



# Smart Protection Server 2.5

Security Made Smarter

## Administrator's Guide



Endpoint Security



Messaging Security



Protected Cloud



Web Security



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

<http://downloadcenter.trendmicro.com/>

Trend Micro, the Trend Micro t-ball logo, TrendLabs, OfficeScan, and Smart Protection Network are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 2008 -2011. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM84993/110727

Release Date: July 2011

Document Version No.: 1.0

Product Name and Version No.: Trend Micro™ Smart Protection Server 2.5

Protected by U.S. Patent No.: (Patents Pending)

The user documentation for Trend Micro™ Smart Protection Server is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the Knowledge Base at the Trend Micro website.

<http://esupport.trendmicro.com>

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

# Contents

## Preface

Smart Protection Server Documentation .....	viii
Audience .....	viii
Document Conventions .....	ix

## Chapter 1: Introducing Trend Micro Smart Protection Server

How Does Trend Micro Smart Protection Server Work? .....	1-2
The Need for a New Solution .....	1-2
Smart Protection Network Solutions .....	1-3
About Pattern Files .....	1-4
What's New .....	1-8
Features and Benefits .....	1-10
Trend Micro Smart Protection Network .....	1-11
About File Reputation .....	1-11
About Web Reputation .....	1-12
About Smart Feedback .....	1-12

## Chapter 2: Using Smart Protection Server

Using the Product Console .....	2-2
Accessing the Product Console .....	2-3
Using Smart Protection .....	2-4
Using Reputation Services .....	2-4
File Reputation .....	2-4
Web Reputation .....	2-5
Using the Approved/Blocked URL List .....	2-5
Using Smart Feedback .....	2-7
Updating .....	2-8
Configuring Manual Updates .....	2-8
Configuring Scheduled Updates .....	2-8
Updating Pattern Files .....	2-9
Updating Program Files .....	2-9
Performing Updates .....	2-9
Configuring an Update Source .....	2-11
Specifying an Update Source .....	2-12
Administrative Tasks .....	2-12
Using SNMP Service .....	2-12
Configuring SNMP Service .....	2-12
Downloading the MIB file .....	2-13
Configuring Proxy Settings .....	2-17
Specifying Proxy Settings .....	2-17
Downloading System Information for Support .....	2-18
Downloading the System Information File .....	2-18
Changing the Product Console Password .....	2-18

## Chapter 3: Monitoring Smart Protection Server

Using the Summary Screen .....	3-2
Using Tabs .....	3-3
Using Widgets .....	3-3
Adding Widgets .....	3-3
Editing Server Information in Widgets .....	3-4
Refreshing Server Information in Widgets .....	3-4
Removing a Widget from a Tab .....	3-4
Logs .....	3-5
Blocked Web Access Log .....	3-5
Viewing Blocked Web Access Log Entries .....	3-5
Reputation Service Log .....	3-5
Viewing Reputation Service Log Entries .....	3-5
Update Log .....	3-5
Viewing Update Log Entries .....	3-6
Log Maintenance .....	3-6
Performing Log Maintenance .....	3-6
Configuring Notifications .....	3-6
Email Notifications .....	3-6
Configuring Email Notifications .....	3-7
SNMP Trap Notifications .....	3-9
Configuring SNMP Trap Notifications .....	3-9

## **Chapter 4: Troubleshooting and Contact Information**

Before Contacting Technical Support .....	4-2
Contacting Trend Micro .....	4-2
TrendLabs .....	4-3
Known Issues .....	4-3
About Hot Fixes, Patches, and Service Packs .....	4-3

## **Appendix A: Command Line Interface (CLI) Commands**

List of Commands .....	A-2
------------------------	-----

## **Glossary**



# Preface

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

Topics include:

- *Smart Protection Server Documentation* on page viii
- *Audience* on page viii
- *Document Conventions* on page ix

# Smart Protection Server Documentation

The Smart Protection Server documentation consists of the following:

- **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.

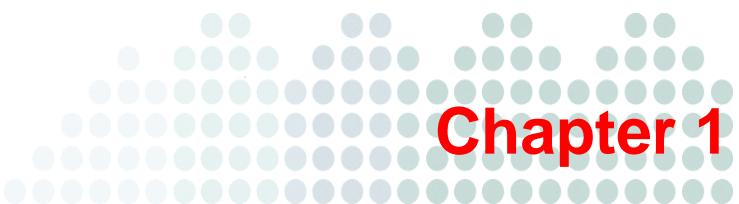
# Document Conventions

To help you locate and interpret information easily, the Smart Protection Server documentation uses the following conventions.

**TABLE P-1. Document conventions**

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
<b>Bold</b>	Menus and menu commands, command buttons, tabs, options, and tasks
<i>Italics</i>	References to other documentation or new technology components
Monospace	Examples, sample command lines, program code, web URL, file name, and program output
<u><b>Note:</b></u>	Configuration notes
<u><b>Tip:</b></u>	Recommendations
<u><b>WARNING!</b></u>	Reminders on actions or configurations that should be avoided





# Chapter 1

## Introducing Trend Micro Smart Protection Server

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

Topics include:

- *How Does Trend Micro Smart Protection Server Work?* on page 1-2
- *What's New* on page 1-8
- *Trend Micro Smart Protection Network* on page 1-11
- *About File Reputation* on page 1-11
- *About Smart Feedback* on page 1-12

## How Does Trend Micro Smart Protection Server Work?

Trend Micro™ Smart Protection Network™ 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 Servers or Trend Micro™ Smart Protection Network™.

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 Servers exist 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.

