TREND MICRO™

3.0 TREND MICRO™ Smart Protection Server

Administrator's Guide

Security Made Smarter

Endpoint Security

Messaging Security

Protected Cloud

Web Security

TREND MICRO SMART PROTECTION NETWORK™

Trend Micro Incorporated reserves the right to make changes to this document and to the product/service described herein without notice. Before installing and using the product/service, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://downloadcenter.trendmicro.com/

Document Part No.: APEM36294/140116

Release Date: March 2014

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

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

Detailed information about how to use specific features within the product/service 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

Table of Contents

Preface

Chapter 1: Introduction

Chapter 2: Using Smart Protection Server

Chapter 3: Monitoring Smart Protection Server

Chapter 4: Getting Help

Appendix A: Command Line Interface (CLI) Commands

Appendix B: Glossary

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 Incorporated 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 Trend Micro Smart Protection Server Work? on page 1-2*
- *New in this Release on page 1-7*
- *Key Features and Benefits on page 1-10*
- *Trend Micro Smart Protection Network on page 1-11*

How Does Trend Micro Smart Protection Server Work?

Trend Micro™ 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 Trend Micro 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 Servers 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 Servers as part of their regular system protection activities. In this solution, agents send identification information, determined by Trend Micro technology, to Smart Protection Servers 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

The cloud-based query process makes use of a small local 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 Servers use several algorithms for an efficient process that uses minimal network bandwidth usage.

There are three pattern files:

- **Smart Scan Pattern**: This pattern is downloaded to and available on Smart Protection Servers and Trend Micro Smart Protection Network. This file is updated hourly.
- **Smart Scan Agent Pattern**: This pattern is stored locally on the endpoint for scans that do not require Smart Protection Servers. This file is updated daily.
- **Web Blocking List**: Smart Protection Servers download this pattern from Trend Micro ActiveUpdate servers. This pattern is used for Web Reputation queries.

Pattern Update Process

Pattern updates are a response to security threats. Smart Protection Network and Smart Protection Servers download the Smart Scan Pattern file from ActiveUpdate servers. Trend Micro products that support Smart Protection Servers 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 Servers. External endpoints are endpoints that are outside of the intranet and unable to connect to Smart Protection Servers or Trend Micro products that support Smart Protection Servers.

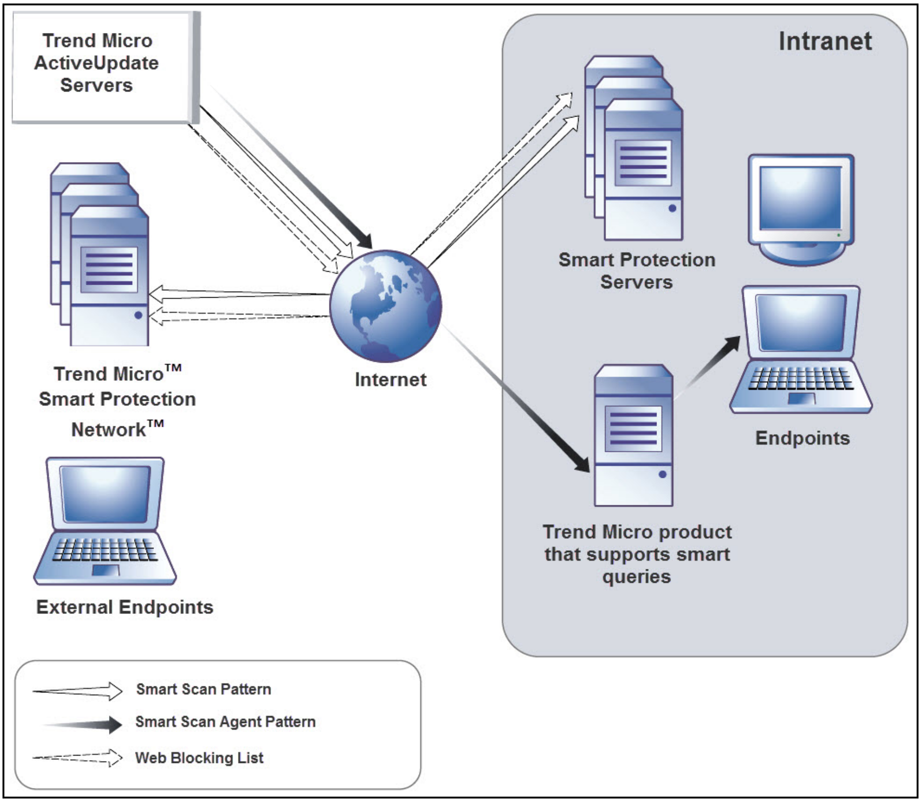


FIGURE 1-1. Pattern update process

The Query Process

Endpoints that are currently in your intranet use Smart Protection Servers 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 Servers, 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 1-1. 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 Servers. • **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 Servers 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 Servers more than once.

An agent that cannot verify a file's risk locally and cannot connect to any Smart Protection Servers 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 Servers to ensure the continuity of protection in the event that connection to a Smart Protection Server is unavailable.

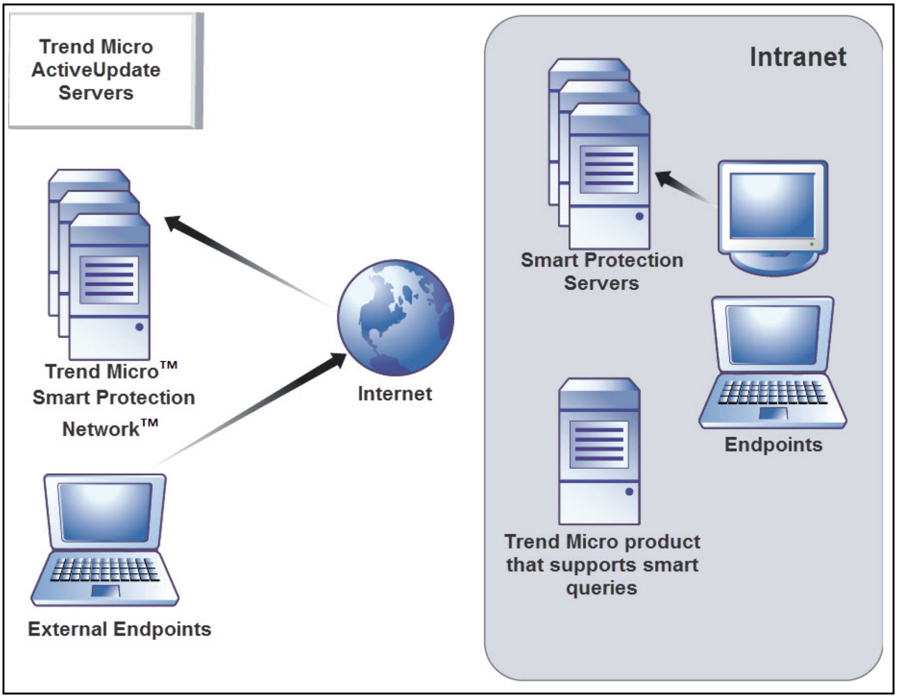

Trend Micro ActiveUpdate Servers
Trend Micro™ Smart Protection Network™
Internet
External Endpoints
Intranet
Smart Protection Servers
Endpoints
Trend Micro product that supports smart queries

Figure 1-2. Query process

New in this Release

Trend Micro™ Smart Protection Server™ includes the following new features and enhancements:

TABLE 1-2. New for Version 3.0

FEATURE	DESCRIPTION
Enhanced pattern performance	Improved the performance of File and Web Reputation Services to reduce the memory resource usage when loading patterns. • Web Reputation Services Enhanced Web Reputation Services by allowing incremental updates for the Web Blocking List. This reduces the memory and network bandwidth usage when loading the Web Blocking List. • File Reputation Services Enhanced the File Reputation Services log import mechanism to update the database directly from the web server. This ensures the following: • Importing access logs into the database is now in real-time and there will be less processing times for the same amount of data and improves disk I/O performance. • Reduction in the server load and resource usage.
Enhanced capacity	A standalone Smart Protection Server can now support up to 25,000 Trend Micro™ OfficeScan™ 11 agents.
Dashboard Enhancement	• Provides new layouts and tables for widgets. • Widgets now get the data from the web server on a daily basis. • Fixed time out issues and some minor bugs.

