TREND MICRO™

3.3 TREND MICRO™ Smart Protection Server

Patch 2

Administrator's Guide

Security Made Smarter

Endpoint Security

Messaging Security

Protected Cloud

Web Security

Document Part No.: APEM38673/190603

Release Date: July 2019

Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

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

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Smart Protection Server collects and provides detailed instructions on how to disable the specific features that feedback the information.

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

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Table of Contents

Preface

Chapter 1: Introduction

Chapter 2: Using Smart Protection Server

Chapter 3: Monitoring Smart Protection Server

Chapter 4: Trend Micro Apex Central / Control Manager Integration

Chapter 5: Technical Support

Appendix A: Command Line Interface (CLI) Commands

Index

Preface

Preface

Welcome to the Smart Protection Server™ Administrator's Guide. This document contains information about product settings.

Topics include:

About Trend Micro™

Trend Micro provides virus protection, antispam, and content-filtering security software and services. Trend Micro helps customers worldwide stop malicious code from harming their computers.

Product Documentation

The Smart Protection Server documentation consists of the following:

DOCUMENTATION	DESCRIPTION
Installation and Upgrade Guide	Helps you plan for installation, upgrades, and deployment.
Administrator's Guide	Helps you configure all product settings.
Online Help	Provides detailed instructions on each field and how to configure all features through the user interface.
Readme file	Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

The documentation is available at:

http://downloadcenter.trendmicro.com/

Audience

The Smart Protection Server documentation is written for IT managers and administrators. The documentation assumes that the reader has in-depth knowledge of computer networks.

The documentation does not assume the reader has any knowledge of virus/malware prevention or spam prevention technology.

Document Conventions

The Smart Protection Server User's Guide uses the following conventions.

TABLE 1. Document Conventions

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
 **Note**	Configuration notes
 **Tip**	Recommendations or suggestions
 **WARNING!**	Critical actions and configuration options

Chapter 1

Introduction

This chapter introduces and describes Trend Micro™ Smart Protection Server™ features.

Topics include:

How Does Smart Protection Server Work?

Smart Protection Server is a next-generation, in-the-cloud based, advanced protection solution. At the core of this solution is an advanced scanning architecture that leverages malware prevention signatures that are stored in-the-cloud.

This solution leverages file reputation and web reputation technology to detect security risks. The technology works by off loading a large number of malware prevention signatures and lists that were previously stored on endpoints to Smart Protection Server.

Using this approach, the system and network impact of the ever-increasing volume of signature updates to endpoint is significantly reduced.

The Need for a New Solution

In the current approach to file-based threat handling, patterns (or definitions) required to protect an endpoint are, for the most part, delivered on a scheduled basis. Patterns are delivered in batches from Trend Micro to endpoints. When a new update is received, the virus/malware prevention software on the endpoint reloads this batch of pattern definitions for new virus/malware risks into memory. If a new virus/malware risk emerges, this pattern once again needs to be updated partially or fully and reloaded on the endpoint to ensure continued protection.

Over time, there has been a significant increase in the volume of unique emerging threats. The increase in the volume of threats is projected to grow at a near-exponential rate over the coming years. This amounts to a growth rate that far outnumbers the volume of currently known security risks. Going forward, the volume of security risks represents a new type of security risk. The volume of security risks can impact server and workstation performance, network bandwidth usage, and, in general, the overall time it takes to deliver quality protection - or "time to protect".

A new approach to handling the volume of threats has been pioneered by Trend Micro that aims to make Trend Micro customers immune to the threat of virus/malware volume. The technology and architecture used in this pioneering effort leverages technology that off load the storage of virus/malware signatures and patterns to the cloud. By off loading the storage of these virus/malware signatures to the cloud, Trend

Micro is able to provide better protection to customers against the future volume of emerging security risks.

Smart Protection Network Solutions

The cloud-based query process makes use of two network-based technologies:

- Trend Micro Smart Protection Network™: A globally scaled, Internet-based, infrastructure that provides services to users who do not have immediate access to their corporate network.
- Smart Protection Server: Smart Protection Server exists in the local network. This is made available for users who have access to their local corporate network. These servers are designed to localize operations to the corporate network to optimize efficiency.

Note

Install multiple Smart Protection Server computers to ensure the continuity of protection in the event that connection to a Smart Protection Server is unavailable.

These two network-based solutions host the majority of the virus/malware pattern definitions and web reputation scores. Trend Micro Smart Protection Network and Smart Protection Server make these definitions available to other endpoints on the network for verifying potential threats. Queries are only sent to Smart Protection Servers if the risk of the file or URL cannot be determined by the endpoint.

Endpoints leverage file reputation and web reputation technology to perform queries against Smart Protection Server computers as part of their regular system protection activities. In this solution, agents send identification information, determined by Trend Micro technology, to Smart Protection Server computers for queries. Agents never send the entire file when using file reputation technology. The risk of the file is determined using identification information.

Pattern Files

Smart protection pattern files are used for File Reputation Services and Web Reputation Services. Trend Micro releases these pattern files through the Trend Micro ActiveUpdate server.

The following are the pattern files:

TABLE 1-1. Smart Protection Server Pattern Files

REPUTATION SERVICE	PATTERN	DETAILS
File Reputation Services	**Smart Scan Pattern**	The cloud-based query process makes use of the smart scan pattern file combined with a real-time cloud query system. The cloud query system verifies files, URLs, and other components against a Smart Protection Server during the verification process. Smart Protection Server computers use several algorithms for an efficient process that uses minimal network bandwidth usage. The Smart Scan Pattern is automatically updated hourly.
Web Reputation Services	**Web Blocking Pattern**	Products that use Web Reputation Services (such as Apex One and Deep Security) verify a website's reputation against the Web Blocking Pattern by sending web reputation queries to Smart Protection Server. These products correlate the reputation data received from the smart protection source with the web reputation policy enforced on the endpoint. Depending on the policy, they will either allow or block access to the site. **Note** For a list of products that use Web Reputation Services, see: *Integration with Trend Micro Products and Services on page 2-30*

Pattern Update Process

Pattern updates are a response to security threats. Smart Protection Network and Smart Protection Server computers download the Smart Scan Pattern file from ActiveUpdate servers. Trend Micro products that support Smart Protection Server computers download Smart Scan Agent Patterns from ActiveUpdate servers.

Endpoints within your intranet download Smart Scan Agent Pattern files from Trend Micro products that support Smart Protection Server computers. External endpoints are endpoints that are outside of the intranet and unable to connect to Smart Protection Server computers or Trend Micro products that support Smart Protection Server computers.

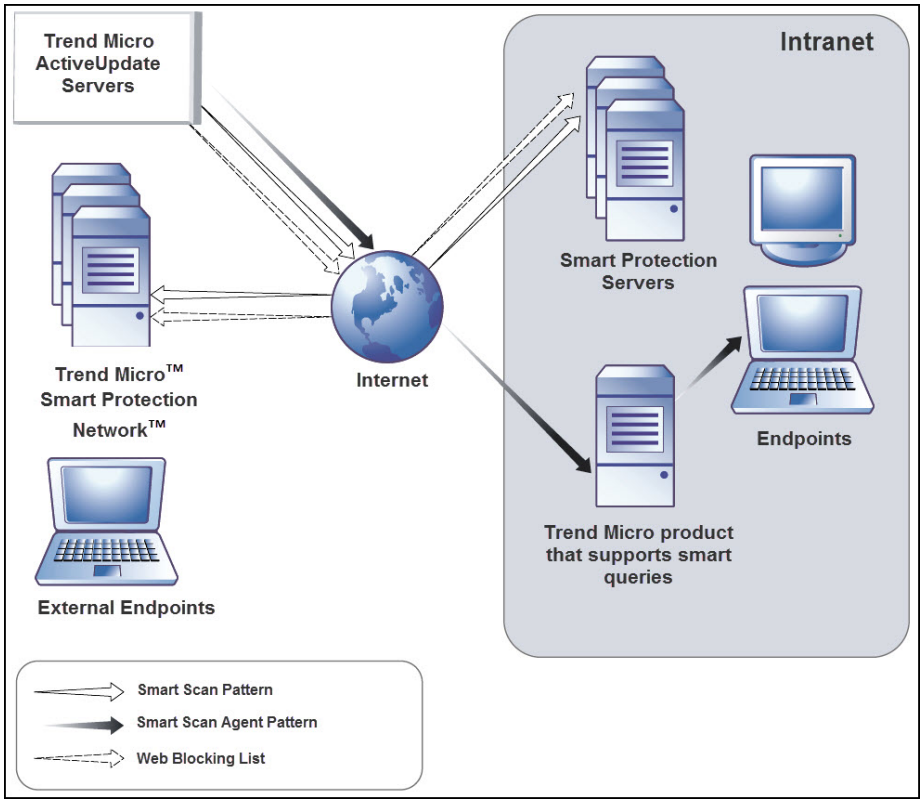


FIGURE 1-1. Pattern update process

The Query Process

Endpoints that are currently in your intranet use Smart Protection Server computers for queries. Endpoints that are currently not in your intranet can connect to Trend Micro Smart Protection Network for queries.

While a network connection is required for utilizing Smart Protection Server computers, endpoints without access to network connection still benefit from Trend Micro technology. Smart Scan Agent Pattern and scan technology that reside on endpoints protect endpoints that do not have access to a network connection.

Agents installed on endpoints first perform scanning on the endpoint. If the agent cannot determine the risk of the file or URL, the agent verifies the risk by sending a query to a Smart Protection Server.

TABLE 1-2. Protection behaviors based on access to intranet

LOCATION	PATTERN FILE AND QUERY BEHAVIOR
Access to intranet	• **Pattern Files**: Endpoints download the Smart Scan Agent Pattern file from Trend Micro products that support Smart Protection Server computers. • **Queries**: Endpoints connect to Smart Protection Server for queries.
Without access to intranet	• **Pattern Files**: Endpoints do not download the latest Smart Scan Agent Pattern file unless connection to a Trend Micro product that support Smart Protection Server computers is available. • **Queries**: Endpoints scan files using local resources such as the Smart Scan Agent Pattern file.

Advanced filtering technology enables the agent to "cache" the query result. This improves scan performance and eliminates the need to send the same query to Smart Protection Server computers more than once.

An agent that cannot verify a file's risk locally and cannot connect to any Smart Protection Server computers after several attempts will flag the file for verification and temporarily allow access to the file. When connection to a Smart Protection Server is restored, all the files that have been flagged are re-scanned. Then, the appropriate scan action is performed on files that have been confirmed as a threat to your network.

Tip

Install multiple Smart Protection Server computers to ensure the continuity of protection in the event that connection to a Smart Protection Server is unavailable.

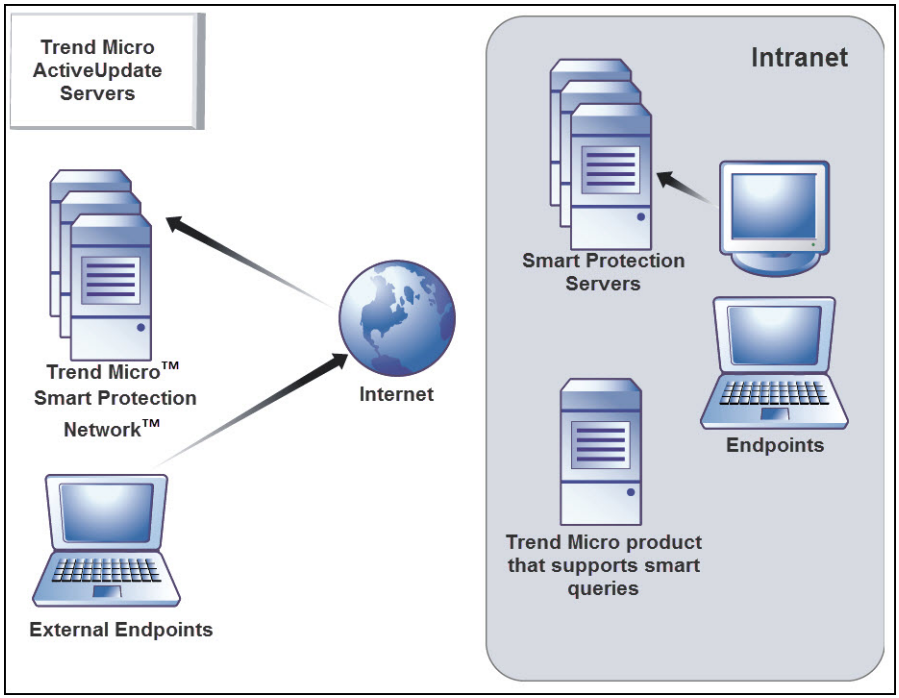


FIGURE 1-2. Query process

What's New

Smart Protection Server includes the following new features and enhancements:

TABLE 1-3. New for Version 3.3 Patch 2

FEATURE	DESCRIPTION
Trend Micro Apex Central Integration	Smart Protection Server integrates with Apex Central through the following features: • Single sign-on (SSO) to Smart Protection Server from the Apex Central console • Automatic synchronization for the Suspicious Objects List • Smart Protection Server status information such as pattern version, service running status, and server build versions are displayed on the Apex Central console For more information, see *Supported Apex Central / Control Manager Versions on page 4-2*.