---

**Tip:** 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.

## About 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.

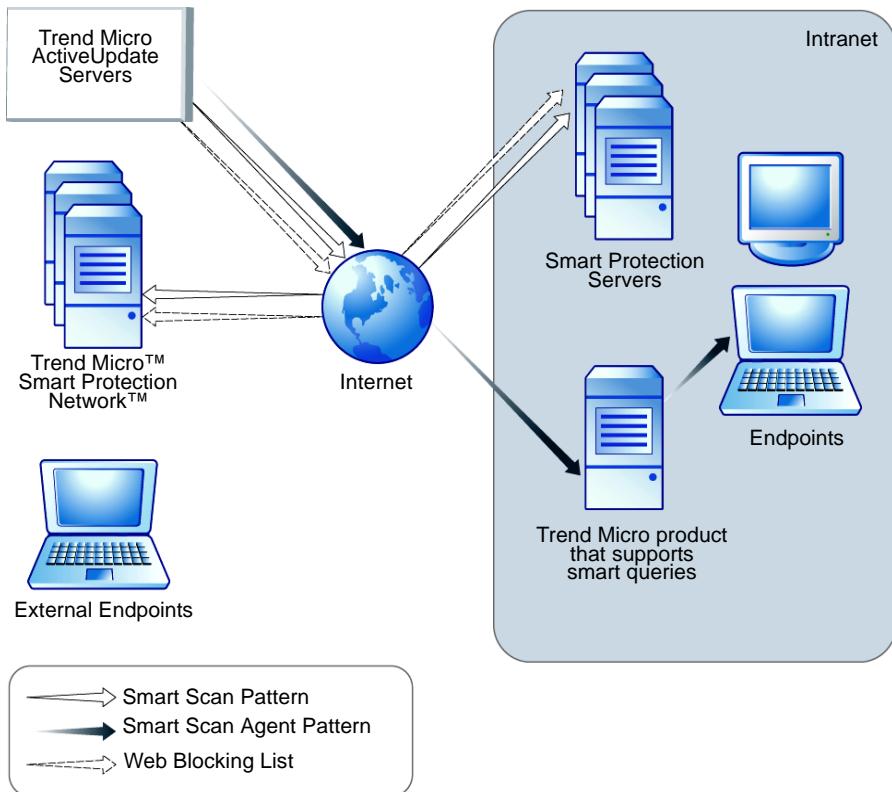
There are three pattern files:

- 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	<ul style="list-style-type: none"><li>• Pattern Files: Endpoints download the Smart Scan Agent Pattern file from Trend Micro products that support.</li><li>• Queries: Endpoints connect to Smart Protection Server for queries.</li></ul>
Without access to intranet	<ul style="list-style-type: none"><li>• 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.</li><li>• Queries: Endpoints scan files using local resources such as the Smart Scan Agent Pattern file.</li></ul>

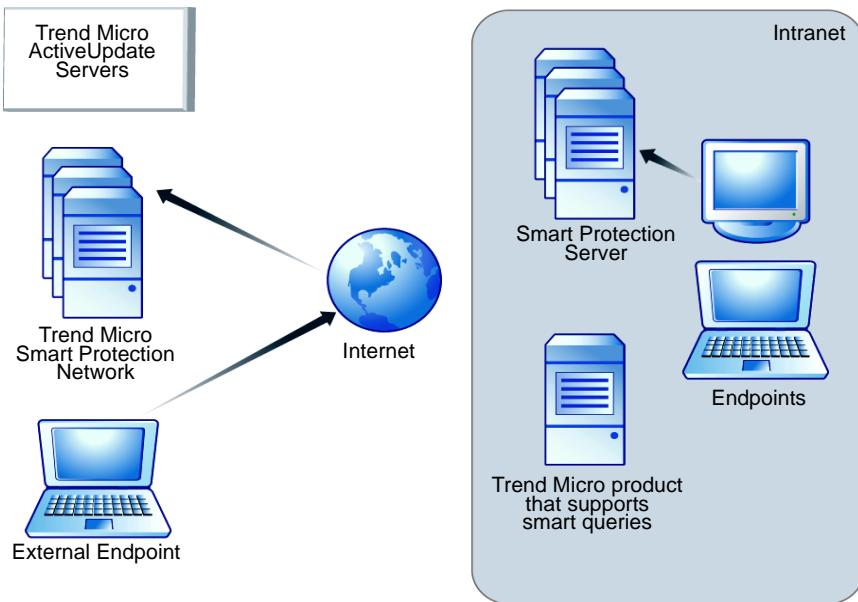
Advanced filtering technology enables the agent to "cache" the query result. This improves scan performance and eliminates the need to send the same query to Smart Protection Servers more than once.

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.

---



**FIGURE 1-2. Query process**

## What's New

*Table 1-2* is a list of new features for Smart Protection Server:

**TABLE 1-2. Version 2.5**

NEW FEATURE	DESCRIPTION
IPv6	This version of Smart Protection Server supports IPv6 environments.
Dashboard Enhancement	The dashboard and widgets have a new look and feel. The dashboard also provide new layouts and options.
New Log Types	<b>Blocked Web Access Log:</b> This log only displays Web Reputation queries for malicious websites, based on keywords, the data range, and product entities. <b>Reputation Service Log:</b> This log displays information about File/Web Reputation service status checking events. Administrators can delete logs that are no longer needed from the Log Maintenance screen.

**TABLE 1-3. Version 2.0**

NEW FEATURE	DESCRIPTION
Web Reputation Widgets	Additional widgets have been added for Web Reputation.
Smart Protection	This version of Smart Protection Server includes Web Reputation and Smart Feedback.

**TABLE 1-3. Version 2.0**

NEW FEATURE	DESCRIPTION
Multilingual User Interface	This version of Smart Protection Server includes Multilingual User Interface support, that allows customers to select a preferred display language.
Logs	This version of Smart Protection Server includes logs for monitoring activity.
Notifications	This version of Smart Protection Server includes notifications for events.

## Features and Benefits

*Table 1-4* lists the features and benefits.

**TABLE 1-4. Features and benefits**

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).

**TABLE 1-4. Features and benefits (Continued)**

FEATURES AND BENEFITS	
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.

## About File Reputation

File reputation technology from Trend Micro checks the reputation of each file against an extensive in-the-cloud database before permitting user access. 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.