Feature	Description
New management information base (MIB) for system information	Provided the capability to query Smart Protection Server system information directly from a third-party MIB browser tool. These are: • SNMP MIB-2 System (1.3.6.1.2.1.1) • SNMP MIB-2 Interfaces (1.3.6.1.2.1.2) For more information, refer to *Supported MIB on page 2-19*.
New Command Line Interface (CLI) Commands	Provided new commands for the following: • Setting up an NTP server (`configure ntp`) • Changing the service port (`configure port`) **Important** Use this command only if there is a conflict with the current service port. For more information, refer to *Command Line Interface (CLI) Commands on page A-1*.
Enhanced virtual machine capabilities	• Smart Protection Server now supports VMware VMXNET 3 network adapter in an IPv6 environment. • Fixed the IPv6 Microsoft Hyper-V network adapter issue with Linux Kernel version 5.8.

TABLE 1-3. New for Version 2.6 Patch 1

FEATURE	DESCRIPTION
Deep Discovery Advisor integration and the Virtual Analyzer list	Smart Protection Servers can integrate with Deep Discovery Advisor to obtain the Virtual Analyzer C&C server list. The Deep Discovery Advisor Virtual Analyzer evaluates potential risks in a secure environment and, through use of advanced heuristics and behavioral testing methods, assigns a risk level to the analyzed threats. The Virtual Analyzer populates the Virtual Analyzer list with any threat that attempts to connect to a possible C&C server. The Virtual Analyzer list is highly company-specific and provides a more customized defense against targeted attacks. Smart Protection Servers retrieve the list from Deep Discovery Advisor and can evaluate all possible C&C threats against both the Global Intelligence and the local Virtual Analyzer list.

TABLE 1-4. New for Version 2.6

FEATURE	DESCRIPTION
Dashboard Enhancement	The dashboard can now be displayed on devices that do not support Adobe™ Flash™ Player.
Fixed some minor issues	Trend Micro fixed some minor issues.

Key Features and Benefits

Trend Micro 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

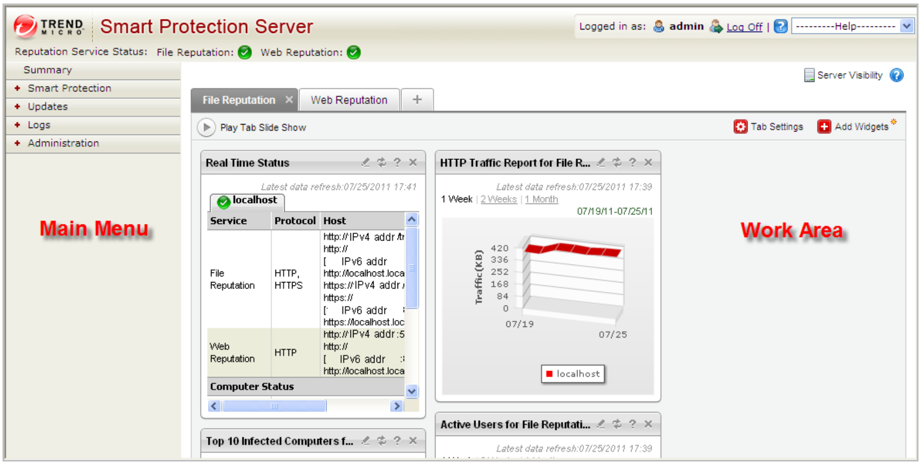
This chapter provides Trend Micro™ Smart Protection Server™ configuration information.

Topics include:

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 Servers, traffic, and detections when you add widgets.
Smart Protection	Provides options for configuring reputation services, an approved/ block URL list, 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.

Menu	Description
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 Servers.

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

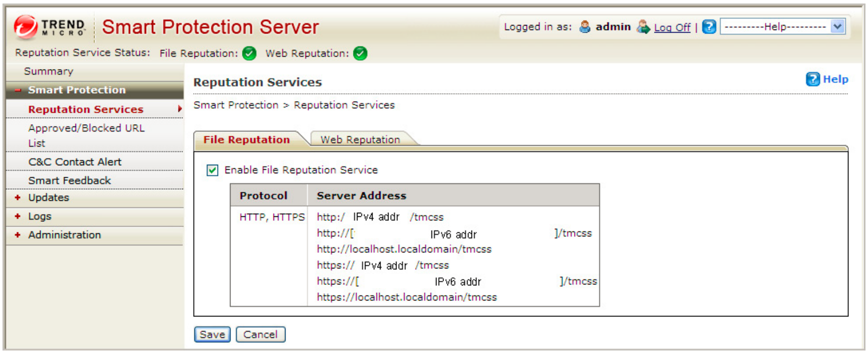
Enable Reputation Services from the product console to allow other Trend Micro products to use smart protection.

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.



☑ Enable File Reputation Service

Protocol	Server Address
HTTP, HTTPS	http:/ IPv4 addr /tmcss http://[IPv6 addr]/tmcss http://localhost.localdomain/tmcss https:// IPv4 addr /tmcss https://[IPv6 addr]/tmcss https://localhost.localdomain/tmcss

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 Servers.

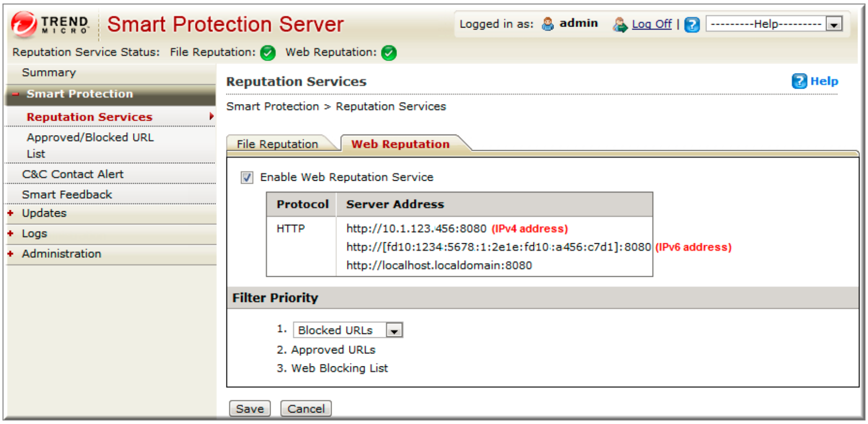
Enabling Web Reputation Services

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 go to the **Web Reputation** tab.