TABLE 1-4. New for Version 3.3

FEATURE	DESCRIPTION
Redesigned Summary Screen	The redesigned Smart Protection Server dashboard provides a more streamlined view of all widgets and tabs. For more information, see *Using the Summary Screen on page 3-2*.
Support for Community Domain/IP Reputation Service	Smart Protection Server now supports Community Domain/IP Reputation Service query. For more information, see *Integration with Trend Micro Products and Services on page 2-30*.

FEATURE	DESCRIPTION
Trend Micro Control Manager Integration	Smart Protection Server integrates with Control Manager through the following features: • Single sign-on (SSO) to Smart Protection Server from the Control Manager console • Automatic synchronization for the Suspicious Objects List • Smart Protection Server status information such as pattern version, service running status, and server build versions are displayed on the Control Manager console For more information, see *Supported Apex Central / Control Manager Versions on page 4-2*.
Web Reputation HTTPS Support	Web Reputation Service in this version of Smart Protection Server now supports HTTPS connection. For more information, see *Command Line Interface (CLI) Commands on page A-1*.
New Browser Support	Smart Protection Server now supports Google Chrome

Key Features and Benefits

Smart Protection Server provides the following features and benefits:

- File Reputation Technology
  - The corporate network will be better positioned to handle the threat of volume.
  - The overall "time to protect" against emerging threats is greatly decreased.
  - The kernel memory consumption on workstations is significantly lowered and increases minimally over time.
  - Streamlines administration and simplifies management. The bulk of pattern definition updates only need to be delivered to one server instead of many

workstations. This reduces the bulk of the impact of a pattern update on many workstations.

- Protects against web-based and blended attacks.
- Stops viruses/malware, Trojans, worms, plus new variants of these security risks.
- Detects and removes spyware/grayware (including hidden rootkits).

- Web Reputation Technology
  - Protects against web-based and blended attacks.
  - Privacy sensitive customers do not need to worry about revealing confidential information through Web Reputation queries to the Smart Protection Network.
  - Smart Protection Server response time to queries is reduced when compared to queries to Smart Protection Network.
  - Installing a Smart Protection Server in your network reduces the gateway bandwidth load.

Trend Micro Smart Protection Network

The Trend Micro™ Smart Protection Network™ is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and web threats. It powers both local and hosted solutions to protect users whether they are on the network, at home, or on the go, using light-weight agents to access its unique in-the-cloud correlation of email, web and file reputation technologies, and threat databases. Customers' protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for its users.

File Reputation Services

File Reputation Services checks the reputation of each file against an extensive in-the-cloud database. Since the malware information is stored in the cloud, it is available

instantly to all users. High performance content delivery networks and local caching servers ensure minimum latency during the checking process. The cloud-client architecture offers more immediate protection and eliminates the burden of pattern deployment besides significantly reducing the overall agent footprint.

Web Reputation Services

With one of the largest domain-reputation databases in the world, Trend Micro Web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis. It will then continue to scan sites and block users from accessing infected ones. Web reputation features help ensure that the pages that users access are safe and free from web threats, such as malware, spyware, and phishing scams that are designed to trick users into providing personal information. To increase accuracy and reduce false positives, Trend Micro Web reputation technology assigns reputation scores to specific pages or links within sites instead of classifying or blocking entire sites, since often, only portions of legitimate sites are hacked and reputations can change dynamically over time.

Web reputation features help ensure that the web pages that users access are safe and free from web threats, such as malware, spyware, and phishing scams that are designed to trick users into providing personal information. Web reputation blocks web pages based on their reputation ratings. When enabled, Web reputation helps deter users from accessing malicious URLs.

Smart Feedback

Trend Micro™ Smart Feedback provides continuous communication between Trend Micro products as well as the company's 24/7 threat research centers and technologies. Each new threat identified through a single customer's routine reputation check automatically updates all Trend Micro threat databases, blocking any subsequent customer encounters of a given threat. By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides "better together" security, much like an automated neighborhood watch that involves the community in protection of others. Because the threat information gathered is based on the reputation of the communication source, not on the content of the specific

communication, the privacy of a customer's personal or business information is always protected.

Chapter 2

Using Smart Protection Server

This chapter provides Smart Protection Server configuration information.

Topics include:

Initial Configuration

Perform the following tasks after installation.

Important

If you are migrating from Smart Protection Server 3.1, execute the Smart Protection Server Migration Tool (Migration.py) to transfer all of your settings to Smart Protection Server 3.3 before continuing.

For more information, refer to Migrating Settings from Smart Protection Server 3.1 on the Installation Guide.

Procedure

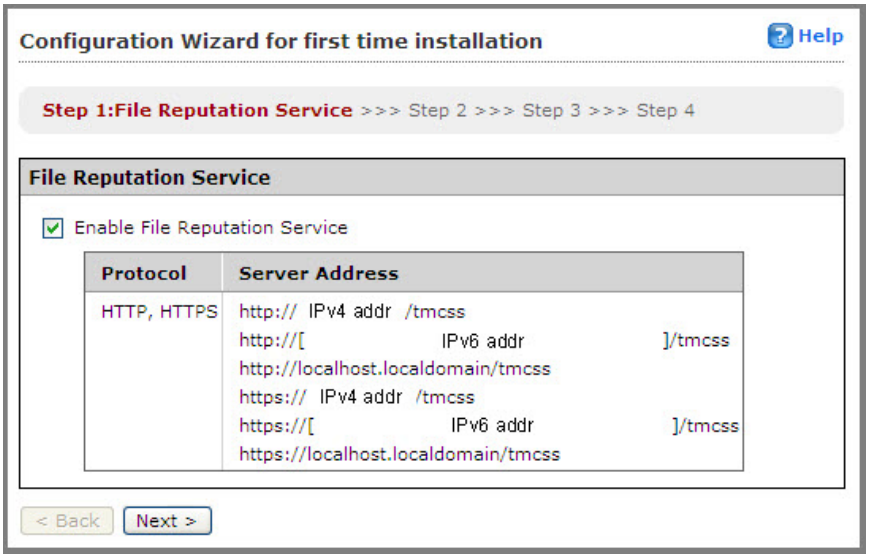
1. Log on to the web console.

   The **Welcome** screen appears.

2. Click **Configure First Time Installation**.

   The first time installation wizard appears.

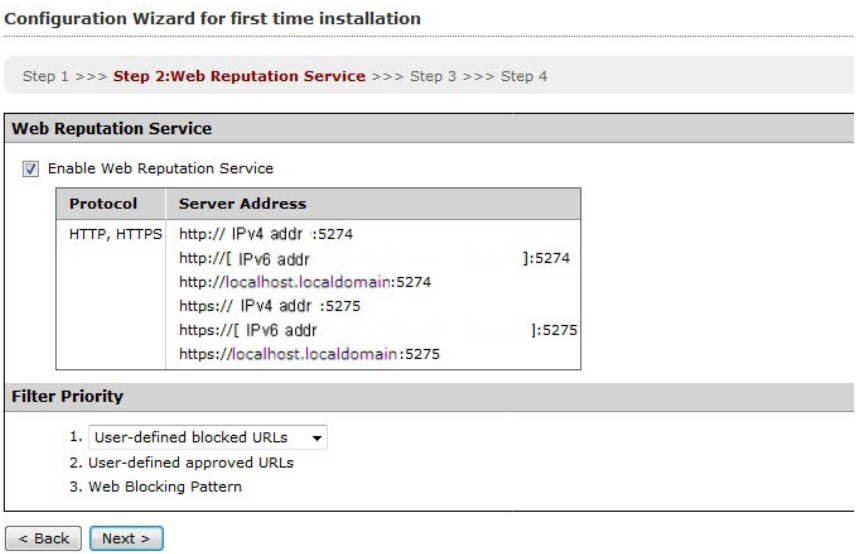
3. Select the **Enable File Reputation Service** check box.



4. Click **Next**.

   The Web Reputation Service screen appears.

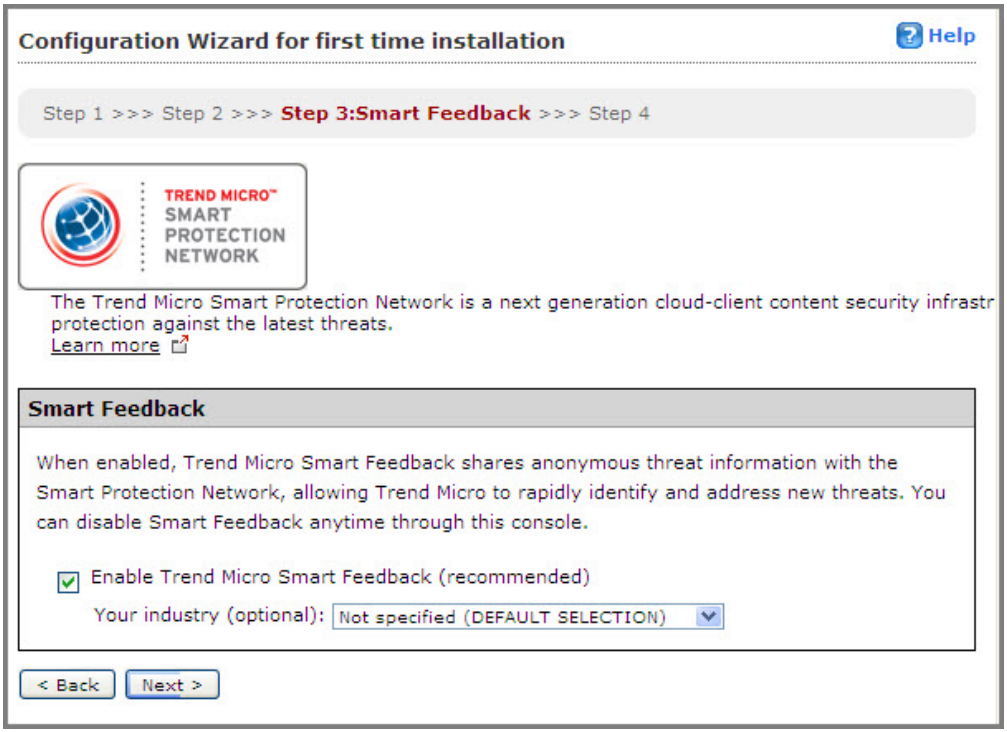
5. Select the **Enable Web Reputation Service** check box.



6. (Optional) The filter priority settings allow you to specify the filter order for URL queries.

7. Click **Next**.

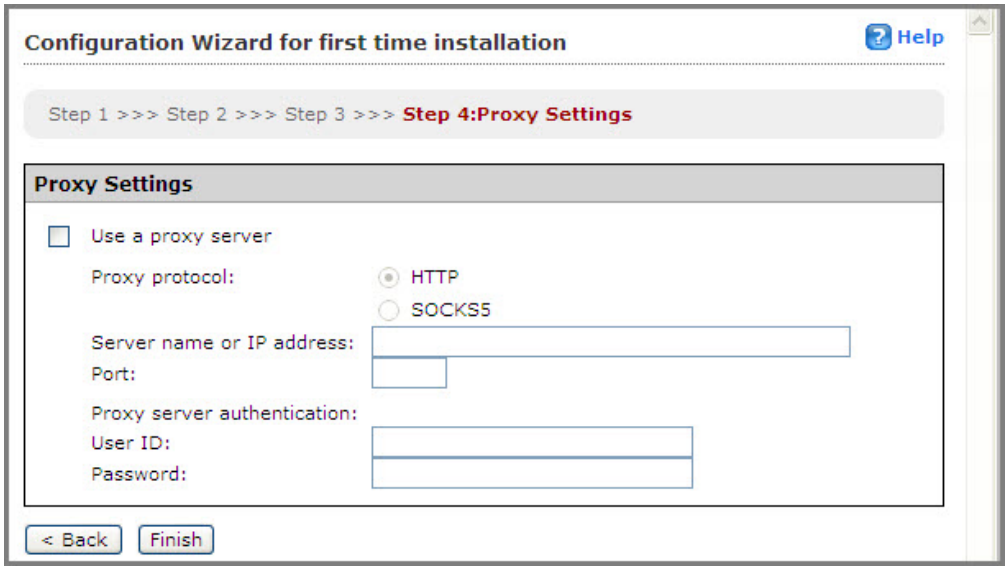
   The Smart Feedback screen appears.