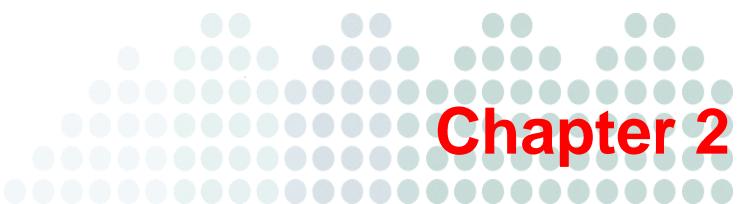
## About Web Reputation

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 Web site'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. 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.

## About Smart Feedback

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



## Chapter 2

# Using Smart Protection Server

This chapter provides Smart Protection Server configuration information.

Topics include:

- [\*Using the Product Console\*](#) on page 2-2
- [\*Using Smart Protection\*](#) on page 2-4
- [\*Updating\*](#) on page 2-8
- [\*Administrative Tasks\*](#) on page 2-12
- [\*Changing the Product Console Password\*](#) on page 2-18

# 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.



FIGURE 2-1. Summary Screen

**TABLE 2-1. Contents of Smart Protection Server Main Menu**

MAIN MENU	
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.
Administration	Provides options to configure SNMP service, notifications, proxy settings, and collecting diagnostic information for troubleshooting.

## Accessing the Product Console

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

**To access the web console:**

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.

### File Reputation

Enable File Reputation to support queries from endpoints.

#### Configuring File Reputation

##### To enable File Reputation:

#### Navigation Path: Smart Protection > Reputation Services

1. Navigate to the File Reputation Tab.



2. Select the **Enable File Reputation Service** check box.
3. Click **Save**. The Server Address can now be used for File Reputation queries by other Trend Micro products that support Smart Protection Servers.

## Web Reputation

Enable Web Reputation to support URL queries from endpoints.

### Configuring Web Reputation

**To enable Web Reputation:**

**Navigation Path: Smart Protection > Reputation Services > Web Reputation**

1. Navigate to the **Web Reputation** tab.



2. Select the **Enable Web Reputation Service** check box.
3. (Optional) Click **Advanced Settings** to display additional Web Reputation settings.
4. (Optional) Specify the priority of the Approved/Blocked URL List when filtering URLs.
5. Click **Save**.

## Using the Approved/Blocked URL List

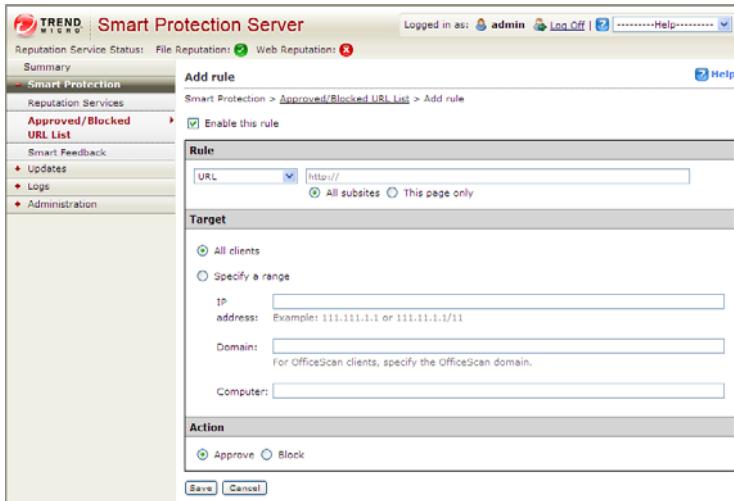
The Approved/Blocked URL List allows you to specify a custom list of approved and/or blocked URLs. This list is used for Web Reputation.

## Configuring the Approved/Blocked URL List

### To add a rule to the Approved/Blocked URL List:

#### Navigation Path: Smart Protection > Approved/Blocked URL List

1. Click **Add**. The Add rule screen displays.



2. Select the **Enable this rule** check box.
3. 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.

4. 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.
5. Select **Approve or Block**.
6. Click **Save**.

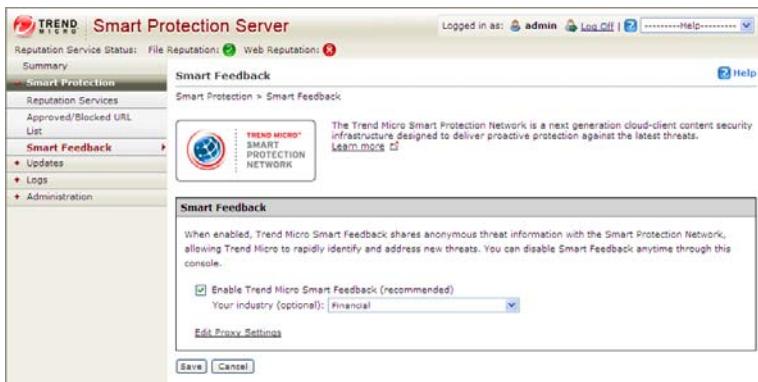
## Using Smart Feedback

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.

### To enable Smart Feedback:

#### Navigation Path: Smart Protection > Smart Feedback

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



2. Select your industry.
3. Click **Edit Proxy Settings** to navigate to the Proxy Settings screen if your network uses a proxy server and proxy server settings were not previously configured.
4. Click **Save**.

# Updating

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.

**To configure manual updates:**

**Navigation Path: Updates**

1. Click **Pattern** or **Program** from the drop down menu.
2. 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.

**To configure scheduled updates:**

**Navigation Path: Updates**

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

## Updating Pattern Files

Update pattern files to help ensure that the latest information is applied to queries. A brief description of the available options is below.