☑ Enable Web Reputation Service

Protocol	Server Address
HTTP	http://10.1.123.456:8080 (IPv4 address) http://[fd10:1234:5678:1:2e1e:fd10:a456:c7d1]:8080 (IPv6 address) http://localhost.localdomain:8080

Filter Priority

1. Blocked URLs
2. Approved URLs
3. Web Blocking List

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

3. (Optional) Specify the priority of the Approved/Blocked URL List when filtering URLs.

4. Click **Save**.

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

Configuring the Approved and Blocked URL Lists

The Approved/Blocked URL List allows you to specify a custom list of approved and/or blocked URLs. This list is used for Web Reputation. These are the options available on this screen.

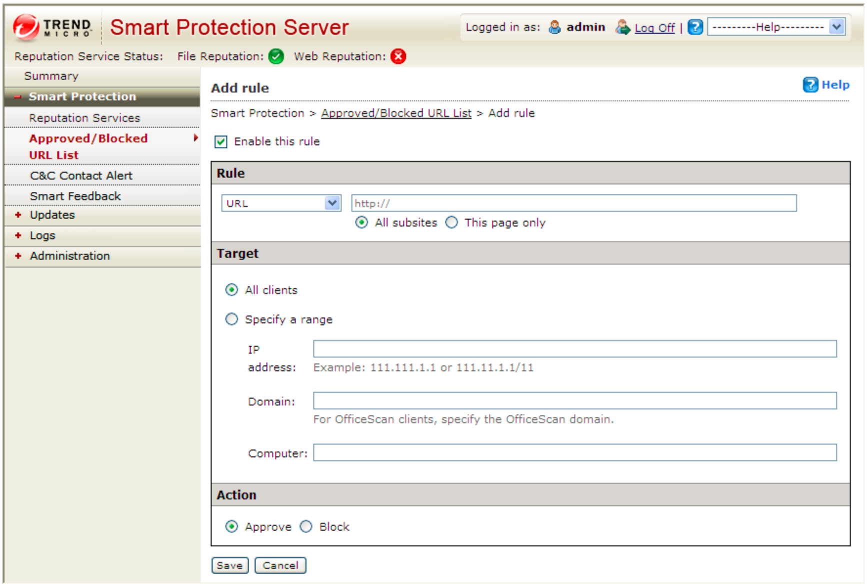
- **Search Rule**: Select to search for a string in the list of rules.
- **Test URL**: Select to search for the rules that the URL will trigger. The URL must start with `http://` or `https://`.

Procedure

1. Go to **Smart Protection** > **Approved/Blocked URL List**.

2. Click **Add**.

   The **Add rule** screen displays.



TREND MICRO Smart Protection Server

Logged in as: admin Log Off | ? ---------Help---------

Reputation Service Status: File Reputation: ✓ Web Reputation: ✗

- Summary
- − Smart Protection
  - Reputation Services
  - Approved/Blocked URL List
  - C&C Contact Alert
  - Smart Feedback
- + Updates
- + Logs
- + Administration

Add rule ? Help

Smart Protection > Approved/Blocked URL List > Add rule

☑ Enable this rule

Rule

URL ▾ http://

● All subsites ○ This page only

Target

● All clients

○ Specify a range

IP address: Example: 111.111.1.1 or 111.11.1.1/11

Domain: For OfficeScan clients, specify the OfficeScan domain.

Computer:

Action

● Approve ○ Block

Save Cancel

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 endpoints**: to apply to all endpoints.
- **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**.

Configuring C&C Contact Alert Services

Trend Micro Command & Control (C&C) Contact Alert Services provides enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks. C&C Contact Alert Services are integrated with Web Reputation Services which determines the action taken on detected callback addresses based on the web reputation security level.

These are the options available on this screen.

- **Server**: The server name or IP address of the Deep Discovery Advisor server, which provides the Virtual Analyzer C&C list.
- **API key**: The API key of the Deep Discovery Advisor. The API key can be found in the **About** page of the Deep Discovery Advisor web console.
- **Test connection**: Use this button to verify that the server name or IP address and API key of the Deep Discovery Advisor is correct.
- **Register**: Use this button to register Smart Protection Server to Deep Discovery Advisor.
- **Unregister**: Use this button to unregister Smart Protection Server from Deep Discovery Advisor.
- **Enable Virtual Analyzer C&C list**: Enable this option to allow Smart Protection Server to use the custom C&C list analyzed by the Deep Discovery Advisor server.

- **Sync Now**: Use this button to get an updated Virtual Analyzer C&C list from Deep Discovery Advisor.

Procedure

1. Type the server name or IP address of the Deep Discovery Advisor server.

   Note

   The server name supports FQDN formats and the IP address supports IPv4 format.

2. Type the API key.

3. Click **Register** to connect to the Deep Discovery Advisor server.

   Note

   Administrators can test the connection to the server before registering to the server.

4. Select **Enable Virtual Analyzer C&C list** to allow supported servers to use the custom C&C list analyzed by the local Deep Discovery Advisor server.

   Note

   The **Enable Virtual Analyzer C&C list** option is only available after establishing a successful connection to the Deep Discovery Advisor server.

5. 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.

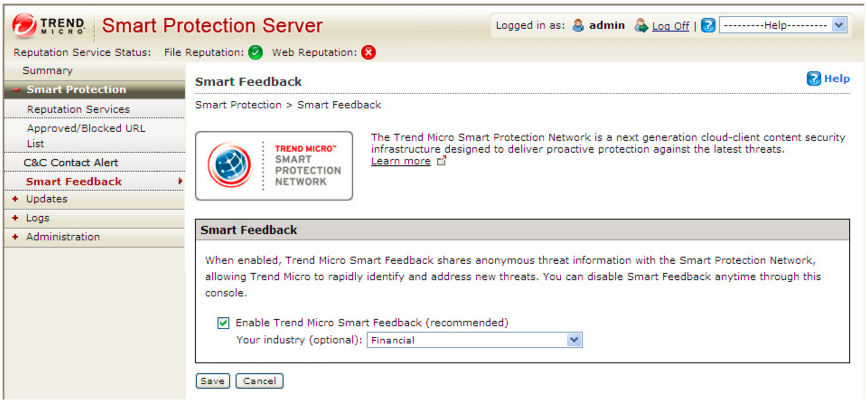
Procedure

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**.



The Trend Micro Smart Protection Network is a next generation cloud-client content security infrastructure designed to deliver proactive protection against the latest threats.

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

☑ Enable Trend Micro Smart Feedback (recommended)

Your industry (optional): Financial

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

You can perform manual updates for the Smart Scan Pattern and Web Blocking List.

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

Smart Protection Server can perform scheduled updates for the Smart Scan Pattern and Web Blocking List.

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.