8. Select to use Smart Feedback to help Trend Micro provide faster solutions for new threats.

9. Click **Next**.

   The Proxy Settings screen appears.



10. Specify proxy settings if your network uses a proxy server.

11. Click **Finish** to complete the initial configuration of Smart Protection Server.

    The Summary screen of the web console displays.

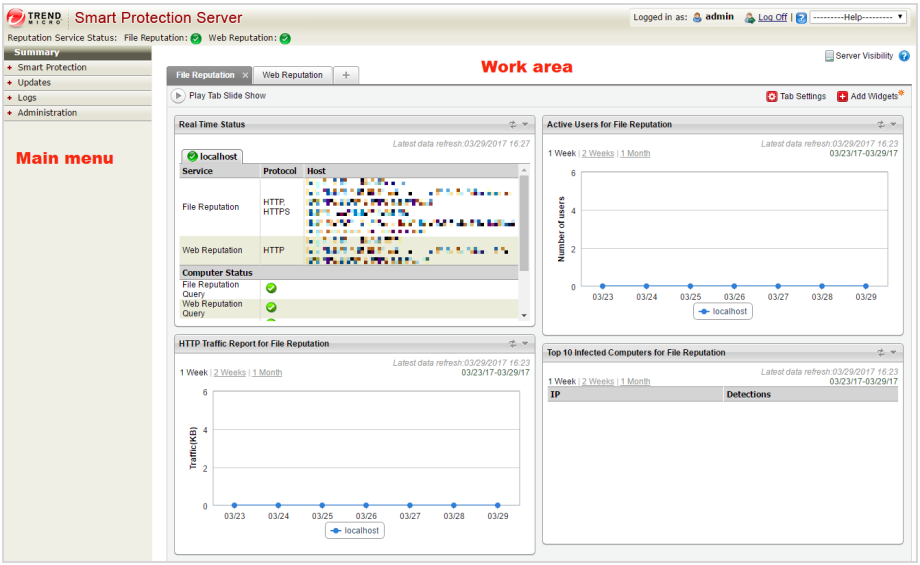
> **Note**
>
> Smart Protection Server will automatically update pattern files after initial configuration.

Using the Product Console

The product console consists of the following elements:

- **Main menu**: Provides links to the **Summary**, **Smart Protection**, **Updates**, **Logs**, and **Administration** screens.

- **Work area**: View summary information and component status, configure settings, update components, and perform administrative tasks.



Menu	Description
Summary	Displays customized information about Smart Protection Server computers, traffic, and detections when you add widgets.
Smart Protection	Provides options for configuring reputation services, user-defined URLs, suspicious objects, and Smart Feedback.
Updates	Provides options for configuring scheduled updates, manual program updates, program package uploads, and the update source.
Logs	Provides options for querying logs and log maintenance.
Administration	Provides options to configure SNMP service, notifications, proxy settings, and collecting diagnostic information for troubleshooting.

Accessing the Product Console

After logging on to the web console, the initial screen displays the status summary for Smart Protection Server computers.

Procedure

1. Open a web browser and type the URL indicated on the initial CLI banner after installation.
2. Type `admin` for the user name and the password in the corresponding fields.
3. Click **Log on**.

Using Smart Protection

This version of Smart Protection Server includes File Reputation and Web Reputation Services.

Using Reputation Services

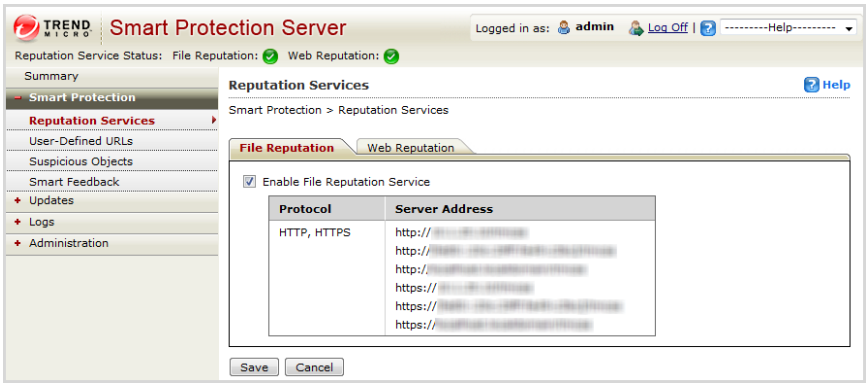
Enable Reputation Services from the product console to allow other Trend Micro products to use smart protection.

Enabling File Reputation Services

Enable File Reputation Services to support queries from endpoints.

Procedure

1. Go to **Smart Protection** > **Reputation Services**, and then go to the **File Reputation** tab.



2. Select the **Enable File Reputation Service** check box.

3. Click **Save**.

   The Server Address can now be used for File Reputation queries by other Trend Micro products that support Smart Protection Server computers.

Enabling Web Reputation Services

Enable Web Reputation Services to support URL queries from endpoints. These are the options available on this screen.

- **Enable Web Reputation Service**: Select to support Web Reputation queries from endpoints.
- **Server Address**: Used by other Trend Micro products for Web Reputation queries.
- **Filter Priority**: Select to specify the priority when filtering URLs.

Procedure

1. Go to **Smart Protection** > **Reputation Services**, and then click the **Web Reputation** tab.

2. Select the **Enable Web Reputation Service** check box.

3. (Optional) Specify the priority of the user-defined approved and blocked URLs when filtering URLs. For example, if **user-defined blocked URLs** has first priority, then **user-defined approved URLs** will be second priority.

4. Click **Save**.

   The Server Address can now be used for Web Reputation queries by other Trend Micro products that support Smart Protection Server.

Configuring User-Defined URLs

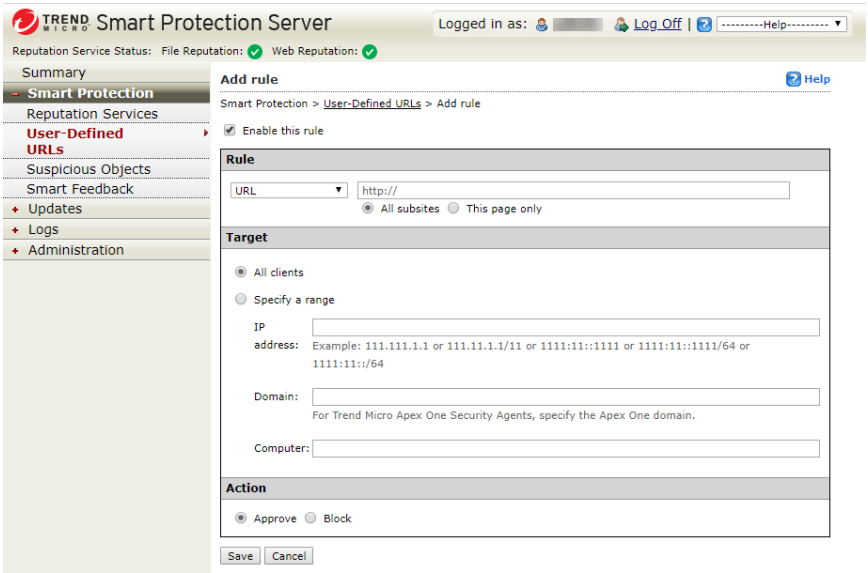
User-Defined URLs allows you to specify your own approved and/or blocked URLs. This is used for Web Reputation. These are the options available on this screen.

- **Search Rule**: Select to search for a string in the list of rules.
- **Test URL**: Select to search for the rules that the URL will trigger. The URL must start with `http://` or `https://`.

Procedure

1. Go to **Smart Protection** > **User-Defined URLs**.
2. Under **Search Criteria**, click **Add**.

   The **Add rule** screen displays.



3. Select the **Enable this rule** check box.
4. Select one of the following:

   - **URL**: to specify a URL and apply to all of the URL's subsites or only one page.
   - **URL with keyword**: to specify a string and use regular expressions.

   Click **Test** to view the results of applying this rule to the most common 20 URLs and the previous day's top 100 URLs in the Web Access Log.

5. Select one of the following:

- **All clients**: to apply to all clients.
- **Specify a range**: to apply to a range of IP addresses, domain names, and computer names.

Note

This supports both IPv4 and IPv6 addresses.

6. Select **Approve** or **Block**.
7. Click **Save**.

Import User-Defined URLs

Use this screen to import user-defined URLs from another Smart Protection Server. These are the options available on this screen.

- **Browse**: Click to select a `.csv` file from your computer.
- **Upload**: Click to upload the selected `.csv` file.
- **Cancel**: Click to return to the previous screen.

Configuring Suspicious Objects

A suspicious object is a known malicious or potentially malicious IP address, domain, URL, or SHA-1 value found in submitted samples.

Smart Protection Server can subscribe to the following sources to synchronize suspicious objects:

TABLE 2-1. Smart Protection Server Suspicious Object Sources

SOURCE	SUSPICIOUS OBJECT TYPE	DESCRIPTION
Deep Discovery Analyzer • **Virtual Analyzer**	URL	Virtual Analyzer is a cloud-based virtual environment designed for analyzing suspicious files. Sandbox images allow observation of file behavior in an environment that simulates endpoints on your network without any risk of compromising the network. Virtual Analyzer in managed products tracks and analyzes submitted samples. Virtual Analyzer flags suspicious objects based on their potential to expose systems to danger or loss.
Apex Central / Control Manager • Consolidated suspicious objects • **User-defined suspicious objects** • **Virtual Analyzer suspicious objects**	URL	Deep Discovery Analyzer sends a list of suspicious objects to Apex Central / Control Manager. Apex Central / Control Manager administrators can add objects they consider suspicious but are not currently in the list of Virtual Analyzer suspicious objects. User-defined suspicious objects have a higher priority than Virtual Analyzer suspicious objects. Apex Central / Control Manager consolidates suspicious objects and scan actions against the objects and then distributes them to Smart Protection Server.

When subscribed, Smart Protection Server relays:

- Suspicious URL information to Trend Micro products (such as Apex One, ScanMail, and Deep Security) that send Web Reputation queries
- Actions against suspicious URLs to Security Agents that send Web Reputation queries.

Note

- For more information on how Apex Central manages suspicious objects, see the *Apex Central Administrator's Guide*.

  You can download a PDF version of the guide, or view the guide online, using the following link:

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

- For more information on how Control Manager manages suspicious objects, see the *Connected Threat Defense Primer* for your version of Control Manager at the following link:

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

Procedure

1. Go to **Smart Protection** > **Suspicious Objects**.
2. Type the FQDN or IP address of the Suspicious Objects **Source**.
3. Type the **API Key** obtained by the suspicious object source.
4. Optional: Click **Test connection** to verify that the server name, IP address, and API key are valid, and that the source is available.
5. Click **Subscribe**.
6. To immediately synchronize suspicious objects, select **Synchronize and enable suspicious objects** and then click **Sync Now**.

   Note

   The option is available only if Smart Protection Server successfully connects to the source.

7. Click **Save**.

Enabling Smart Feedback

Trend Micro Smart Feedback shares anonymous threat information with Trend Micro Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats. You can disable Smart Feedback anytime through this console.

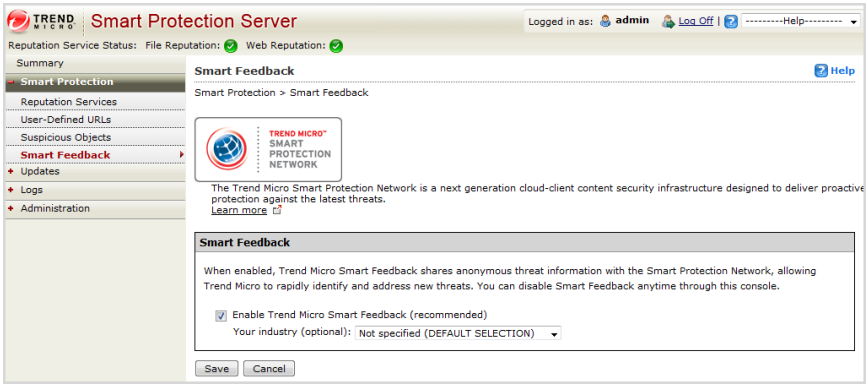
Procedure

1. Go to **Smart Protection** > **Smart Feedback**.

   Note

   Make sure that the Smart Protection Server has Internet connection before enabling Smart Feedback.