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

## Updating Program Files

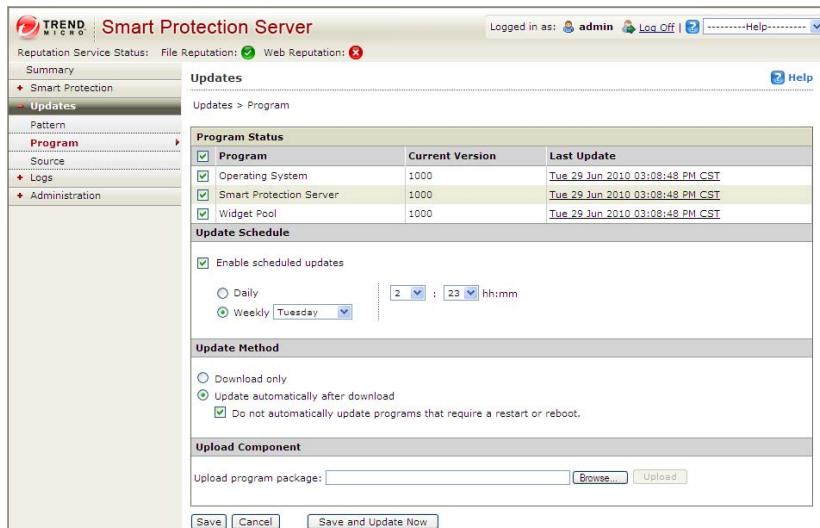
Update to the latest version of the product program to take advantage of product enhancements.

## Performing Updates

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

**To configure a scheduled update:****Navigation Path: Updates > Program**

1. Select **Enable scheduled updates** and select the update schedule.



The screenshot shows the 'Updates > Program' configuration page. The left sidebar has a tree view with 'Updates' selected. The main area has three tabs: 'Program Status', 'Update Schedule', and 'Update Method'. The 'Program Status' tab shows a table of updates for 'Operating System', 'Smart Protection Server', and 'Widget Pool' with their current version and last update time. The 'Update Schedule' tab has a checked checkbox for 'Enable scheduled updates' and a dropdown for 'Weekly' with 'Tuesday' selected. The 'Update Method' tab has three radio buttons: 'Download only' (unchecked), 'Update automatically after download' (checked), and 'Do not automatically update programs that require a restart or reboot' (checked). At the bottom are 'Save', 'Cancel', and 'Save and Update Now' buttons.

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**.

**To perform a manual update:****Navigation Path: Updates > Program**

1. 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.
2. Click **Save and Update Now.**

**To perform an update by uploading a program file:****Navigation Path: Updates > Program**

1. 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.

---

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

## Configuring an Update Source

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

## Specifying an Update Source

**To configure an update source:**

**Navigation Path: Updates > Source > File Reputation tab | Web Reputation tab**

1. Select **Trend Micro ActiveUpdate Server** or select **Other update source** and type a URL.
2. Click **Save**.

## Administrative Tasks

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

### Using SNMP Service

Smart Protection Servers supports SNMP to provide further flexibility in monitoring the product. Configure settings and download the MIB file from the Administration > SNMP Service screen.

### Configuring SNMP Service

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

### To configure SNMP Service:

#### Navigation Path: Administration > SNMP Service

1. Select the **Enable SNMP Service** check box.

2. Specify a **Community name**.
3. Select the **Enable IP restriction** check box to prevent unauthorized access to the SNMP service. Classless Inter-Domain Routing (CIDR) is not supported for IP restriction.
4. Specify an IP address.
5. Specify a subnet mask.
6. Click **Save**.

### Downloading the MIB file

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

#### To download the MIB file:

#### Navigation Path: Administration > SNMP Service

1. Click **Smart Protection Server MIB** to download the MIB file. A confirmation prompt displays.
2. Click **Save**. The Save As screen displays.

3. Specify the save location.
4. Click **Save**.

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

**TABLE 2-2. Description of 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:: TBLLastSuccessfulUp-date	1.3.6.1.4.1.6101 .1.2.1.2	Returns the date and time of the last successful Smart Scan Pattern update.
Trend-MIB:: LastUpdateError	1.3.6.1.4.1.6101 .1.2.1.3	Returns the status of the last Smart Scan Pattern update. 0 – Last pattern update was successful. <error code> - Last pattern update was unsuccessful.
Trend-MIB:: LastUpdateErrorMessage	1.3.6.1.4.1.6101 .1.2.1.4	Returns an error message if the last Smart Scan Pattern update was unsuccessful.
Trend-MIB:: WCSVersion	1.3.6.1.4.1.6101 .1.2.1.5	Returns the current Web Blocking List version.
Trend-MIB:: WCSLastSuccessfulUp-date	1.3.6.1.4.1.6101 .1.2.1.6	Returns the date and time of the last successful Web Blocking List update.

**TABLE 2-2. Description of Smart Protection Server MIB (Continued)**

OBJECT NAME	OBJECT IDENTIFIER (OID)	DESCRIPTION
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.

**TABLE 2-2. Description of Smart Protection Server MIB (Continued)**

OBJECT NAME	OBJECT IDENTIFIER (OID)	DESCRIPTION
Trend-MIB:: WCSLastVerifyError	1.3.6.1.4.1.6101 .1.2.2.3	Returns the status of web reputation query. 0 – Web reputation query is behaving as expected. <error code> - Web reputation query is not behaving as expected.
Trend-MIB:: LastVerifyErrorMessage	1.3.6.1.4.1.6101 .1.2.2.4	Returns an error message if the last health status of a File Reputation query was unsuccessful.
Trend-MIB:: WCSLastVerifyErrorMessage	1.3.6.1.4.1.6101 .1.2.2.5	Returns an error message if the last health status of a Web Reputation query was unsuccessful.

## Configuring Proxy Settings

If you use a proxy server in the network, configure proxy settings.

**Note:** SOCKS4 proxy configuration has been removed from Smart Protection Server. After upgrading to this version, if in the previous version SOCKS4 was configured for the proxy settings, the proxy settings need to be re-configured.