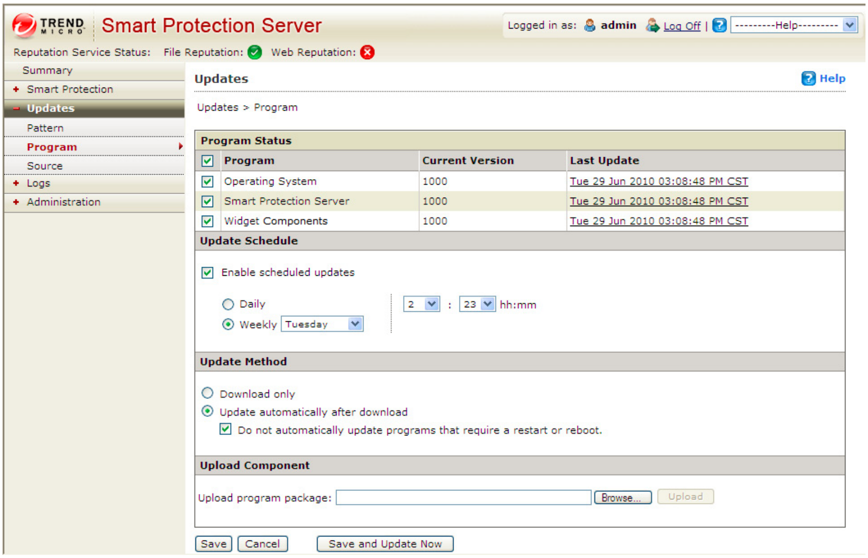
- **Operating System**: Select to update operating system components.
- **Smart Protection Server**: Select to update the product server program file.
- **Widget Components**: Select to update widgets.
- **Enable scheduled updates**: Select to update program files daily at a specified time or weekly.
- **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.



Reputation Service Status: File Reputation: ✓ Web Reputation: ✗

Updates

Updates > Program

Program Status

☑ Program	Current Version	Last Update
☑ Operating System	1000	Tue 29 Jun 2010 03:08:48 PM CST
☑ Smart Protection Server	1000	Tue 29 Jun 2010 03:08:48 PM CST
☑ Widget Components	1000	Tue 29 Jun 2010 03:08:48 PM CST

Update Schedule

☑ Enable scheduled updates

○ Daily
● Weekly Tuesday

2 : 23 hh:mm

Update Method

○ Download only
● Update automatically after download
☑ Do not automatically update programs that require a restart or reboot.

Upload Component

Upload program package:

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.

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 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.

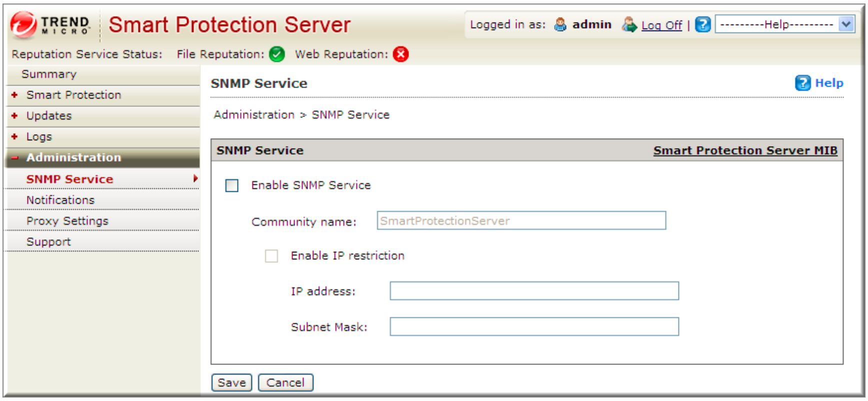
- **IP address**: Specify an IP address for using the SNMP service to monitor Health Status.
- **Subnet Mask**: Specify a netmask to define the IP address range for using the SNMP service to monitor computer status.
- **Smart Protection Server MIB**: Click to download the Smart Protection Server MIB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



□ Enable SNMP Service

Community name: SmartProtectionServer

□ Enable IP restriction

IP address:

Subnet Mask:

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.

Object Name	Object Identifier (OID)	Description
Trend-MIB:: WCSVersion	1.3.6.1.4.1.6101.1.2.1.5	Returns the current Web Blocking List 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 List update.
Trend-MIB:: WCSLastUpdateError	1.3.6.1.4.1.6101.1.2.1.7	Returns the status of the last Web Blocking List 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 List update was unsuccessful.
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.

Object Name	Object Identifier (OID)	Description
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.
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

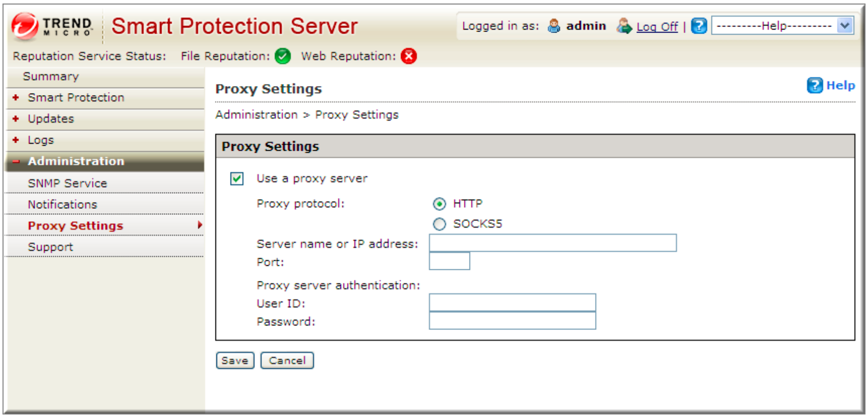
If you use a proxy server in the network, configure proxy settings. These are the options available on this screen.

- **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**.



Proxy Settings

Administration > Proxy Settings

Proxy Settings

☑ Use a proxy server

Proxy protocol: ● HTTP ○ SOCKS5

Server name or IP address:

Port:

Proxy server authentication:

User ID:

Password:

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.

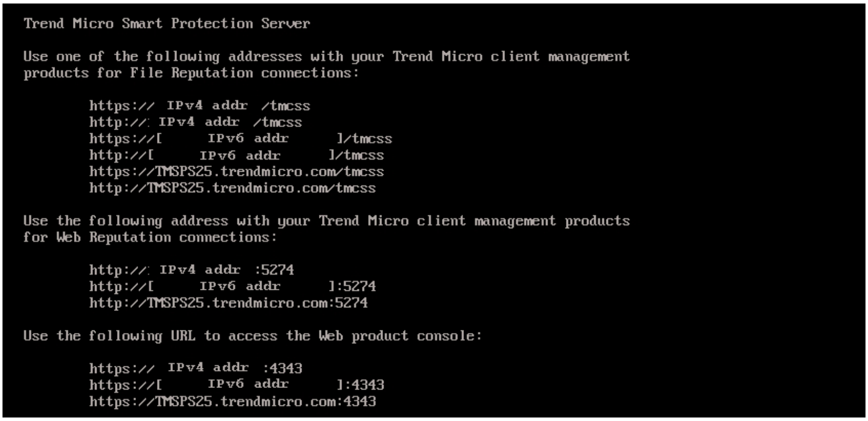
Tip

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.



```
Trend Micro Smart Protection Server

Use one of the following addresses with your Trend Micro client management
products for File Reputation connections:

        https:// IPv4 addr  /tmcss
        http:// IPv4 addr  /tmcss
        https://[      IPv6 addr      ]/tmcss
        http://[      IPv6 addr      ]/tmcss
        https://TMSPS25.trendmicro.com/tmcss
        http://TMSPS25.trendmicro.com/tmcss

Use the following address with your Trend Micro client management products
for Web Reputation connections:

        http:// IPv4 addr  :5274
        http://[      IPv6 addr      ]:5274
        http://TMSPS25.trendmicro.com:5274

Use the following URL to access the Web product console:

        https:// IPv4 addr  :4343
        https://[      IPv6 addr      ]:4343
        https://TMSPS25.trendmicro.com:4343
```

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.