2. Select **Enable Trend Micro Smart Feedback**.



3. Select your industry.
4. Click **Save**.

Updates

The effectiveness of Smart Protection Server depends upon using the latest pattern files and components. Trend Micro releases new versions of the Smart Scan Pattern files hourly.

Tip

Trend Micro recommends updating components immediately after installation.

Configuring Manual Updates

To manually update patterns:

Procedure

1. Go to **Updates**.
2. Click **Pattern** or **Program** from the drop down menu.
3. Click **Update Now** or **Save and Update Now** to apply updates immediately.

Configuring Scheduled Updates

To perform scheduled updates:

Procedure

1. Go to **Updates**.
2. Click **Pattern** or **Program** from the drop down menu.
3. Specify the update schedule.
4. Click **Save**.

Pattern File Updates

Update pattern files to help ensure that the latest information is applied to queries. These are the options available on this screen:

- **Enable scheduled updates**: Select to configure automatic updates every hour or every 15 minutes.
- **Update Now**: Click to immediately update all pattern files.

Program File Updates

Update to the latest version of the product program to take advantage of product enhancements. These are the options available on this screen.

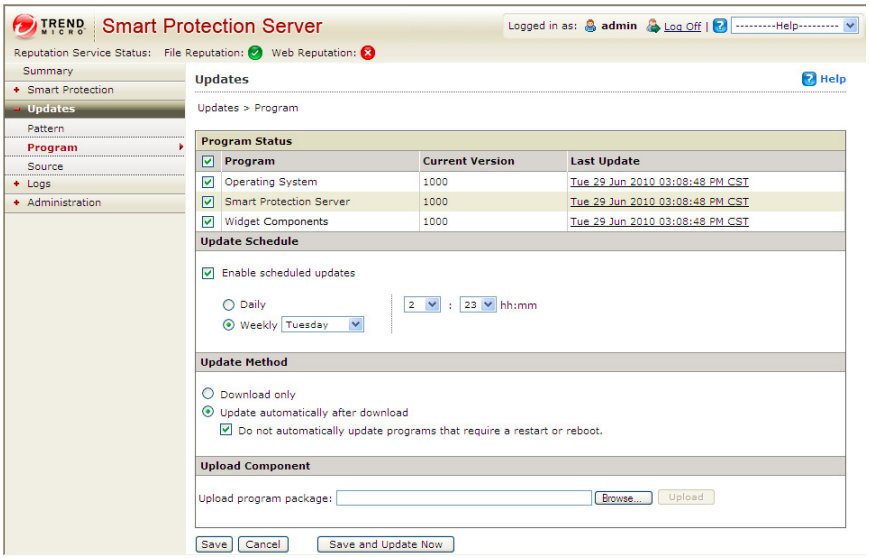
- **Operating System**: Select to update operating system components.
- **Smart Protection Server**: Select to update the product server program file.
- **Widget Components**: Select to update widgets.
- **Enable scheduled updates**: Select to update program files daily at a specified time or weekly.
- **Download only**: Select to download updates and receive a prompt to update program files.
- **Update automatically after download**: Select to apply all updates to the product after download regardless of whether a restart or reboot is required.
- **Do not automatically update programs that require a restart or reboot**: Select to download all updates and only install programs that do not require a restart or reboot.
- **Upload**: Click to upload and update a program file for Smart Protection Server.
- **Browse**: Click to locate a program package.
- **Save and Update Now**: Click to apply settings and perform an update immediately.

There are three ways to update the program file: scheduled updates, manual updates, and by uploading the component.

Enabling Scheduled Updates

Procedure

1. Go to **Updates** > **Program**.
2. Select **Enable scheduled updates** and select the update schedule.



3. Select one of the following update methods:
   - **Download only**: Select this check box to download program files without installing them. A message appears on the web product console when program file updates are available for installation.
   - **Update automatically after download**: Select this check box to automatically install program file updates once the updates have been downloaded.

- **Do not automatically update programs that require a restart or reboot**: Select this check box to receive a prompt on the web product console if the update requires a restart or reboot. Program updates that do not require a restart or reboot will be installed automatically.

4. Click **Save**.

Performing Manual Updates

Procedure

1. Go to **Updates** > **Program**.
2. Select one of the following update methods:
   - **Download only**: Select this check box to download program files without installing them. A message appears on the web product console when program file updates are available for installation.
   - **Update automatically after download**: Select this check box to automatically install program file updates once the updates have been downloaded.
     - **Do not automatically update programs that require a restart or reboot**: Select this check box to receive a prompt on the web product console if the update requires a restart or reboot. Program updates that do not require a restart or reboot will be installed automatically.
3. Click **Save and Update Now**.

Uploading Files to Perform Manual Updates

Procedure

1. Go to **Updates** > **Program**.

Important

Make sure the Smart Protection Server is not performing an update before continuing. If you have to update the program or a component, disable scheduled component updates first before continuing.

2. Under **Upload Component**, click **Browse...** to locate the program file for manual program updates.

Note

Locate the program file that you downloaded from the Trend Micro website or obtained from Trend Micro.

3. Locate the file and click **Open**.
4. Click **Upload**.

Note

If you disabled scheduled scan to update the program or a component, enable it again after uploading and updating.

Available Program Files

Use this screen to update available program files. These are the options available on this screen.

- <Check boxes>: Select the check box for the available program to update.
- **Update Now**: Click to update selected program files.

Configuring an Update Source

Use this screen to specify the update source for File Reputation and Web Reputation. The default update source is the Trend Micro ActiveUpdate Server. These are the options available on this screen.

- **Trend Micro ActiveUpdate Server**: Select to download updates from Trend Micro ActiveUpdate Server.
- **Other update source**: Select to specify an update source, such as Trend Micro Apex Central / Control Manager.

Procedure

1. Go to **Updates** > **Source** and select either the **File Reputation** tab or the **Web Reputation** tab.
2. Select **Trend Micro ActiveUpdate Server** or select **Other update source** and type a URL.
3. Click **Save**.

Administrative Tasks

Administrative tasks allow you to configure SNMP Service settings, notifications, proxy server settings, or download diagnostic information.

SNMP Service

Smart Protection Server supports SNMP to provide further flexibility in monitoring the product. Configure settings and download the Management Information Base (MIB) file from the **SNMP Service** screen. These are the options available on this screen.

- **Enable SNMP Service**: Select to use SNMP.
- **Community name**: Specify an SNMP community name.
- **Enable IP restriction**: Select to enable IP address restriction.

Note

Classless Inter-Domain Routing (CIDR) is not supported for IP restriction. Prevent unauthorized access to the SNMP service by enabling IP address restriction.

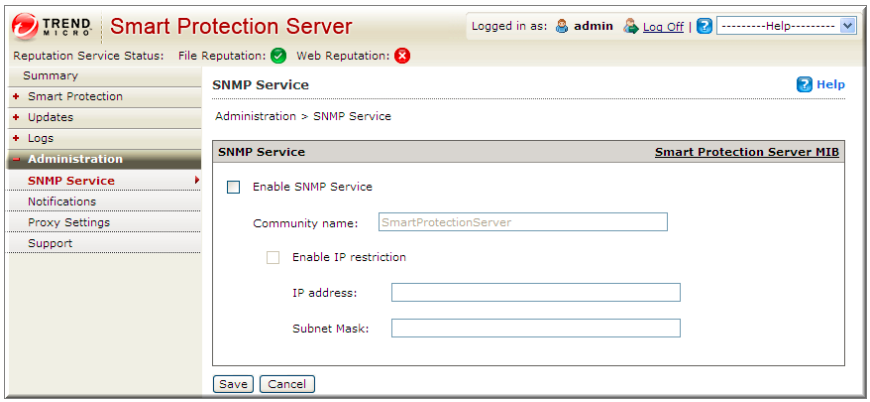
- **IP address**: Specify an IP address for using the SNMP service to monitor Health Status.
- **Subnet Mask**: Specify a netmask to define the IP address range for using the SNMP service to monitor computer status.
- **Smart Protection Server MIB**: Click to download the Smart Protection Server MIB file.
- **Save**: Click to retain the settings.
- **Cancel**: Click to discard changes.

Configuring SNMP Service

Configure SNMP Service settings to allow SNMP managing systems to monitor Smart Protection Server status.

Procedure

1. Go to **Administration** > **SNMP Service**.



2. Select the **Enable SNMP Service** check box.
3. Specify a **Community name**.

4. Select the **Enable IP restriction** check box to prevent unauthorized access to the SNMP service.

Note

Classless Inter-Domain Routing (CIDR) is not supported for IP restriction.

5. Specify an IP address.
6. Specify a subnet mask.
7. Click **Save**.

Downloading the MIB File

Download the MIB file from the web console to use SNMP Service.

Procedure

1. Go to **Administration** > **SNMP Service**.
2. Click **Smart Protection Server MIB** to download the MIB file. A confirmation prompt displays.
3. Click **Save**.

   The **Save As** screen displays.
4. Specify the save location.
5. Click **Save**.

Smart Protection Server MIB

The following table provides a description of the Smart Protection Server MIB.

Object Name	Object Identifier (OID)	Description
Trend-MIB:: TBLVersion	1.3.6.1.4.1.6101.1.2.1.1	Returns the current Smart Scan Pattern version.
Trend-MIB:: TBLLastSuccessfulUpdate	1.3.6.1.4.1.6101.1.2.1.2	Returns the date and time of the last successful Smart Scan Pattern update.
Trend-MIB:: LastUpdateError	1.3.6.1.4.1.6101.1.2.1.3	Returns the status of the last Smart Scan Pattern update. • 0: Last pattern update was successful. • <error code>: Last pattern update was unsuccessful.
Trend-MIB:: LastUpdateErrorMessage	1.3.6.1.4.1.6101.1.2.1.4	Returns an error message if the last Smart Scan Pattern update was unsuccessful.
Trend-MIB:: WCSVersion	1.3.6.1.4.1.6101.1.2.1.5	Returns the current Web Blocking Pattern version.
Trend-MIB:: WCSLastSuccessfulUpdate	1.3.6.1.4.1.6101.1.2.1.6	Returns the date and time of the last successful Web Blocking Pattern update.
Trend-MIB:: WCSLastUpdateError	1.3.6.1.4.1.6101.1.2.1.7	Returns the status of the last Web Blocking Pattern update. • 0: Last pattern update was successful. • <error code>: Last pattern update was unsuccessful.
Trend-MIB:: WCSLastUpdateErrorMessage	1.3.6.1.4.1.6101.1.2.1.8	Returns an error message if the last Web Blocking Pattern update was unsuccessful.

OBJECT NAME	OBJECT IDENTIFIER (OID)	DESCRIPTION
Trend-MIB:: LastVerifyError	1.3.6.1.4.1.6101.1.2.2.2	Returns the status of file reputation query. • 0: File reputation query is behaving as expected. • <error code>: File reputation query is not behaving as expected.
Trend-MIB:: WCSLastVerifyError	1.3.6.1.4.1.6101.1.2.2.3	Returns the status of web reputation query. • 0: Web reputation query is behaving as expected. • <error code>: Web reputation query is not behaving as expected.
Trend-MIB:: LastVerifyErrorMessage	1.3.6.1.4.1.6101.1.2.2.4	Returns an error message if the last health status of a File Reputation query was unsuccessful.
Trend-MIB:: WCSLastVerifyErrorMessage	1.3.6.1.4.1.6101.1.2.2.5	Returns an error message if the last health status of a Web Reputation query was unsuccessful.

Supported MIB

The following table provides a description of other supported MIBs.

OBJECT NAME	OBJECT IDENTIFIER (OID)	DESCRIPTION
SNMP MIB-2 System	1.3.6.1.2.1.1	The system group includes information about the system on which the entity resides. Object in this group are useful for fault management and configuration management. See IETF RFC 1213.

Object Name	Object Identifier (OID)	Description
SNMP MIB-2 Interfaces	1.3.6.1.2.1.2	The interfaces object group contains information about each interface on a network device. This group provides useful information on fault management, configuration management, performance management and accounting management. See IETF RFC 2863.