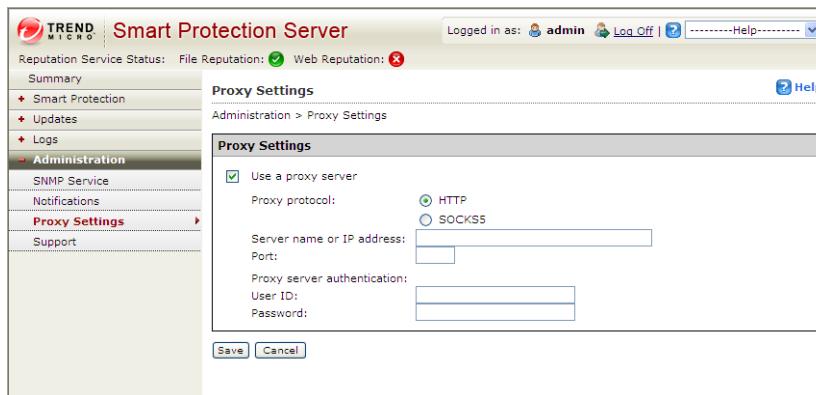
## Specifying Proxy Settings

SOCKS4 proxy configuration has been removed from Smart Protection Server. After upgrading to this version, if in the previous version SOCKS4 was configured for the proxy settings, the proxy settings need to be re-configured.

### To configure proxy settings:

#### Navigation Path: Administration > Proxy Settings

1. Select the **Use a proxy server for updates** check box.



2. Select **HTTP** or **SOCKS5** for the Proxy protocol.
3. Type the server name or IP address.
4. Type the port number.
5. If your proxy server requires credentials, type the **User ID** and **Password**.

6. Click **Save**.

## Downloading System Information for Support

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

### Downloading the System Information File

**To download diagnostic information:**

#### **Navigation Path: Administration > Support**

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

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

---

**To change the product console password using the CLI:**

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://IMSPS25.trendmicro.com/tmcss
    http://IMSPS25.trendmicro.com/tmcss

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

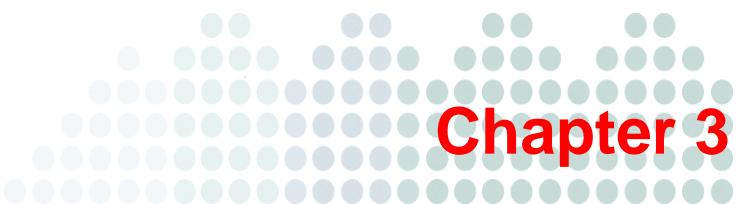
    http:// IPv4 addr :5274
    https:// IPv6 addr      :5274
    http://IMSPS25.trendmicro.com:5274

Use the following URL to access the Web product console:

    https:// IPv4 addr :4343
    https://[ IPv6 addr      ]:4343
    https://IMSPS25.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 Smart Protection Server with logs and from the Summary screen with widgets.

Topics include:

- [\*Using the Summary Screen\*](#) on page 3-2
- [\*Using Widgets\*](#) on page 3-3
- [\*Logs\*](#) on page 3-5
- [\*Configuring Notifications\*](#) on page 3-6

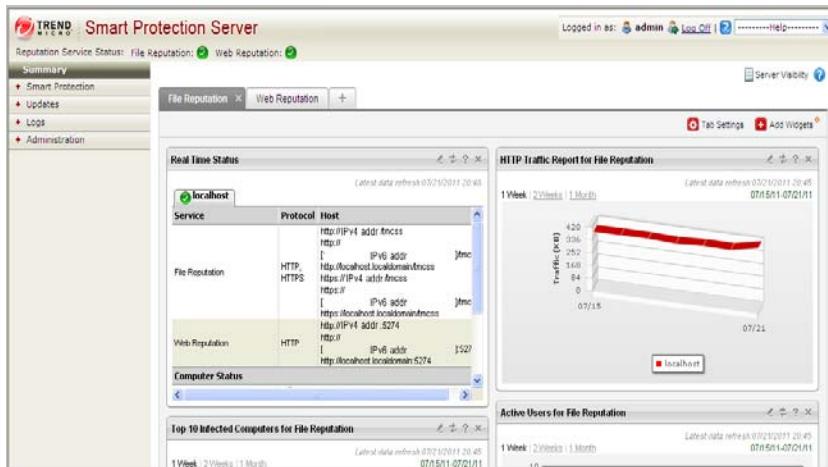
## Using the Summary Screen

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

You can do the following with the Summary screen:

- Add widgets that display information such as real time status, the number of active users, endpoints with the highest number of infections, endpoints with the highest number of blocked URLs, and server traffic.
- Organize widgets using tabs.
- Customize tab layout to display different numbers of columns that align the widgets.
- View information from multiple Smart Protection Servers.

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.



**FIGURE 3-1. Summary Screen**

To view customized information, add widgets to this screen. Drag and drop widgets to change the display order.

## Using Tabs

Customize and manage widgets by adding and configuring tabs. Up to 30 tabs can be added.

### To add a new tab:

#### Navigation Path: Summary



1. Click **Add** from the work area.
2. Specify the **Title**.
3. Select the **Layout**.

---

**Note:** The tab layout can be changed by clicking **Tab Settings**.

---

4. Select **Auto-fit** to specify that all widgets in a tab have the same height.
5. Click **Save**.

## Using 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.

### Adding Widgets

Select from a list of available widgets to add to each tab.

### To add widgets:

#### Navigation Path: Summary

1. Click **Add widgets** from the work area.
2. Select the widgets that you want to add.
3. Click **Add**.

## Editing Server Information in Widgets

Editing server information is the same for all widgets. View information from multiple scan servers on one widget by selecting servers from the list of servers that displays.

### To edit server information displayed in widgets:

1. Click the edit icon  in the upper left hand corner of the widget.
2. Select the check box for the Smart Protection Server to add to the information displayed in the widget.
3. Click **Save**. The widget automatically refreshes and displays the information of the selected scan servers.

---

**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.

---

## Refreshing Server Information in Widgets

Refreshing server information is the same for all widgets. When you click the refresh button, only information from selected servers will refresh.

## Removing a Widget from a Tab

Click the close button  to remove a widget from a tab. The widget no longer displays.

## 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.

#### Viewing Blocked Web Access Log Entries

**To view Blocked Web Access Log entries:**

**Navigation Path: Logs > Blocked Web Access Log**

1. Specify the search criteria.
2. Click **Display Log**.

### Reputation Service Log

The Reputation Service Log screen displays service status information for Web Reputation and File Reputation.

