angezeigt werden, gibt es auch destruktivere Formen, die Dateien löschen, die Festplatte formatieren oder sonstigen Schaden anrichten können. Selbst wenn der Virus keine Schadensroutine enthält, kann er doch unangenehme Folgen haben: Beispielsweise kann er den Speicher auslasten und die allgemeine Leistung Ihres Computers erheblich beeinträchtigen.
Web	Das World Wide Web oder Internet.
Web server	Ein Serverprozess, der Websites hostet und Webseiten auf Anforderung via HTTP von Remote-Browsern versendet.
Arbeitsstation (auch: Client)	Ein universeller Computer, der jeweils von einer Person verwendet werden kann und eine höhere Leistung bietet als ein normaler PC, insbesondere hinsichtlich der Grafik, der Prozessorleistung und der Fähigkeit, mehrere Aufgaben gleichzeitig auszuführen.

Stichwortverzeichnis

D

Dokumentationskonventionen, vii

F

Fenster "Zusammenfassung"

- Registerkarten, 3-3
- Widgets, 3-6

P

Pattern der intelligenten Suche, 1-4

R

Registerkarten, 3-3

S

Smart Protection Network, 1-3

Smart Protection Server, 1-3

Smart Scan Agent-Pattern, 1-4

Support

- knowledge base, 4-2
- Probleme schneller beheben, 4-5
- TrendLabs, 4-5

T

TrendLabs, 4-5

Trend Micro

- Info über, vi

W

Websperrliste, 1-4

Widgets, 3-6

TREND MICRO INCORPORATED

Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland

Tel.: +49 (0) 811 88990-700 Fax: +4981188990799

sales@trendmicro.de marketing@trendmicro.de

www.trendmicro.com

Item Code: APEM36294/140116