Proxy Settings

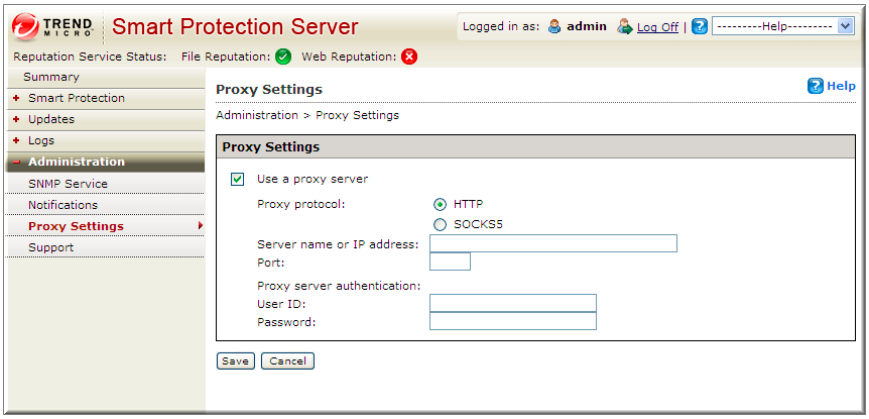
If you use a proxy server in the network, configure proxy settings. These are the options available on this screen.

- **Use a proxy server**: Select if your network uses a proxy server.
- **HTTP**: Select if your proxy server uses HTTP as the proxy protocol.
- **SOCKS5**: Select if your proxy server uses SOCKS5 as the proxy protocol.
- **Server name or IP address**: Type the proxy server name or IP address.
- **Port**: Type the port number.
- **User ID**: Type the user ID for the proxy server if your proxy server requires authentication.
- **Password**: Type the password for the proxy server if your proxy server requires authentication.

Configuring Proxy Settings

Procedure

1. Go to **Administration** > **Proxy Settings**.



2. Select the **Use a proxy server** for updates check box.
3. Select **HTTP** or **SOCKS5** for the Proxy protocol.

> **Note**
>
> Smart Protection Server no longer supports SOCKS4 proxy configurations.

4. Type the server name or IP address.
5. Type the port number.
6. If your proxy server requires credentials, type the **User ID** and **Password**.
7. Click **Save**.

Support

Use the web console to download diagnostic information for troubleshooting and support.

Click **Start** to begin collecting diagnostic information.

Downloading System Information for Support

Procedure

1. Go to **Administration** > **Support**.
2. Click **Start**.

   The download progress screen appears.
3. Click **Save** when the prompt for the downloaded file appears.
4. Specify the location and file name.
5. Click **Save**.

Changing the Product Console Password

The product console password is the primary means to protect Smart Protection Server from unauthorized changes. For a more secure environment, change the console password on a regular basis and use a password that is difficult to guess. The admin account password can be changed through the Command Line Interface (CLI). Use the "configure password" command from the CLI to make changes.

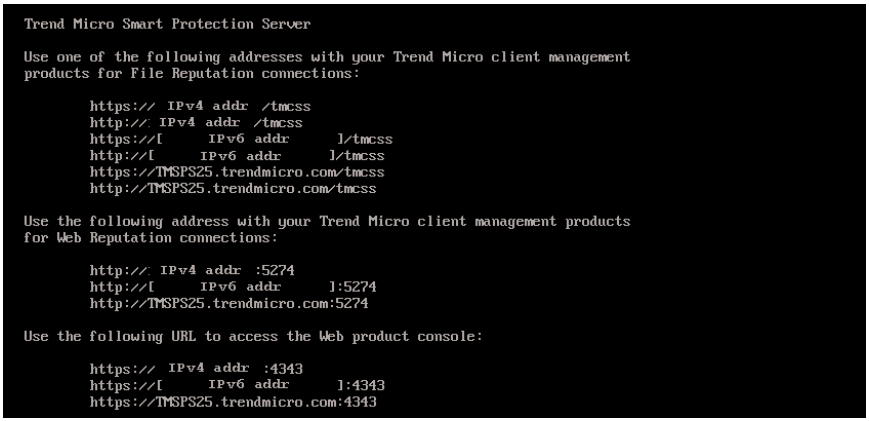
Tip

To design a secure password consider the following:

- Include both letters and numbers.
- Avoid words found in any dictionary (of any language).
- Intentionally misspell words.
- Use phrases or combine words.
- Use a combination of uppercase and lowercase letters.
- Use symbols.

Procedure

1. Log on to the CLI console with the admin account.



2. Type the following to enable administrative commands:

   `enable`

3. Type the following command:

   `configure password admin`

4. Type the new password.

5. Type the new password a second time to confirm the password.

Importing Certificates

This Smart Protection Server version allows administrators to regenerate or import the server certificate for safety and security.

Procedure

1. Go to **Administration** > **Certificate**.

   The current "Server Certificate Information" displays.

2. Click **Replace the current certificate**.

3. Click **Browse...** to select a valid certificate to upload. The certificate must be a .pem file.

4. Click **Next**.

5. Check the details for the new certificate, and click **Finish**. Wait a few seconds for the certificate to import.

Integration with Trend Micro Products and Services

Smart Protection Server integrates with the Trend Micro products and services listed in the following tables. Refer to the relevant sections of the integrating products' online help for integration details.

TABLE 2-2. File Reputation Services

COMPONENTS USED	COMPONENT SOURCE	INTEGRATING PRODUCTS AND MINIMUM SUPPORTED VERSIONS	FIRST SMART PROTECTION SERVER VERSION
Smart Scan Pattern **Note** Smart Scan Pattern works in conjunction with the Smart Scan Agent Pattern installed on the integrating product.	• Trend Micro ActiveUpdate Server (default) • HTTP or HTTPS supported as an other update source	• Apex One 2019 • OfficeScan 10 • Core Protection Module 10.5 • Deep Security 7.5 • InterScan Messaging Security Virtual Appliance 9.1 • InterScan Web Security Virtual Appliance 6.5 SP1 • ScanMail for Microsoft Exchange 10 SP1 • PortalProtect 2.1 for SharePoint 2.1 • Threat Mitigator 2.5 • Worry-Free Business Security 6.0	1.0
Smart Protection Service Proxy (used for Community File Reputation)	N/A (built in)	• Apex One 2019 • Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1 • OfficeScan XG	3.0 Patch 2

TABLE 2-3. Web Reputation Services

COMPONENTS USED	COMPONENT SOURCE	INTEGRATING PRODUCTS AND MINIMUM SUPPORTED VERSIONS	FIRST SMART PROTECTION SERVER VERSION
Web Blocking Pattern	• Trend Micro Active Update Server (default) • Other update source supported	• Apex One 2019 • OfficeScan 10.5 • Core Protection Module 10.5 • Deep Discovery Inspector 2.6 • Deep Security 7.5 • ScanMail for Microsoft Exchange 10.0 SP1 • ScanMail for Lotus Domino 5.6 • PortalProtect 2.1 • Trend Micro Security (for Mac) 2.0	2.0
Approved/Blocked URLs	N/A (list configured directly on the Smart Protection Server console)		2.0
Suspicious URLs	• Apex Central 2019 • Control Manager 6.0 SP2 • Deep Discovery Analyzer 5.0		2.6 Patch 1
Enhanced Suspicious URLs	• Apex Central 2019 • Control Manager 6.0 SP3	• Apex One 2019 • OfficeScan 11 SP1	3.0 Patch 1

Components Used	Component Source	Integrating Products and Minimum Supported Versions	First Smart Protection Server Version
Smart Protection Service Proxy (used for Web Inspection Service)	N/A (built in)	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1	3.0 Patch 2
Smart Protection Service Proxy (used for Community Domain/IP Reputation Service)	N/A (built in)	• Deep Discovery Inspector 5.0 • Deep Discovery Analyzer 6.0	3.3

Table 2-4. Mobile App Reputation Services

Components Used	Component Source	Integrating Products and Minimum Supported Versions	First Smart Protection Server Version
Smart Protection Service Proxy	N/A (built in)	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1	3.0 Patch 2

TABLE 2-5. Certified Safe Software Service

COMPONENTS USED	COMPONENT SOURCE	INTEGRATING PRODUCTS AND MINIMUM SUPPORTED VERSIONS	FIRST SMART PROTECTION SERVER VERSION
Smart Protection Service Proxy	N/A (built in)	• Deep Discovery Email Inspector 2.5 • Deep Discovery Inspector 3.8 SP2 • Deep Discovery Analyzer 5.5 SP1	3.0 Patch 2

TABLE 2-6. Predictive Machine Learning

COMPONENTS USED	COMPONENT SOURCE	INTEGRATING PRODUCTS AND MINIMUM SUPPORTED VERSIONS	FIRST SMART PROTECTION SERVER VERSION
Smart Protection Service Proxy	N/A (built in)	• Apex One 2019 • OfficeScan XG • Deep Discovery Inspector 5.0 • Deep Discovery Email Inspector 3.0 • Deep Discovery Analyzer 6.0	3.1

Note

The Smart Protection Service Proxy redirects query requests from integrated products to the Smart Protection Network for further analysis.

Chapter 3

Monitoring Smart Protection Server

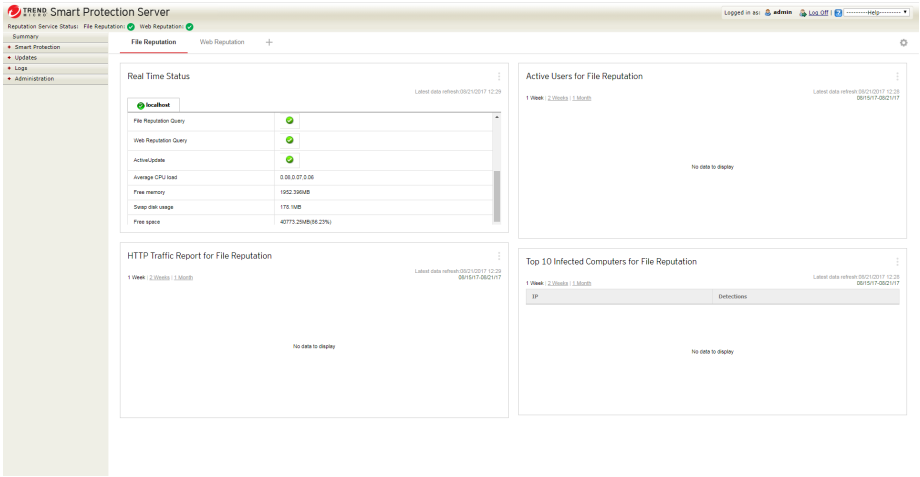
Monitor Smart Protection Server with logs and from the Summary screen with widgets.

Topics include:

Using the Summary Screen

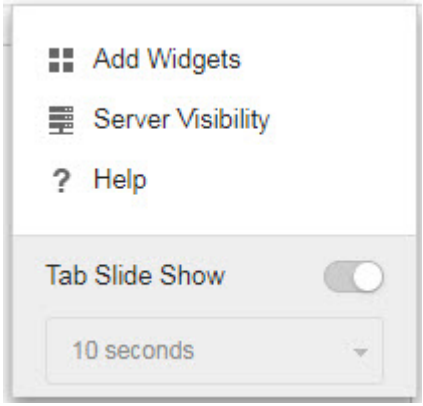
The **Summary** screen can display customized information about Smart Protection Server computers, traffic, and detections.

File Reputation Services and Web Reputation Services support both HTTP and HTTPS protocols. HTTPS provides a more secure connection while HTTP uses less bandwidth. Smart Protection Server addresses are displayed on the Command Line Interface (CLI) console banner.



Click the gear icon (⚙) to access the **Server Visibility** list on the **Summary** screen.

FIGURE 3-1. Server Visibility



Use the **Server Visibility** list to add servers to the Server Visibility list or configure proxy server settings for connection to servers in the Server Visibility list. Editing server information is the same for all widgets.

Note

Smart Protection Server Addresses are used with Trend Micro products that manage endpoints. Server Addresses are used for configuring endpoint connections to Smart Protection Server computers.

Working with Tabs

Manage tabs by adding, renaming, changing the layout, deleting, and automatically switching between tab views.

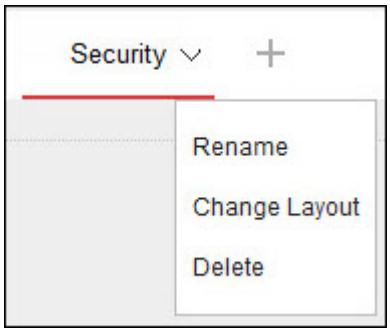
Procedure

1. Go to the **Summary Screen**.
2. To add a new tab:
   a. Click add icon.

b. Type a name for the new tab.