#### Viewing Reputation Service Log Entries

**To view Reputation Service Log entries:**

**Navigation Path: Logs > Reputation Service Log**

1. Specify the search criteria.
2. Click **Display Log**.

### Update Log

The Update Log screen displays information about pattern or program file updates. A brief description of the available options is below.

- **Date Range:** Select the date range that the update took place.

- **Type:** Select the type of update to display.

## Viewing Update Log Entries

**To view Update Log entries:**

### Navigation Path: Logs > Update Log

1. Specify the search criteria by selecting a date range or type.
2. Click **Display Log**.

## Log Maintenance

Perform log maintenance to delete logs that are no longer needed.

## Performing Log Maintenance

**To perform log maintenance:**

### Navigation Path: Logs > Log Maintenance

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

## Configuring 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

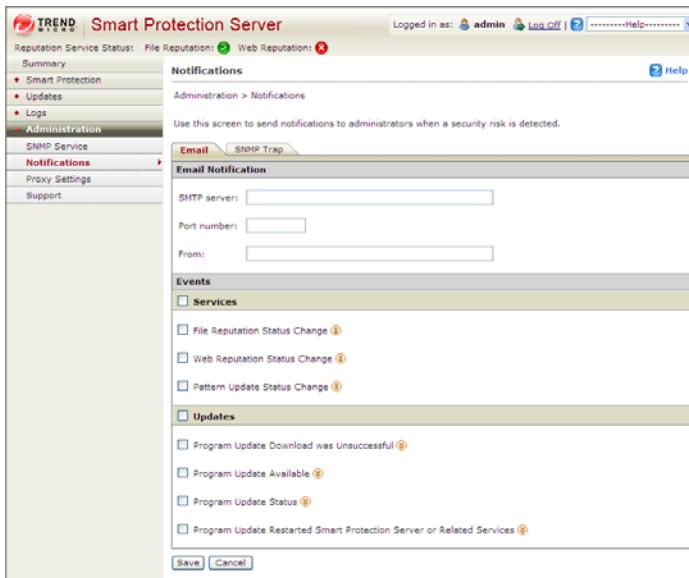
Configure email notification settings to notify administrators through email messages when there is a status change in services or updates.

## Configuring Email Notifications

To configure email notifications:

### Navigation Path: Administration > Notifications

1. Click the **Email** tab. The tab for email notifications appears.



The screenshot shows the 'Smart Protection Server' administration interface. The left sidebar has a 'Notifications' section selected. The main content area is titled 'Notifications' and shows the 'Email' tab is active. It contains fields for 'SMTP server', 'Port number', and 'From'. Below these are sections for 'Events' (with 'Services' and 'Updates' subsections) and a list of checkboxes for various notification types. At the bottom are 'Save' and 'Cancel' buttons.

Reputation Service Status: File Reputation:  Web Reputation: 

Logged in as: admin [Log Off](#) [Help](#)

Notifications

Administration > Notifications

Help

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

**Email** **SNMP Trap**

**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 

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. 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.

### Configuring SNMP Trap Notifications

**To configure SNMP trap notifications:**

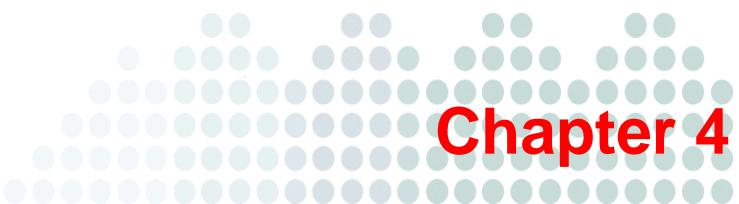
#### Navigation Path: Administration > Notifications

1. Click the **SNMP Trap** tab. The tab for SNMP trap notifications appears.



2. Select the **Services** check box or select from the following:
  - **File Reputation Status Change:** Select to send a notification for status changes and specify the message.
  - **Web Reputation Status Change:** Select to send a notification for status changes and specify the message.
  - **Pattern Update Status Change:** Select to send a notification for status changes and specify the message.
3. Type the SNMP trap server IP address.
4. Type the SNMP community name.
5. Click **Save**.





## Chapter 4

# Troubleshooting and Contact Information

Trend Micro is committed to providing service and support that exceeds our users' expectations. This chapter contains information on how to get technical support. Remember, you must register your product to be eligible for support.

Topics include:

- *Before Contacting Technical Support* on page 4-2
- *Contacting Trend Micro* on page 4-2
- *TrendLabs* on page 4-3
- *Known Issues* on page 4-3

## Before Contacting Technical Support

Before contacting technical support, here are two things you can quickly do to try and find a solution to your problem:

- **Check your documentation:** Search documents to see if they contain your solution.
- **Visit the Trend Micro Technical Support Website:** The Trend Micro Technical Support website contains the latest information about all Trend Micro products. The support website has answers to previous user inquiries.

To search the Knowledge Base, visit

<http://esupport.trendmicro.com>

## Contacting Trend Micro

In addition to phone support, Trend Micro provides the following resources:

- Readme: late-breaking product news, installation instructions, known issues, and version specific information
- Knowledge Base: technical information procedures provided by the Support team:  
<http://esupport.trendmicro.com>
- Product updates and patches  
<http://www.trendmicro.com/download/>
- To locate the Trend Micro office nearest you, visit:  
<http://us.trendmicro.com/us/about-us/contact/index.html>
- Email support  
[support@trendmicro.com](mailto:support@trendmicro.com)

**To speed up the problem resolution, when you contact our staff please provide as much of the following information as you can:**

1. Product build version
2. Virtualization platform (VMware™ or Hyper-V™) and version
3. Exact text of the error message, if any
4. Steps to reproduce the problem
5. Collect system information from the web console.