Chapter 3

Monitoring Smart Protection Server™

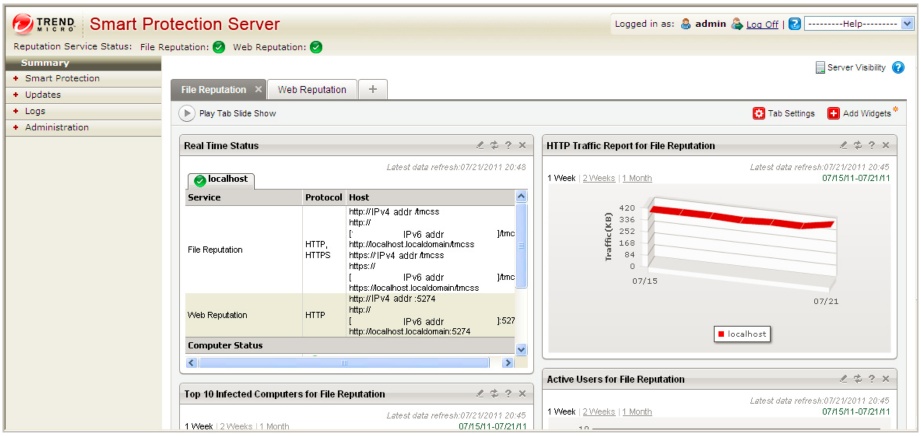
Monitor Trend Micro™ Smart Protection Server™ with logs and from the Summary screen with widgets.

Topics include:

Using the Summary Screen

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

Smart Protection Server supports both HTTP and HTTPS protocols for File Reputation Service connections and HTTP protocol for Web Reputation Service connections. 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.



Real Time Status

Latest data refresh:07/21/2011 20:48

localhost

Service	Protocol	Host
File Reputation	HTTP, HTTPS	http://IPv4 addr /tmcss http:// [IPv6 addr]/tmc http://localhost.localdomain/tmcss https://IPv4 addr /tmcss https:// [IPv6 addr]/tmc https://localhost.localdomain/tmcss
Web Reputation	HTTP	http://IPv4 addr :5274 http:// [IPv6 addr]:527 http://localhost.localdomain:5274
Computer Status		

The **Summary** screen consists of the following user interface elements:

- **Server Visibility**: Click 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 Servers.

- Tabs provide a container for widgets. For details, see *Tabs on page 3-3*.

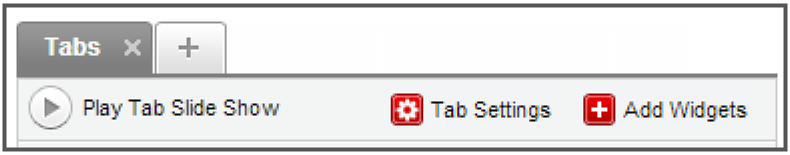
- Widgets are the core components of the dashboard. For details, see *Widgets on page 3-5*.

Tabs

Tabs provide a container for widgets. Each tab on the **Summary** screen can hold up to 20 widgets. The **Summary** screen itself supports up to 30 tabs.

Tab Tasks

The following table lists all the tab-related tasks:

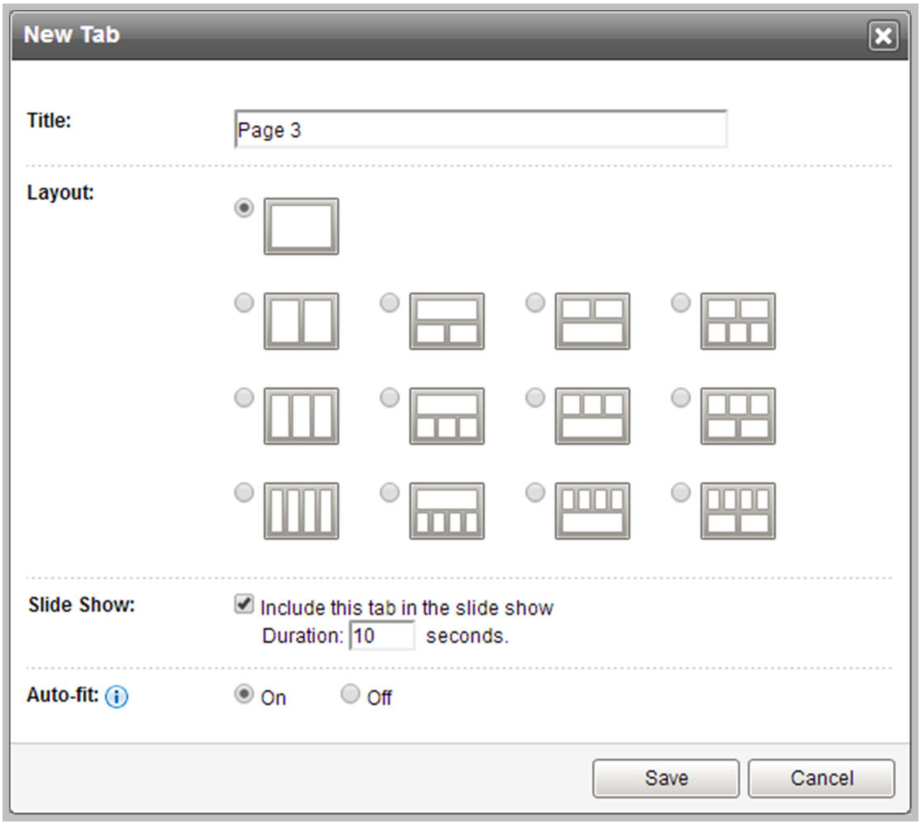


Task	Steps
Add a tab	Click the plus icon (+) on top of the **Summary** screen. The **New Tab** window displays. For details about this window, see *New Tab Window on page 3-4*.
Edit tab settings	Click **Tab Settings**. A window similar to the **New Tab** window opens, where you can edit settings.
Play Tab Slide Show	Click **Play Tab Slide Show**. The information in the selected tabs will change similar to a slide show.
Move tab	Use drag-and-drop to change a tab’s position.
Delete tab	Click the delete icon (✕) next to the tab title. Deleting a tab also deletes all the widgets in the tab.

New Tab Window

The **New Tab** window opens when you add a new tab in the **Summary** screen.

This window includes the following options:



New Tab

Title: Page 3

Layout: ● (single-panel layout selected)

Slide Show: ☑ Include this tab in the slide show
Duration: 10 seconds.

Auto-fit: ● On ○ Off

Option	Steps
Title	Type the name of the tab.
Layout	Choose from the available layouts.