3. To rename a tab:

   a. Hover over the tab name and click the down arrow.



   b. Click **Rename** and type the new tab name.

4. To change the layout of the widgets for a tab:

   a. Hover over the tab name and click the down arrow.

   b. Click **Change Layout**.

   c. Select the new layout from the screen that appears.

   d. Click **Save**.

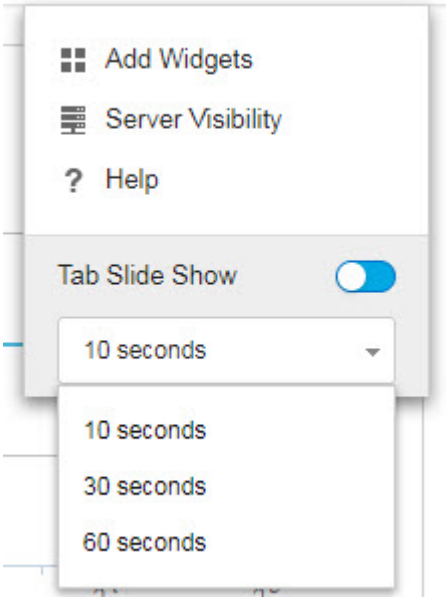
5. To delete a tab:

   a. Hover over the tab name and click the down arrow.

   b. Click **Delete** and confirm.

6. To play a tab slide show:

   a. Click the **Settings** icon to the right of the tab display.



b. Enable the **Tab Slide Show** control.

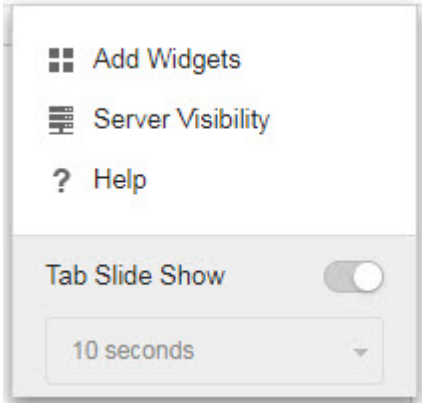
c. Select the length of time each tab displays before switching to the next tab.

Working with Widgets

Manage widgets by adding, moving, resizing, renaming, and deleting items.

Procedure

1. Go to the **Summary Screen**.
2. Click a tab.
3. To add a widget:
   a. Click the **Settings** icon to the right of the tab display.



b. Click **Add Widgets**.

c. Select the widgets to add.

- In the drop-down on top of the widgets, select a category to narrow down the selections.
- Use the search text box on top of the screen to search for a specific widget.

d. Click **Add**.

4. To move a widget to a new location on the same tab, drag-and-drop a widget to a new location.

5. Resize widgets on a multi-column tab by pointing the cursor to the right edge of the widget and then moving the cursor to the left or right.

6. To rename a widget:

   a. Click the settings icon (>).

   b. Type the new title.

   c. Click **Save**.

7. To delete a widget, click the delete icon (>).

Available Widgets

The following widgets are available in this release.

Real Time Status

Use the real time status widget to monitor the Smart Protection Server status.

Note

When this widget displays on the Summary screen, the product console session will not expire. The Computer Status is updated every minute which means the session will not expire due to the requests sent to the server. However, the session will still expire if the tab that is currently displayed does not contain this widget.

TABLE 3-1. Widget Data

DATA	DESCRIPTION
Service	Services provided by the Smart Protection Server.
Protocol	This displays the protocols supported by services. File Reputation Services and Web Reputation Services support both HTTP and HTTPS protocols. HTTPS provides a more secure connection while HTTP uses less bandwidth.
Host	File Reputation and Web Reputation Service addresses. These addresses are used with Trend Micro products that support Smart Protection Server computers. The addresses are used for configuring connections to Smart Protection Server computers.

DATA	DESCRIPTION
Computer Status	The following items are displayed under Health Status: • **File Reputation Query**: displays whether File Reputation is functioning as expected. • **Web Reputation Query**: displays whether Web Reputation is functioning as expected. • **ActiveUpdate**: displays whether ActiveUpdate is functioning as expected. • **Average CPU load**: displays the computer load average for the past 1, 5, and 15 minutes generated by the kernel. • **Free memory**: displays the available physical memory on the computer. • **Swap disk usage**: displays the swap disk usage. • **Free space**: displays the available free disk space on the computer.

Active Users for File Reputation

The Active Users widget displays the number of users that have made file reputation queries to the Smart Protection Server. Each unique client computer is considered an active user.

Note

This widget displays information in a 2-D graph and is updated every hour or click the refresh icon ( ) at any time to update the data.

TABLE 3-2. Widget Data

DATA	DESCRIPTION
Users	The number of users that sent queries to Smart Protection Server computers.
Date	The date of the query.

HTTP Traffic Report for File Reputation

The HTTP Traffic Report widget displays the total amount of network traffic in kilobytes (KB) that has been sent to the Smart Protection Server from file reputation queries generated by clients. The information in this widget is updated hourly. You can also click the refresh icon () at any time to update the data.

TABLE 3-3. Widget Data

DATA	DESCRIPTION
Traffic (KB)	The network traffic generated by queries.
Date	The date of the queries.

Top 10 Infected Computers for File Reputation

This widget displays the top 10 computer IP addresses which have been classified as infected computers after Smart Protection Server receives a known virus from file reputation query. Information in this widget is displayed in a table, which includes the computer IP address and the total number of detections on each computer. The information in this widget is updated hourly or you can click the refresh icon () at any time to update the data.

Use this widget to track computers with the most number of infections on your network.

Note

If you enable more than one Smart Protection Server in this widget, this widget will calculate the total number of detections on the selected Smart Protection Server and display the top 10 infected computers from the selected Smart Protection Server computers in the list.

TABLE 3-4. Widget Data

DATA	DESCRIPTION
IP	The IP address of the computer

DATA	DESCRIPTION
Detections	The number of security threats detected by this computer

Active Users for Web Reputation

The Active Users widget displays the number of users that have made web reputation queries to the Smart Protection Server. Each unique client computer is considered an active user.

Note

This widget displays information in a 2-D graph and is updated every 5 minutes or click the refresh icon ( ) at any time to update the data.

TABLE 3-5. Widget Data

DATA	DESCRIPTION
Users	The number of users that sent queries to Smart Protection Server computers.
Date	The date of the query.

HTTP Traffic Report for Web Reputation

The HTTP Traffic Report widget displays the total amount of network traffic in kilobytes (KB) that has been sent to the Smart Protection Server from web reputation queries generated by clients. The information in this widget is updated hourly. You can also click the refresh icon ( ) at any time to update the data.

TABLE 3-6. Widget Data

DATA	DESCRIPTION
Traffic (KB)	The network traffic generated by queries.
Date	The date of the queries.

Top 10 Blocked Computers for Web Reputation

This widget displays the top 10 computer IP addresses which have been classified as blocked computers after the Smart Protection Server receives a URL for web reputation query. Information in this widget is displayed in a table, which includes the computer IP address and the total number of blocked URLs on each computer. The information in this widget is updated daily or you can click the refresh icon ( ) at any time to update the data.

Use this widget to track computers who access the most number of blocked sites on your network.

Note

If you enable more than one Smart Protection Server in this widget, this widget will calculate the total number of detections on the selected Smart Protection Server and display the top 10 blocked computers from the selected Smart Protection Server computers in the list.

TABLE 3-7. Widget Data

DATA	DESCRIPTION
IP	The IP address of the computer.
Detections	The number of blocked URLs from this computer.

Logs

Use logs to monitor the status of Smart Protection Server. To view log information, perform a query.

Blocked URLs

The **Blocked URLs** screen displays information for Web Reputation queries that return malicious results.

Below are the options available on this screen.

- **Keyword**: Specify keywords to use when searching for URLs.
- **Date Range**: Select a date range.
- **Source**: Select one or more sources to display the corresponding logs.
  - **User-defined blocked URLs**: Displays blocked URLs that match the Smart Protection Server user-defined blocked URLs.
  - **Web Blocking Pattern**: Displays blocked URLs that match entries in the Web Blocking Pattern.
  - **C&C URLs matched with:** Displays blocked URLs that match entries in the following sources:
    - **Apex Central user-defined suspicious objects**: A subset of the user-defined suspicious objects in Apex Central / Control Manager
    - **Virtual Analyzer**: A subset of the suspicious objects in Virtual Analyzer enabled products, such as Deep Discovery Advisor, Deep Discovery Analyzer, and Apex Central / Control Manager
    - **Global Intelligence in Web Blocking Pattern**: Trend Micro Smart Protection Network compiles the Global Intelligence list from sources all over the world and tests and evaluates the risk level of each C&C callback address. Web Reputation Services uses the Global Intelligence list in conjunction with the reputation scores for malicious websites to provide enhanced security against advanced threats. The web reputation security level determines the action taken on malicious websites or C&C servers based on assigned risk levels.

Below are the details displayed on this screen:

- **Date and time**: The date and time of the blocked URL event.
- **URL**: The blocked URL.
- **Display log**: Displays source information about the blocked URL.
- **Client GUID**: The GUID of the computer that attempted to access the blocked URL.
- **Server GUID**: The GUID of the Trend Micro product that supports Smart Protection Server computers.

- **Client IP**: The IP address of the computer that attempted to access the blocked URL.
- **Computer**: The name of the computer that attempted to access the blocked URL.
- **Product Entity**: The Trend Micro product that detected the URL.

Update Log

The Update Log screen displays information about pattern or program file updates. These are the options available on this screen.

- **Date Range**: Select the date range that the update took place.
- **Type**: Select the type of update to display.

Log Details:

- **Date and time**: The date and time the server was updated.
- **Component Name**: The component that was updated.
- **Result**: This can either be successful or unsuccessful.
- **Description**: This describes the update event.
- **Update Method**: This shows either conventional or smart scan.

Reputation Service Log

The Reputation Service Log screen displays service status information for Web Reputation and File Reputation. These are the options available on this screen.

- **Service**: Specify the service.
- **Result**: Specify the result type.
- **Date Range**: Select a date range.

Log Details:

- **Date and time**: The date and time the reputation checked the service status for Web Reputation or File Reputation.
- **Service**: This can either be Web Reputation or File Reputation.
- **Result**: This can either be successful or unsuccessful.
- **Description**: This describes the service status for Web Reputation or File Reputation.

Log Maintenance

Perform log maintenance to delete logs that are no longer needed. These are the options available on this screen.

- **Pattern Update Log**: Select to purge pattern update log entries.
- **Program Update Log**: Select to purge update log entries.
- **Blocked URLs**: Select to purge URL query entries.
- **Reputation Service Log**: Select to purge reputation service event entries.
- **Delete all logs**: Select to delete all logs.
- **Purge logs older than the following number of days**: Select to purge older logs.
- **Enable scheduled purge**: Select to schedule automatic purge.

Procedure

1. Go to **Logs** > **Log Maintenance**.
2. Select the log types to purge.
3. Select to delete all logs or logs older than a specified number of days.
4. Select a purge schedule or click **Purge Now**.
5. Click **Save**.

Notifications

You can configure Smart Protection Server to send email message or Simple Network Management Protocol (SNMP) trap notifications to designated individuals when there is a status change in services or updates.

Email Notifications

Configure email notification settings to notify administrators through email messages when there is a status change in services or updates. These are the options available on this screen.

- **SMTP server**: Type the SMTP server IP address.
- **Port number**: Type the SMTP server port number.
- **From**: Type an email address for the sender field of email notifications.
- **Services**: Select to send notifications for status changes in File Reputation, Web Reputation, and Pattern Update.
- **To**: Type an email address, or multiple email addresses, to send notifications for this event.
- **Subject**: Type a new subject or use the default subject text for this event.
- **Message**: Type a new message or use the default message text for this event.
- **File Reputation Status Change**: Select to send a notification for status changes and specify the recipient for this notification.
- **Web Reputation Status Change**: Select to send a notification for status changes and specify the recipient for this notification.
- **Pattern Update Status Change**: Select to send a notification for status changes and specify the recipient for this notification.
- **Updates**: Select to send notifications for all program related notifications.