## TrendLabs

Trend Micro TrendLabs<sup>SM</sup> is a global network of virus prevention and Web threat research and product support centers providing continuous 24/7 coverage to Trend Micro customers worldwide.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers worldwide ensure rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters has earned ISO 9002 certification for its quality management procedures in 2000 - one of the first antivirus research and support facilities to be so accredited. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, visit:

<http://www.trendmicro.com/en/security/trendlabs/overview.htm>

## 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>

## About 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.

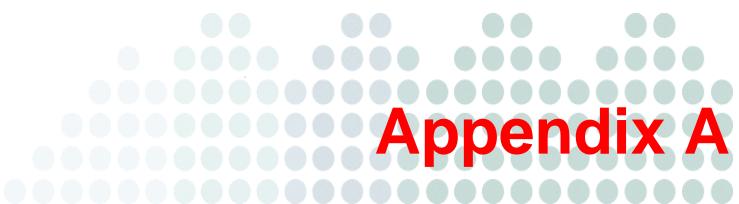
The following is a summary of the items Trend Micro may release:

- 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://www.trendmicro.com/download>

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



## 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.

Topics include:

- *List of Commands* on page A-2

## List of 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.

**TABLE A-1. Command Line Interface (CLI) Commands**

COMMAND	SYNTAX	DESCRIPTION
configure date	configure date <date> <time>	Configure date and save to CMOS  <i>date</i> DATE_FIELD [DATE_FIELD] <i>time</i> TIME_FIELD [TIME_FIELD]
configure dns ipv4	configure dns ipv4 <dns1> [dns2]	Configure IPv4 DNS settings  <i>dns1</i> <u>IPv4_ADDR</u> Primary DNS server  <i>dns2</i> <u>IPv4_ADDR</u> Secondary DNS server []
configure dns ipv6	configure dns ipv6 <dns1> [dns2]	Configure IPv6 DNS settings  <i>dns1</i> <u>IPv6_ADDR</u> Primary DNS server  <i>dns2</i> <u>IPv6_ADDR</u> Secondary DNS server []

**TABLE A-1. Command Line Interface (CLI) Commands (Continued)**

COMMAND	SYNTAX	DESCRIPTION
configure hostname	configure hostname <hostname>	Configure the hostname hostname <u>HOSTNAME</u> 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
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)

**TABLE A-1. Command Line Interface (CLI) Commands (Continued)**

COMMAND	SYNTAX	DESCRIPTION
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]
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]

**TABLE A-1. Command Line Interface (CLI) Commands (Continued)**

COMMAND	SYNTAX	DESCRIPTION
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  <i>user</i> <b>USER</b> 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 inter-face <ifname>	Configure the default server settings
configure timezone Africa Cairo	configure timezone Africa Cairo	Configure timezone to Africa/Cairo location.
configure timezone Africa Harare	configure timezone Africa Harare	Configure timezone to Africa/Harare location.
configure timezone Africa Nairobi	configure timezone Africa Nairobi	Configure timezone to Africa/Nairobi location
configure timezone America Anchorage	configure timezone America Anchorage	Configure timezone to America/Anchorage location
configure timezone America Bogota	configure timezone America Bogota	Configure timezone to America/Bogota location

**TABLE A-1. Command Line Interface (CLI) Commands (Continued)**

COMMAND	SYNTAX	DESCRIPTION
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

**TABLE A-1. Command Line Interface (CLI) Commands (Continued)**

COMMAND	SYNTAX	DESCRIPTION
configure timezone America Phoenix	configure timezone America Phoenix	Configure timezone to America/Phoenix
configure timezone America Santiago	configure timezone America Santiago	Configure timezone to America/Santiago
configure timezone America St_Johns	configure timezone America St_Johns	Configure timezone to America/St_Johns
configure timezone America Tegucigalpa	configure timezone America Tegucigalpa	Configure timezone to America/Tegucigalpa
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

**TABLE A-1. Command Line Interface (CLI) Commands (Continued)**

COMMAND	SYNTAX	DESCRIPTION
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
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

**TABLE A-1. Command Line Interface (CLI) Commands (Continued)**

COMMAND	SYNTAX	DESCRIPTION
configure timezone Asia Singapore	configure timezone Asia Singapore	Configure timezone to Asia/Singapore location
configure timezone Asia Taipei	configure timezone Asia Taipei	Configure timezone to Asia/Taipei location
configure timezone Asia Tehran	configure timezone Asia Tehran	Configure timezone to Asia/Tehran location
configure timezone Asia Tokyo	configure timezone Asia Tokyo	Configure timezone to Asia/Tokyo location
configure timezone Asia Yakutsk	configure timezone Asia Yakutsk	Configure timezone to Asia/Yakutsk location
configure timezone Atlantic Azores	configure timezone Atlantic Azores	Configure timezone to Atlantic/
configure timezone Australia Adelaide	configure timezone Aus-tralia Adelaide	Configure timezone to Australia/Adelaide location
configure timezone Australia Brisbane	configure timezone Aus-tralia Brisbane	Configure timezone to Australia/Brisbane location
configure timezone Australia Darwin	configure timezone Aus-tralia Darwin	Configure timezone to Australia/Darwin location
configure timezone Australia Hobart	configure timezone Aus-tralia Hobart	Configure timezone to Australia/Hobart location
configure timezone Australia Melbourne	configure timezone Aus-tralia Melbourne	Configure timezone to Australia/Melbourne location
configure timezone Australia Perth	configure timezone Aus-tralia Perth	Configure timezone to Australia/

**TABLE A-1. Command Line Interface (CLI) Commands (Continued)**

COMMAND	SYNTAX	DESCRIPTION
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
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

**TABLE A-1. Command Line Interface (CLI) Commands (Continued)**

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

**TABLE A-1. Command Line Interface (CLI) Commands (Continued)**

COMMAND	SYNTAX	DESCRIPTION
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.
history	history [limit]	Display the current session's command line history  <i>limit</i> 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  <i>time</i> <u>UNIT</u> Time in minutes to reboot this machine [0]
show date	show date	Display current date/time
show hostname	show hostname	Display network host-name
show interfaces	show interfaces	Display network interface information
show ipv4 address	show ipv4 address	Display network IPv4 address