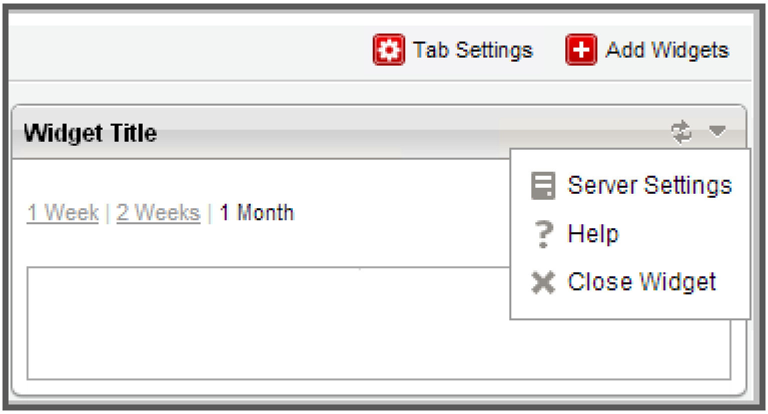
Option	Steps
Slide Show	The information in the selected tabs will change similar to a slide show. If you enable this option, you can select which tabs you want to appear in your slide show, and you can also control the speed at which your slide show plays.
Auto-fit	Auto-fit adjusts a widget to fit the size of a box.

Widgets

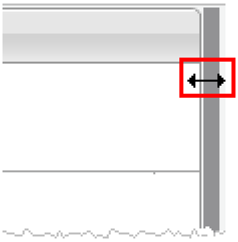
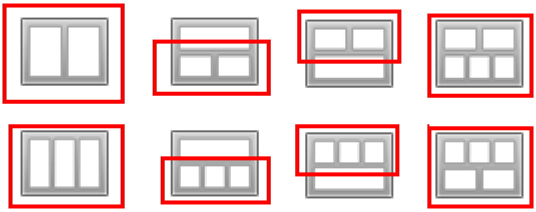
Widgets allow you to customize the information displayed on the **Summary** screen. New widgets can be added to the web console. Widgets can be dragged and dropped to customize the order in which they display. Available widget packages can be downloaded and updated by using the Program Update screen. After updating the widget package, the new widget can be added from the **Summary** screen.

Widget Tasks

The following table lists widget-related tasks:



TASK	STEPS
Add a widget	Open a tab and then click **Add Widgets** at the top right corner of the tab. The **Add Widgets** screen displays.
Refresh widget data	Click the refresh icon (⟳).
Configure server settings	Click the triangle icon (▼) and then click **Server Settings** (▤) to include/exclude the widget from getting information from the server. You can also click **Check Server Visibility** to add servers from the Server Visibility list or configure proxy server settings to establish connection with the servers in the Server Visibility list.
View help	Click the triangle icon (▼) and then click **Help** (?).
Delete a widget	Click the triangle icon (▼) and then click **Close Widget** (✖). This action removes the widget from the tab that contains it, but not from the other tabs that contain it or from the widget list in the **Add Widgets** screen.
Move a widget	Use drag-and-drop to move a widget to a different location within the tab.

Task	Steps
Resize a widget	To resize a widget, point the cursor to the right edge of the widget. When you see a thick vertical line and an arrow (as shown in the following image), hold and then move the cursor to the left or right.  Only widgets on multi-column tabs can be resized. These tabs have any of the following layouts and the highlighted sections contain widgets that can be resized. 

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 supports both HTTP and HTTPS protocols. Web reputation supports HTTP. 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 Servers. The addresses are used for configuring connections to Smart Protection Servers.
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 Servers.
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 and the data is displayed in a 3-D graph. You can also click the refresh icon (⟳) at any time to update the data.

Note

On the 3-D graph, right-clicking the graph provides options to reset the graph or display the graph in 2D, 3D, 100%, and best fit. You can also click the server name to display the values for each day on the graph.

TABLE 3-3. Widget Data

DATA	DESCRIPTION
Traffic (KB)	The network traffic generated by queries.

Data	Description
Date	The date of the queries.

Top 10 Blocked 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 Servers in the list.

Table 3-4. Widget Data

Data	Description
IP	The IP address of the computer.
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 Servers.
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 and the data is displayed in a 3-D graph. You can also click the refresh icon (⟳) at any time to update the data.

Note

On the 3-D graph, right-clicking the graph provides options to reset the graph or display the graph in 2D, 3D, 100%, and best fit. You can also click the server name to display the values for each day on the graph.

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 Servers 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 Web Access Log

The Blocked Web Access Log screen displays information for Web Reputation queries that return malicious results. These are the options available on this screen.

- **Keyword**: Specify keywords to use when searching for URLs.
- **Date Range**: Select a date range.
- **Display Log**: Use the following to filter your log query:
  - **All**: Displays logs of all blocked sites.

  - **Blocked**: Displays logs of sites that were blocked because the sites matched an entry on the user-defined, blocked URL list.
  - **Virtual Analyzer C&C**: Displays logs of sites that were blocked because the sites matched a URL or IP address on the Virtual Analyzer C&C list.
  - **Web blocking**: Displays logs of sites that were blocked because the sites matched an URL or IP address on the Web blocking list and Global Intelligence C&C list.
- **C&C List Source**: Displays logs of sites that were blocked because it is in the Global Intelligence or Virtual Analyzer list.

Log Details:

- **Date and time**: The date and time of the blocked URL event.
- **URL**: The URL that was blocked by Web Reputation.
- **Filter**: The list that triggered blocking the URL or IP address. This could be the user-defined blocked URL list, Virtual Analyzer C&C list, or the Trend Micro Web Blocking List.
- **C&C List Source**: This can either be the Global Intelligence list or the Virtual Analyzer list.
- **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 Servers.
- **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.
- **User**: The endpoint user name.
- **Domain**: The domain name of the endpoint.
- **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 Web Access Log**: 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.

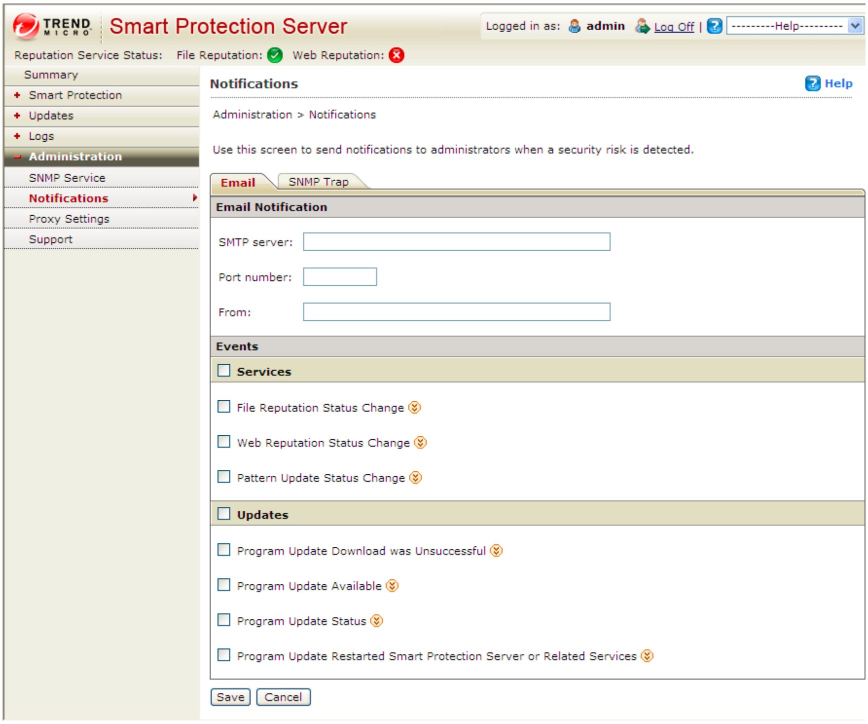
- **Program Update Download was Unsuccessful**: Select to send a notification if the program update did not download successfully and specify the recipient for this notification.
- **Program Update Available**: Select to send a notification if a program update is available that requires confirmation 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.