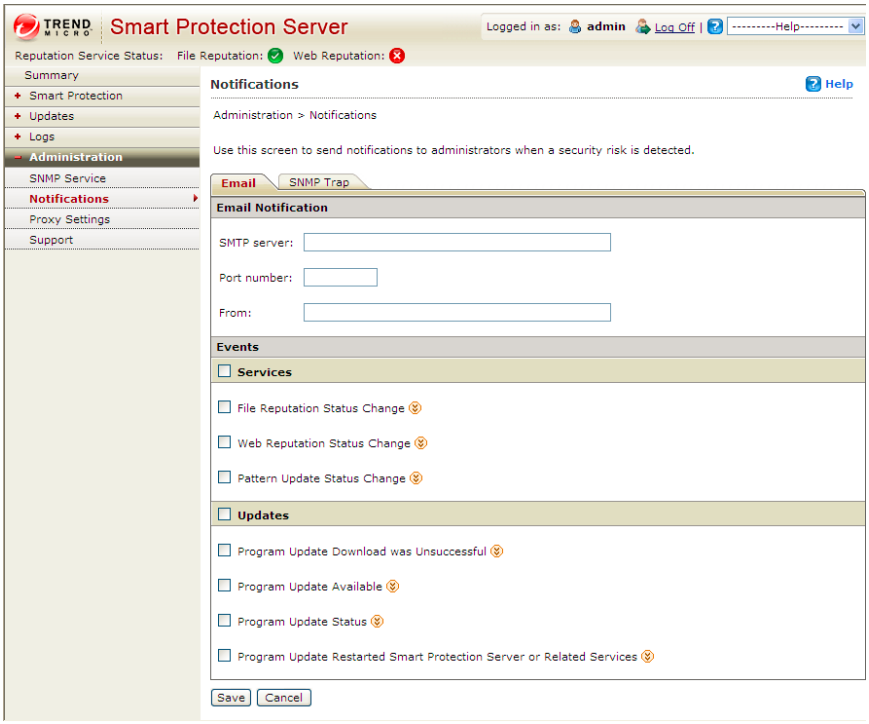
- **Program Update Download was Unsuccessful**: Select to send a notification if the program update did not download successfully and specify the recipient for this notification.
- **Program Update Available**: Select to send a notification if a program update is available that requires confirmation and specify the recipient for this notification.
- **Program Update Status**: Select to send a notification a program has been updated and specify the recipient for this notification.
- **Program Update Restarted Smart Protection Server or Related Services**: Select to send a notification if the program update process restarted Smart Protection Server or related services and specify the recipient for this notification.
- **Default Message**: Click to revert the Subject and Message fields to Trend Micro default text.

Configuring Email Notifications

Procedure

1. Go to **Administration** > **Notifications** and then go to the **Email** tab.

The tab for email notifications appears.



2. Select the **Services** check box to receive an email notification for status changes for all the services or select specific services from the options shown:

   - **File Reputation Status Change**: Select to send a notification for status changes and specify the recipient, subject, and message.
   - **Web Reputation Status Change**: Select to send a notification for status changes and specify the recipient, subject, and message.
   - **Pattern Update Status Change**: Select to send a notification for status changes and specify the recipient, subject, and message.

3. Select the **Updates** check box or select from the following:

- **Program Update Download was Unsuccessful**: Select to send a notification for this event and specify the recipient, subject, and message.
- **Program Update Available**: Select to send a notification for this event and specify the recipient, subject, and message.
- **Program Update Status**: Select to send a notification for this event and specify the recipient, subject, and message.
- **Program Update Restarted Smart Protection Server or Related Services**: Select to send a notification for this event and specify the recipient, subject, and message.

4. Type the SMTP server IP address in the **SMTP server** field.
5. Type the SMTP port number.
6. Type an email address in the **From** field. All email notifications will show this address in the From field of email messages.
7. Click **Save**.

SNMP Trap Notifications

Configure Simple Network Management Protocol (SNMP) notification settings to notify administrators through SNMP trap when there is a status change in services. These are the options available on this screen.

- **Server IP address**: Specify the SNMP trap receiver IP address.
- **Community name**: Specify the SNMP community name.
- **Services**: Select to send an SNMP notification for status changes in File Reputation, Web Reputation, and pattern updates.
- **Message**: Type a new message or use the default message text for this event.
- **File Reputation Status Change**: Select to send a notification for status changes.
- **Web Reputation Status Change**: Select to send a notification for status changes.

- **Pattern Update Status Change**: Select to send a notification for status changes.
- **Default Message**: Click to revert the Message fields to Trend Micro default text.

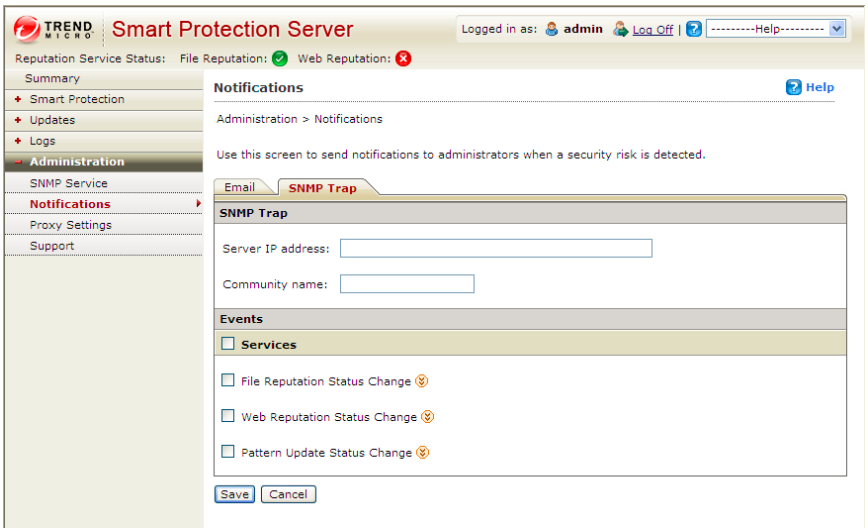
Configuring SNMP Trap Notifications

Configure Simple Network Management Protocol (SNMP) notification settings to notify administrators through SNMP trap when there is a status change in services.

Procedure

1. Go to **Administration** > **Notifications** and then go to the **SNMP** tab.

   The tab for SNMP trap notifications appears.



2. Select the **Services** check box or select from the following check boxes:

   - **File Reputation Status Change**: Select to send a notification for status changes and specify the recipient, subject, and message.
   - **Web Reputation Status Change**: Select to send a notification for status changes and specify the recipient, subject, and message.

- **Pattern Update Status Change**: Select to send a notification for status changes and specify the recipient, subject, and message.

3. Type the SNMP trap server IP address.

4. Type the SNMP community name.

5. Click **Save**.

Chapter 4

Trend Micro Apex Central™ / Control Manager™ Integration

Smart Protection Server integrates with Apex Central / Control Manager.

Topics include:

About Apex Central / Control Manager

Trend Micro Apex Central™ / Control Manager™ is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. The Apex Central / Control Manager web-based management console provides a single monitoring point for managed products and services throughout the network.

Apex Central / Control Manager allows system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy components throughout the network, helping ensure that protection is consistent and up-to-date. Apex Central / Control Manager allows both manual and pre-scheduled updates, and the configuration and administration of products as groups or as individuals for added flexibility.

Supported Apex Central / Control Manager Versions

This Smart Protection Server version supports the following Apex Central / Control Manager versions.

Features	Apex Central Version	Control Manager Version		
	2019	7.0	6.0 SP3	6.0 SP2 or Earlier
Synchronize suspicious objects and actions	Yes	Yes	Yes	No

Features	Apex Central Version	Control Manager Version		
	2019	7.0	6.0 SP3	6.0 SP2 or Earlier
Use Apex Central / Control Manager as an alternative update source	Yes	Yes	Yes	Yes

Note

Smart Protection Server only connects to Apex Central / Control Manager pure IPv4 or dual-stack networks.

Apex Central / Control Manager Integration in Smart Protection Server

This Smart Protection Server release supports the following Apex Central / Control Manager features:

TABLE 4-1. Integration with Apex Central / Control Manager

FEATURE	DESCRIPTION
Synchronization of suspicious objects and actions	1. Apex Central / Control Manager consolidates suspicious objects and scan actions, and then relays this information to Smart Protection Server. 2. Smart Protection Server relays suspicious URLs and actions to Security Agents. For products that send Web Reputation queries (such as Portal Protect and Deep Security), Smart Protection Server relays suspicious URLs only. **Note** • For more information on how Apex Central manages suspicious objects, see the *Apex Central Administrator's Guide*. You can download a PDF version of the guide, or view the guide online, using the following link: http://docs.trendmicro.com/en-us/enterprise/apex-central.aspx • For more information on how Control Manager manages suspicious objects, see the *Connected Threat Defense Primer* for your version of Control Manager at the following link: http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx
Apex Central / Control Manager as an alternative update source	Apex Central / Control Manager can act as an update source if Smart Protection Server does not have an Internet connection.
Single sign-on (SSO) login	Apex Central / Control Manager allows you to single sign-on (SSO) to Smart Protection Server from the Apex Central / Control Manager console.

Chapter 5

Technical Support

Learn about the following topics:

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to http://esupport.trendmicro.com.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

Tip

To submit a support case online, visit the following URL:

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

A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia

provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

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

- Trend Micro product documentation:

  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

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

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

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

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

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

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

http://www.trendmicro.com/download/

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

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

Appendix A

Command Line Interface (CLI) Commands

This section describes the Command Line Interface (CLI) commands that you can use in the product to perform monitoring, debugging, troubleshooting, and configuration tasks. Log on to the CLI through the virtual machine with your admin account. CLI commands allow administrators to perform configuration tasks and to perform debug and troubleshooting functions. The CLI interface also provides additional commands to monitor critical resources and functions. To access the CLI interface, you will need to have the administrator account and password.

COMMAND	SYNTAX	DESCRIPTION
certificate regen self-sign	**certificate regen self-sign** <Issued_to> <Issued_by> <Validity>	Regenerate self-sign certificate. <Issued_to>: Common Name or CN of the recipient of the certificate <Issued_by>: Common Name or CN of the issuer of the certificate <Validity>: The number of days the certificate is valid for
certificate update CA	**certificate update CA**	Download the latest CA bundle

COMMAND	SYNTAX	DESCRIPTION
configure date	**configure date** <date> <time>	Configure date and save to CMOS date DATE_FIELD [DATE_FIELD] time TIME_FIELD [TIME_FIELD]
configure dns ipv4	**configure dns ipv4** <dns1> [dns2]	Configure IPv4 DNS settings dns1 IPv4_ADDR Primary DNS server dns2 IPv4_ADDR Secondary DNS server []
configure dns ipv6	**configure dns ipv6** <dns1> [dns2]	Configure IPv6 DNS settings dns1 IPv6_ADDR Primary DNS server dns2 IPv6_ADDR Secondary DNS server []
configure hostname	**configure hostname** <hostname>	Configure the hostname hostname HOSTNAME Hostname or FQDN
configure ipv4 dhcp	**configure ipv4 dhcp [vlan]**	Configure the default Ethernet interface to use DHCP vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure ipv4 static	**configure ipv4 static** <ip> <mask> <gateway> [vlan]	Configure the default Ethernet interface to use the static IPv4 configuration vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure ipv6 auto	**configure ipv6 auto** [vlan]	Configure the default Ethernet interface to use the automatic neighbor discovery IPv6 configuration vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]

COMMAND	SYNTAX	DESCRIPTION
configure ipv6 dhcp	**configure ipv6 dhcp** [vlan]	Configure the default Ethernet interface to use the dynamic IPv6 configuration (DHCPv6) vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure ipv6 static	**configure ipv6 static** <v6ip> <v6mask> <v6gate> [vlan]	Configure the default Ethernet interface to use the static IPv6 configuration vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure locale de_DE	**configure locale de_DE**	Configure system locale to German
configure locale en_US	**configure locale en_US**	Configure system locale to English
configure locale es_ES	**configure locale es_ES**	Configure system locale to Spanish
configure locale fr_FR	**configure locale fr_FR**	Configure system locale to French
configure locale it_IT	**configure locale it_IT**	Configure system locale to Italian
configure locale ja_JP	**configure locale ja_JP**	Configure system locale to Japanese
configure locale ko_KR	**configure locale ko_KR**	Configure system locale to Korean
configure locale ru_RU	**configure locale ru_RU**	Configure system locale to Russian
configure locale zh_CN	**configure locale zh_CN**	Configure system locale to Chinese (Simplified)
configure locale zh_TW	**configure locale zh_TW**	Configure system locale to Chinese (Traditional)

COMMAND	SYNTAX	DESCRIPTION
configure ntp	**configure ntp <ip or FQDN>**	Configure the NTP server
configure port	**configure port <frs_http_port> <frs_https_port> <wrs_http_port>> <wrs_https_port>**	To change the service ports of the File and Web Reputation Services.
configure password	**configure password** <user>	Configure account password user USER The user name for which you want to change the password. The user could be 'admin', 'root', or any user in the Smart Protection Server's Administrator group.
configure proxy-service	**configure proxy-service** <wis_url> <cfr_url> <grid_url> <mars_url>	Modify Trend Micro global protection service URLs. <wis_url>: Web Inspection Service URL <cfr_url>: Community File Reputation URL <grid_url>: Goodware Resource and Information Database URL <mars_url>: Mobile App Reputation Service URL
configure service	**configure service inter-face** <ifname>	Configure the default server settings
configure timezone Africa Cairo	**configure timezone Africa Cairo**	Configure timezone to Africa/Cairo location.
configure timezone Africa Harare	**configure timezone Africa Harare**	Configure timezone to Africa/Harare location.
configure timezone Africa Nairobi	**configure timezone Africa Nairobi**	Configure timezone to Africa/Nairobi location.