**TABLE A-1. Command Line Interface (CLI) Commands (Continued)**

COMMAND	SYNTAX	DESCRIPTION
show ipv4 dns	show ipv4 dns	Display network IPv4 DNS servers
show ipv4 gateway	show ipv4 gateway	Display network IPv4 gateway
show ipv4 route	show ipv4 route	Display network IPv4 routing table
show ipv4 type	show ipv4 type	Display network IPv4 configuration type (dhcp / static)
show ipv6 address	show ipv6 address	Display network IPv6 address
show ipv6 dns	show ipv6 dns	Display network IPv6 DNS servers
show ipv6 gateway	show ipv6 gateway	Display network IPv6 gateway
show ipv6 route	show ipv6 route	Display network IPv6 routing table
show ipv6 type	show ipv6 type	Display network IPv6 configuration type (auto / dhcp / static)
show timezone	show timezone	Display network timezone
show uptime	show uptime	Display current system uptime
show url management	show url management	Display web management console URL

**TABLE A-1. Command Line Interface (CLI) Commands (Continued)**

COMMAND	SYNTAX	DESCRIPTION
show url FileReputationService	show url FileReputation-Service	Display endpoint connection addresses for File Reputation Service
show url WebReputationService	show url WebReputation-Service	Display endpoint connection addresses for Web Reputation Service
shutdown	shutdown [time]	Shut down this machine after a specified delay or immediately <i>time UNIT</i> Time in minutes to shutdown this machine [0]

# Glossary

This glossary describes special terms used in the product documentation set.

**TABLE G-1. Glossary of Terms**

TERM	EXPLANATION
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 "system administrator"—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.

**TABLE G-1. Glossary of Terms (Continued)**

TERM	EXPLANATION
authentication	<p>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).</p> <p>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.</p> <p><i>Also see public-key encryption and digital signature.</i></p>
client	<p>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.</p>
configuration	<p>Selecting options for how your Trend Micro product will function, for example, selecting whether to quarantine or delete a virus-infected email message.</p>
default	<p>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.</p>
(administrative) domain	<p>A group of computers sharing a common database and security policy.</p>

**TABLE G-1. Glossary of Terms (Continued)**

TERM	EXPLANATION
domain name	The full name of a system, consisting of its local host name and its domain name, for example, <code>tellsitall.com</code> . 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.
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.

**TABLE G-1. Glossary of Terms (Continued)**

TERM	EXPLANATION
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.
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.

**TABLE G-1. Glossary of Terms (Continued)**

TERM	EXPLANATION
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—See 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. <i>Also see Java file.</i>

**TABLE G-1. Glossary of Terms (Continued)**

TERM	EXPLANATION
JavaScript virus	<p>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.</p> <p>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.</p> <p><i>Also see VBscript virus.</i></p>
KB	Kilobyte—1024 bytes of memory.
license	Authorization by law to use a Trend Micro product.
link (also called hyperlink)	<p>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.</p>
local area network (LAN)	<p>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.</p>

**TABLE G-1. Glossary of Terms (Continued)**

TERM	EXPLANATION
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.
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.

**TABLE G-1. Glossary of Terms (Continued)**

TERM	EXPLANATION
notification  (Also see action and target)	<p>A message that is forwarded to one or more of the following:</p> <ul style="list-style-type: none"> <li>- system administrator</li> <li>- sender of a message</li> <li>- recipient of a message, file download, or file transfer</li> </ul> <p>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.</p>
operating system	<p>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.</p>
parameter	<p>A variable, such as a range of values (a number from 1 to 10).</p>
pattern file (also known as Official Pattern Release)	<p>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.</p>
port	<p>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.</p>
proxy	<p>A process providing a cache of items available on other servers which are presumably slower or more expensive to access.</p>

**TABLE G-1. Glossary of Terms (Continued)**

TERM	EXPLANATION
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.

**TABLE G-1. Glossary of Terms (Continued)**

TERM	EXPLANATION
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.
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 <i>trigger</i> 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, <a href="http://www.trendmicro.com">www.trendmicro.com</a> . 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.

**TABLE G-1. Glossary of Terms (Continued)**

TERM	EXPLANATION
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.
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.

**TABLE G-1. Glossary of Terms (Continued)**

TERM	EXPLANATION
virus	<p>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.</p> <p>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.</p>
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.

# Index

## **A**

Administrator's Guide P-viii  
Approved/Blocked URL List 2-5  
Audience P-viii

## **C**

CLI 2-3  
Command Line Interface A-1  
continuity of protection 1-3, 1-6

## **D**

design a secure password 2-18  
diagnostic information 2-18  
Document Conventions P-ix  
documentation 4-2

## **F**

File Reputation 1-11, 2-4

## **H**

HTTP 3-2  
HTTPS 3-2

## **I**

Installation and Upgrade Guide P-viii  
intranet 1-6

## **K**

Knowledge Base 4-2–4-3

## **M**

management 1-10

MIB file 2-12–2-13

## **N**

network 1-10  
notification 3-8

## **O**

Online Help P-viii

## **P**

password 2-18  
pattern 1-3, 1-10  
program file 3-5  
protocols 3-2  
proxy server 2-17  
proxy settings 2-17

## **R**

Readme File P-viii  
Readme file 4-3

## **S**

search criteria 3-6  
server information 3-4  
Smart Feedback 2-3, 2-7  
Smart Protection Network 1-3, 1-11  
Smart Protection Server 1-2–1-4, 2-8, 3-4  
Smart Protection Servers 1-4  
smart protection solution 1-3  
Smart Scan Agent Pattern 1-4  
Smart Scan Pattern 1-4, 2-8

SMTP 3-8  
SNMP 2-13  
spyware 1-10  
summary 2-3, 3-2  
support 4-2

## **T**

tabs 3-3  
technical support 4-2  
Trend Micro Smart Protection Network 1-2—1-3  
TrendLabs 4-3  
Trojans 1-10

## **U**

updates 3-5  
URL 2-3, 2-6

## **V**

virus/malware 1-3  
viruses/malware 1-10  
volume of threats 1-2

## **W**

Web Access Log 3-5  
Web Blocking List 2-8  
web console 2-13  
Web Reputation 1-12, 2-4  
Web reputation 1-12  
widget 3-4  
widgets 3-4  
worms 1-10