Notifications

Use this screen to send notifications to administrators when a security risk is detected.

Email Notification

SMTP server:

Port number:

From:

Events

□ Services

□ File Reputation Status Change

□ Web Reputation Status Change

□ Pattern Update Status Change

□ Updates

□ Program Update Download was Unsuccessful

□ Program Update Available

□ Program Update Status

□ Program Update Restarted Smart Protection Server or Related Services

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.

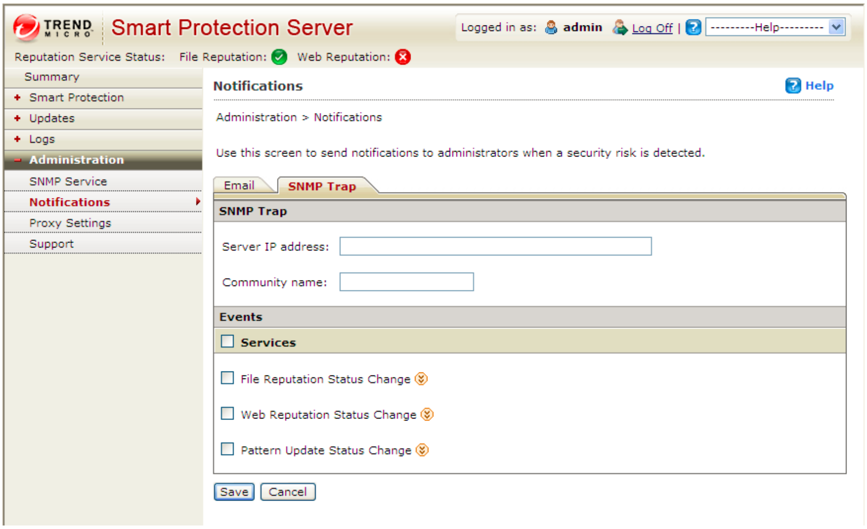
Configuring SNMP Trap Notifications

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.



Smart Protection Server

Logged in as: admin Log Off | ---------Help---------

Reputation Service Status: File Reputation: ✓ Web Reputation: ✗

Summary
+ Smart Protection
+ Updates
+ Logs
− Administration
SNMP Service
Notifications
Proxy Settings
Support

Notifications

Help

Administration > Notifications

Use this screen to send notifications to administrators when a security risk is detected.

Email | SNMP Trap

SNMP Trap

Server IP address:

Community name:

Events

□ Services

□ File Reputation Status Change

□ Web Reputation Status Change

□ Pattern Update Status Change

Save | Cancel

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

Getting Help

This chapter includes details on how to get additional help while working with Trend Micro™ Smart Protection Server™ .

Topics include:

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 a product or service from the appropriate drop-down list and specify any other related information.

   The **Technical Support** product page appears.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

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

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

Known Issues

Known issues document unexpected product behavior that might require a temporary work around. Trend Micro recommends always checking the readme file for information about system requirements and known issues that could affect installation or performance. Readme files also contain a description of what's new in a particular release, and other helpful information.

The latest known issues and possible workarounds can also be found in the Trend Micro Knowledge Base:

http://esupport.trendmicro.com

Hot Fixes, Patches, and Service Packs

After an official product release, Trend Micro often develops hot fixes, patches and service packs to address outstanding issues, enhance product performance, and add new features.

The following is a summary of the items Trend Micro may release:

- **Hot Fix**: a work-around or solution to customer-reported issues. Trend Micro develops and releases hot fixes to specific customers only.
- **Security Patch**: a single hot fix or group of hot fixes suitable for deployment to all customers
- **Patch**: a group of security patches suitable for deployment to all customers
- **Service Pack**: significant feature enhancements that upgrade the product

Your vendor or support provider may contact you when these items become available. Check the Trend Micro website for information on new hot fix, patch, and service pack releases:

http://downloadcenter.trendmicro.com/

All releases include a readme file that contains installation, deployment, and configuration information. Read the readme file carefully before performing installation.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined 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://www.trendmicro.com/vinfo 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, fax, or email:

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
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 hardware connected to the endpoint
- Amount of memory and free hard disk space

- Operating system and service pack version
- Endpoint client version
- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received.
- Virtualization platform (VMware™ or Hyper-V™) and version

TrendLabs

TrendLabs℠ is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

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

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
`configure date`	**`configure date`** `<date> <time>`	Configure date and save to CMOS *`date`* DATE_FIELD [DATE_FIELD] *`time`* TIME_FIELD [TIME_FIELD]

Command	Syntax	Description
`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 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

Command	Syntax	Description
`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)
`configure ntp`	`configure ntp <ip or FQDN>`	Configure the NTP server
`configure port`	`configure port <frs_http_port> <frs_https_port> <wrs_http_port>`	To change the service ports of the File and Web Reputation Services.
`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 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 service`	`configure service interface <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.
`configure timezone America Anchorage`	`configure timezone America Anchorage`	Configure timezone to America/Anchorage location.

Command	Syntax	Description
`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.
`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.

COMMAND	SYNTAX	DESCRIPTION
`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.
`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.
`configure timezone Asia Kabul`	`configure timezone Asia Kabul`	Configure timezone to Asia/Kabul location.

Command	Syntax	Description
`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.
`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.

Command	Syntax	Description
`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.
`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.
`configure timezone Europe Berlin`	`configure timezone Europe Berlin`	Configure timezone to Europe/Berlin location.

Command	Syntax	Description
`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.
`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.

COMMAND	SYNTAX	DESCRIPTION
`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.
`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 hyperv-ic`	`enable hyperv-ic`	Enable Hyper-V Linux Integration Components on Smart Protection Server
`enable ssh`	`enable ssh`	Enable the sshd daemon
`exit`	`exit`	Exit the session
`help`	`help`	Display an overview of the CLI syntax.

COMMAND	SYNTAX	DESCRIPTION
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
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

Command	Syntax	Description
`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
`shutdown`	`shutdown [time]`	Shut down this machine after a specified delay or immediately *time* UNIT Time in minutes to shutdown this machine [0]

Appendix B

Glossary

This glossary describes terms related to Smart Protection Server use.

TERM	DEFINITION
activate	To enable your software after completion of the registration process. Trend Micro products will not be operable until product activation is complete. Activate during installation or after installation (in the management console) on the Product License screen.
ActiveUpdate	ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update website, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, and program files via the Internet or the Trend Micro Total Solution CD.
address	Refers to a networking address (see IP address) or an email address, which is the string of characters that specify the source or destination of an email message.
administrator	Refers to the system administrator or the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.
administrator account	A user name and password that has administrator-level privileges.
antivirus	Computer programs designed to detect and clean computer viruses.