COMMAND	SYNTAX	DESCRIPTION
`configure timezone America Anchorage`	`configure timezone America Anchorage`	Configure timezone to America/Anchorage location.
`configure timezone America Bogota`	`configure timezone America Bogota`	Configure timezone to America/Bogota location.
`configure timezone America Buenos_Aires`	`configure timezone America Buenos_Aires`	Configure timezone to America/Buenos Aires. location.
`configure timezone America Caracas`	`configure timezone America Caracas`	Configure timezone to America/Caracas location.
`configure timezone America Chicago`	`configure timezone America Chicago`	Configure timezone to America/Chicago location.
`configure timezone America Chihuahua`	`configure timezone America Chihuahua`	Configure timezone to America/Chihuahua location.
`configure timezone America Denver`	`configure timezone America Denver`	Configure timezone to America/Denver location.
`configure timezone America Godthab`	`configure timezone America Godthab`	Configure timezone to America/Godthab. location
`configure timezone America Lima`	`configure timezone America Lima`	Configure timezone to America/Lima location.

COMMAND	SYNTAX	DESCRIPTION
`configure timezone America Los_Angeles`	`configure timezone America Los_Angeles`	Configure timezone to America/Los Angeles location.
`configure timezone America Mexico_City`	`configure timezone America Mexico_City`	Configure timezone to America/Mexico City location.
`configure timezone America New_York`	`configure timezone America New_York`	Configure timezone to America/New York location.
`configure timezone America Noronha`	`configure timezone America Noronha`	Configure timezone to America/Noronha location.
`configure timezone America Phoenix`	`configure timezone America Phoenix`	Configure timezone to America/Phoenix location.
`configure timezone America Santiago`	`configure timezone America Santiago`	Configure timezone to America/Santiago location.
`configure timezone America St_Johns`	`configure timezone America St_Johns`	Configure timezone to America/St Johns location.
`configure timezone America Tegucigalpa`	`configure timezone America Tegucigalpa`	Configure timezone to America/Tegucigalpa location.

COMMAND	SYNTAX	DESCRIPTION
configure timezone Asia Almaty	**configure timezone Asia Almaty**	Configure timezone to Asia/Almaty location.
configure timezone Asia Baghdad	**configure timezone Asia Baghdad**	Configure timezone to Asia/Baghdad location.
configure timezone Asia Baku	**configure timezone Asia Baku**	Configure timezone to Asia/Baku location.
configure timezone Asia Bangkok	**configure timezone Asia Bangkok**	Configure timezone to Asia/Bangkok location.
configure timezone Asia Calcutta	**configure timezone Asia Calcutta**	Configure timezone to Asia/Calcutta location.
configure timezone Asia Colombo	**configure timezone Asia Colombo**	Configure timezone to Asia/Colombo location.
configure timezone Asia Dhaka	**configure timezone Asia Dhaka**	Configure timezone to Asia/Dhaka location.
configure timezone Asia Hong_Kong	**configure timezone Asia Hong_Kong**	Configure timezone to Asia/Hong Kong location.
configure timezone Asia Irkutsk	**configure timezone Asia Irkutsk**	Configure timezone to Asia/Irkutsk location.
configure timezone Asia Jerusalem	**configure timezone Asia Jerusalem**	Configure timezone to Asia/Jerusalem location.

COMMAND	SYNTAX	DESCRIPTION
`configure timezone Asia Kabul`	`configure timezone Asia Kabul`	Configure timezone to Asia/Kabul location.
`configure timezone Asia Karachi`	`configure timezone Asia Karachi`	Configure timezone to Asia/Karachi location.
`configure timezone Asia Katmandu`	`configure timezone Asia Katmandu`	Configure timezone to Asia/Katmandu location.
`configure timezone Asia Krasnoyarsk`	`configure timezone Asia Krasnoyarsk`	Configure timezone to Asia/Krasnoyarsk location.
`configure timezone Asia Kuala_Lumpur`	`configure timezone Asia Kuala_Lumpur`	Configure timezone to Asia/Kuala Lumpur location.
`configure timezone Asia Kuwait`	`configure timezone Asia Kuwait`	Configure timezone to Asia/Kuwait location.
`configure timezone Asia Magadan`	`configure timezone Asia Magadan`	Configure timezone to Asia/Magadan location.
`configure timezone Asia Manila`	`configure timezone Asia Manila`	Configure timezone to Asia/Manila location.
`configure timezone Asia Muscat`	`configure timezone Asia Muscat`	Configure timezone to Asia/Muscat location.
`configure timezone Asia Rangoon`	`configure timezone Asia Rangoon`	Configure timezone to Asia/Rangoon location.

COMMAND	SYNTAX	DESCRIPTION
`configure timezone Asia Seoul`	`configure timezone Asia Seoul`	Configure timezone to Asia/Seoul location.
`configure timezone Asia Shanghai`	`configure timezone Asia Shanghai`	Configure timezone to Asia/Shanghai location.
`configure timezone Asia Singapore`	`configure timezone Asia Singapore`	Configure timezone to Asia/Singapore location.
`configure timezone Asia Taipei`	`configure timezone Asia Taipei`	Configure timezone to Asia/Taipei location.
`configure timezone Asia Tehran`	`configure timezone Asia Tehran`	Configure timezone to Asia/Tehran location.
`configure timezone Asia Tokyo`	`configure timezone Asia Tokyo`	Configure timezone to Asia/Tokyo location.
`configure timezone Asia Yakutsk`	`configure timezone Asia Yakutsk`	Configure timezone to Asia/Yakutsk location.
`configure timezone Atlantic Azores`	`configure timezone Atlantic Azores`	Configure timezone to Atlantic/Azores location.
`configure timezone Australia Adelaide`	`configure timezone Australia Adelaide`	Configure timezone to Australia/Adelaide location.

COMMAND	SYNTAX	DESCRIPTION
`configure timezone Australia Brisbane`	`configure timezone Australia Brisbane`	Configure timezone to Australia/Brisbane location.
`configure timezone Australia Darwin`	`configure timezone Australia Darwin`	Configure timezone to Australia/Darwin location.
`configure timezone Australia Hobart`	`configure timezone Australia Hobart`	Configure timezone to Australia/Hobart location.
`configure timezone Australia Melbourne`	`configure timezone Australia Melbourne`	Configure timezone to Australia/Melbourne location.
`configure timezone Australia Perth`	`configure timezone Australia Perth`	Configure timezone to Australia/Perth location.
`configure timezone Europe Amsterdam`	`configure timezone Europe Amsterdam`	Configure timezone to Europe/Amsterdam location.
`configure timezone Europe Athens`	`configure timezone Europe Athens`	Configure timezone to Europe/Athens location.
`configure timezone Europe Belgrade`	`configure timezone Europe Belgrade`	Configure timezone to Europe/Belgrade location.

COMMAND	SYNTAX	DESCRIPTION
`configure timezone Europe Berlin`	`configure timezone Europe Berlin`	Configure timezone to Europe/Berlin location.
`configure timezone Europe Brussels`	`configure timezone Europe Brussels`	Configure timezone to Europe/Brussels location.
`configure timezone Europe Bucharest`	`configure timezone Europe Bucharest`	Configure timezone to Europe/Bucharest location.
`configure timezone Europe Dublin`	`configure timezone Europe Dublin`	Configure timezone to Europe/Dublin location.
`configure timezone Europe Moscow`	`configure timezone Europe Moscow`	Configure timezone to Europe/Moscow location.
`configure timezone Europe Paris`	`configure timezone Europe Paris`	Configure timezone to Europe/Paris location.
`configure timezone Pacific Auckland`	`configure timezone Pacific Auckland`	Configure timezone to Pacific/Auckland location.
`configure timezone Pacific Fiji`	`configure timezone Pacific Fiji`	Configure timezone to Pacific/Fiji location.
`configure timezone Pacific Guam`	`configure timezone Pacific Guam`	Configure timezone to Pacific/Guam location.

COMMAND	SYNTAX	DESCRIPTION
`configure timezone Pacific Honolulu`	`configure timezone Pacific Honolulu`	Configure timezone to Pacific/Honolulu location.
`configure timezone Pacific Kwajalein`	`configure timezone Pacific Kwajalein`	Configure timezone to Pacific/Kwajalein location.
`configure timezone Pacific Midway`	`configure timezone Pacific Midway`	Configure timezone to Pacific/Midway location.
`configure timezone US Alaska`	`configure timezone US Alaska`	Configure timezone to US/Alaska location.
`configure timezone US Arizona`	`configure timezone US Arizona`	Configure timezone to US/Arizona location.
`configure timezone US Central`	`configure timezone US Central`	Configure timezone to US/Central location.
`configure timezone US East-Indiana`	`configure timezone US East-Indiana`	Configure timezone to US/East-Indiana location.
`configure timezone US Eastern`	`configure timezone US Eastern`	Configure timezone to US/Eastern location.
`configure timezone US Hawaii`	`configure timezone US Hawaii`	Configure timezone to US/Hawaii location.
`configure timezone US Mountain`	`configure timezone US Mountain`	Configure timezone to US/Mountain location.

COMMAND	SYNTAX	DESCRIPTION
configure timezone US Pacific	**configure timezone US Pacific**	Configure timezone to US/Pacific location.
disable adhoc-query	**disable adhoc-query**	Disable Web Access Log
disable ssh	**disable ssh**	Disable the sshd daemon
enable	**enable**	Enable administrative commands
enable adhoc-query	**enable adhoc-query**	Enable Web Access Log
enable ssh	**enable ssh**	Enable the sshd daemon
exit	**exit**	Exit the session
help	**help**	Display an overview of the CLI syntax.
history	**history** [limit]	Display the current session's command line history [limit] specifies the number of CLI commands to display. Example: Specifying a [limit] of “5” means 5 CLI commands display.
reboot	**reboot** [time]	Reboot this machine after a specified delay or immediately [time] UNIT Time in minutes to reboot this machine [0]
show date	**show date**	Display current date/time
show hostname	**show hostname**	Display network hostname
show interfaces	**show interfaces**	Display network interface information
show ipv4 address	**show ipv4 address**	Display network IPv4 address

COMMAND	SYNTAX	DESCRIPTION
`show ipv4 dns`	`show ipv4 dns`	Display network IPv4 DNS servers
`show ipv4 gateway`	`show ipv4 gateway`	Display network IPv4 gateway
`show ipv4 route`	`show ipv4 route`	Display network IPv4 routing table
`show ipv4 type`	`show ipv4 type`	Display network IPv4 configuration type (dhcp / static)
`show ipv6 address`	`show ipv6 address`	Display network IPv6 address
`show ipv6 dns`	`show ipv6 dns`	Display network IPv6 DNS servers
`show ipv6 gateway`	`show ipv6 gateway`	Display network IPv6 gateway
`show ipv6 route`	`show ipv6 route`	Display network IPv6 routing table
`show ipv6 type`	`show ipv6 type`	Display network IPv6 configuration type (auto / dhcp / static)
`show timezone`	`show timezone`	Display network timezone
`show uptime`	`show uptime`	Display current system uptime
`show url management`	`show url management`	Display web management console URL
`show url FileReputationService`	`show url FileReputationService`	Display endpoint connection addresses for File Reputation Services
`show url WebReputationService`	`show url WebReputationService`	Display endpoint connection addresses for Web Reputation Services

COMMAND	SYNTAX	DESCRIPTION
shutdown	**shutdown** [time]	Shut down this machine after a specified delay or immediately time UNIT Time in minutes to shutdown this machine [0]

Index

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM38673/190603