TERM	DEFINITION
authentication	The verification of the identity of a person or a process. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from). The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as the Data Encryption Standard (DES) algorithm, or on public-key systems using digital signatures. Also see public-key encryption and digital signature.
client	A computer system or process that requests a service of another computer system or process (a server) using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.
configuration	Selecting options for how your Trend Micro product will function, for example, selecting whether to quarantine or delete a virus-infected email message.
default	A value that pre-populates a field in the management console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them.
(administrative) domain	A group of computers sharing a common database and security policy.
domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution", uses the Domain Name System (DNS).
download (noun)	Data that has been downloaded, for example, from a website via HTTP.
download (verb)	To transfer data or code from one computer to another. Downloading often refers to transfer from a larger host system (especially a server or mainframe) to a smaller client system.
FAQ	Frequently Asked Questions, a list of questions and answers about a specific topic.

Term	Definition
file	An element of data used for storage, such as an email message or HTTP download.
file type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.
spyware/ grayware	A category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.
gateway	A gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached.
GUI	Graphical User Interface, the use of pictures rather than just words to represent the input and output of a program. This contrasts with a command line interface where communication is by exchange of strings of text.
hard disk (or hard drive)	One or more rigid magnetic disks rotating about a central axle with associated read/write heads and electronics, used to read and write hard disks or floppy disks, and to store data. Most hard disks are permanently connected to the drive (fixed disks) though there are also removable disks.
HTTP	Hypertext Transfer Protocol, the client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.
HTTPS	Hypertext Transfer Protocol Secure, a variant of HTTP used for handling secure transactions.
host	A computer connected to a network.

TERM	DEFINITION
Internet	A client-server hypertext information retrieval system, based on a series of networks connected with routers. The Internet is a modern information system and a widely accepted medium for advertising, online sales, and services, as well as university and many other research networks. The World Wide Web is the most familiar aspect of the Internet.
Internet Protocol (IP)	An Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.
intranet	Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet.
IP	Internet Protocol, dee IPv4 address or IPv6 address.
IPv4 address	Internet address for a device on a network, typically expressed using dot notation such as `123.123.123.123`.
IPv6 address	Internet address for a device on a network, typically expressed as `1234:1234:1234:1234:1234:1234:1234:1234`.
IT	Information technology, to include hardware, software, networking, telecommunications, and user support.
Java file	Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java applets. (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet’s code is transferred to your system and is executed by the browser’s Java Virtual Machine.)
Java malicious code	Virus code written or embedded in Java. Also see Java file.

Term	Definition
JavaScript virus	JavaScript is a simple programming language developed by Netscape that allows web developers to add dynamic content to HTML pages displayed in a browser using scripts. Javascript shares some features of Sun Microsystems Java programming language, but was developed independently.A JavaScript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in web pages and download to a user's desktop through the user's browser.Also see VBscript virus.
KB	Kilobyte, 1024 bytes of memory.
license	Authorization by law to use a Trend Micro product.
link (also called hyperlink)	A reference from some point in one hypertext document to some point in another document or another place in the same document. Links are usually distinguished by a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking on it with a mouse, the browser displays the target of the link.
local area network (LAN)	Any network technology that interconnects resources within an office environment, usually at high speeds, such as Ethernet. A local area network is a short-distance network used to link a group of computers together within a building. 10BaseT Ethernet is the most commonly used form of LAN. A hardware device called a hub serves as the common wiring point, enabling data to be sent from one machine to another over the network. LANs are typically limited to distances of less than 500 meters and provide low-cost, high-bandwidth networking capabilities within a small geographical area.
malware (malicious software)	Programming or files that are developed for the purpose of doing harm, such as viruses, worms, and Trojans.
management console	The user interface for your Trend Micro product. Also known as the product console.
Mbps	Millions of bits per second, a measure of bandwidth in data communications.
MB	Megabyte, 1024 kilobytes of data.

TERM	DEFINITION
mixed threat attack	Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the “Nimda” or “Code Red” threats.
Network Address Translation (NAT)	A standard for translating secure IP addresses to temporary, external, registered IP address from the address pool. This allows Trusted networks with privately assigned IP addresses to have access to the Internet. This also means that you don’t have to get a registered IP address for every machine in your network.
network virus	A type of virus that uses network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. Network viruses often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns or even complete network failure.
notification (Also see action and target)	A message that is forwarded to one or more of the following: system administrator, sender of a message, recipient of a message, file download, or file transfer. The purpose of the notification is to communicate that a prohibited action has taken place, or was attempted, such as a virus being detected in an attempted HTTP file download.
operating system	The software which handles tasks such as the interface to peripheral hardware, scheduling tasks, and allocating storage. In this documentation, the term also refers to the software that presents a window system and graphical user interface.
parameter	A variable, such as a range of values (a number from 1 to 10).
pattern file (also known as Official Pattern Release)	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.
port	A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels on the same network interface on the same computer. Each application program has a unique port number associated with it.

TERM	DEFINITION
proxy	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.
proxy server	A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.
scan	To examine items in a file in sequence to find those that meet a particular criteria.
scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
sector	A physical portion of a disk. (Also see partition, which is a logical portion of a disk.)
Secure Socket Layer (SSL)	Secure Socket Layer (SSL), is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.
server	A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server may run continuously (as a daemon), waiting for requests to arrive, or it may be invoked by some higher-level daemon which controls a number of specific servers.
shared drive	A computer peripheral device that is used by more than one person, thus increasing the risk of exposure to viruses.
signature	See virus signature.
SNMP	Simple Network Management Protocol, a protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.
traffic	Data flowing between the Internet and your network, both incoming and outgoing.

TERM	DEFINITION
Transmission Control Protocol/ Internet Protocol (TCP/IP)	A communications protocol which allows computers with different operating systems to communicate with each other. Controls how data is transferred between computers on the Internet.
trigger	An event that causes an action to take place. For example, your Trend Micro product detects a virus in an email message. This may trigger the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient.
true-file type	Used by IntelliScan, a virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).
URL	Universal Resource Locator, a standard way of specifying the location of an object, typically a web page, on the Internet, for example, www.trendmicro.com. The URL maps to an IP address using DNS.
virtual IP address (VIP address)	A VIP address maps traffic received at one IP address to another address based on the destination port number in the packet header.
Virtual Local Area Network (VLAN)	A logical (rather than physical) grouping of devices that constitute a single broadcast domain. VLAN members are not identified by their location on a physical subnetwork but through the use of tags in the frame headers of their transmitted data. VLANs are described in the IEEE 802.1Q standard.
Virtual Private Network (VPN)	A VPN is an easy, cost-effective and secure way for corporations to provide telecommuters and mobile professionals local dial-up access to their corporate network or to another Internet Service Provider (ISP). Secure private connections over the Internet are more cost-effective than dedicated private lines. VPNs are possible because of technologies and standards such as tunneling and encryption.
virtual router	A virtual router is the component of Screen OS that performs routing functions.

Term	Definition
virtual system	A virtual system is a subdivision of the main system that appears to the user to be a stand-alone entity. Virtual systems reside separately from each other in the same Trend Micro GateLock remote appliance; each one can be managed by its own virtual system administrator.
virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.
Web	The World Wide Web, also called the web or the Internet.
Web server	A server process running at a website which sends out web pages in response to HTTP requests from remote browsers.
workstation (also known as client)	A general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer, especially with respect to graphics, processing power and the ability to carry out several tasks at the same time.

TREND MICRO™

TREND MICRO INCORPORATED
10101 North De Anza Blvd. Cupertino, CA., 95014, USA
Tel:+1(408)257-1500/1-800 228-5651   Fax:+1(408)257-2003   info@trendmicro.com

www.trendmicro.com

Item Code: APEM36294/140116