TREND MICRO™

OfficeScan™ 10.5

For Enterprise and Medium Business

Smart Protection Server Getting Started Guide

TREND MICRO™ SMART PROTECTION NETWORK™

Endpoint Security

Protected Cloud

Web Security

Document Part No. OSEM104459/10421

Release Date: August 2010

Protected by U.S. Patent No. 5,623,600; 5,889,943; 5,951,698; 6,119,165

The user documentation for Trend Micro OfficeScan introduces the main features of the software and installation instructions for your production environment. Read through it before 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 online Knowledge Base at Trend Micro's Web site.

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.

Please evaluate this documentation on the following site:
http://www.trendmicro.com/download/documentation/rating.asp

Contents

Chapter 2: Using Smart Protection Services

Chapter 3: Smart Protection Solutions Environment

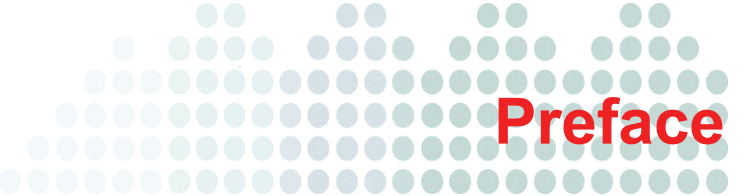
Chapter 4: Managing OfficeScan Clients and Smart Protection Servers

Chapter 5: Getting Help

Appendix A: Scan Method Deployment Tasks

Appendix B: Command Line Interface (CLI) Commands

Index



Preface

Welcome to the *Trend Micro™ Smart Protection Server for OfficeScan™ Getting Started Guide*. This document introduces smart protection solutions concepts, guides users on preparing the smart protection environment, and provides instructions on managing OfficeScan clients using smart protection solutions.

Topics in this chapter:

OfficeScan Documentation

OfficeScan documentation includes the following:

TABLE P-1. OfficeScan documentation

DOCUMENTATION	DESCRIPTION
Trend Micro Smart Protection Server for OfficeScan Getting Started Guide	A PDF document that helps users understand smart protection solutions concepts, prepare the smart protection environment needed to manage OfficeScan client using smart protection solutions
Installation and Upgrade Guide	A PDF document that discusses requirements and procedures for installing and upgrading the OfficeScan server
Administrator's Guide	A PDF document that discusses getting started information, client installation procedures, and OfficeScan server and client management
Help	HTML files compiled in WebHelp or CHM format that provide "how to's", usage advice, and field-specific information. The Help is accessible from the OfficeScan server, client, and Policy Server consoles, and from the OfficeScan Master Setup.
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site: http://esupport.trendmicro.com/support

Download the latest versions of the PDF documents and readme at:

http://www.trendmicro.com/download

Audience

OfficeScan documentation is intended for the following users:

- **OfficeScan Administrators:** Responsible for OfficeScan management, including server and client installation and management. These users are expected to have advanced networking and server management knowledge.
- **Cisco NAC administrators:** Responsible for designing and maintaining security systems with Cisco NAC servers and Cisco networking equipment. They are assumed to have experience with this equipment.
- **End users:** Users who have the OfficeScan client installed on their computers. The computer skill level of these individuals ranges from beginner to power user.

Document Conventions

To help you locate and interpret information easily, the OfficeScan documentation uses the following conventions:

TABLE P-2. 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, options, and tasks
Italics	References to other documentation or new technology components
TOOLS > CLIENT TOOLS	A "breadcrumb" found at the start of procedures that helps users navigate to the relevant Web console screen. Multiple breadcrumbs means that there are several ways to get to the same screen.
<Text>	Indicates that the text inside the angle brackets should be replaced by actual data. For example, C:\Program Files\<file_name> can be C:\Program Files\sample.jpg.

TABLE P-2. Document conventions (Continued)

CONVENTION	DESCRIPTION
Note: text	Provides configuration notes or recommendations
Tip: text	Provides best practice information and Trend Micro recommendations
WARNING! text	Provides warnings about activities that may harm computers on your network

Terminology

The following table provides the official terminology used throughout the OfficeScan documentation:

TABLE P-3. OfficeScan terminology

TERMINOLOGY	DESCRIPTION
Client	The OfficeScan client program
Client computer or endpoint	The computer where the OfficeScan client is installed
Client user (or user)	The person managing the OfficeScan client on the client computer
Server	The OfficeScan server program
Server computer	The computer where the OfficeScan server is installed

TABLE P-3. OfficeScan terminology (Continued)

TERMINOLOGY	DESCRIPTION
Administrator (or OfficeScan administrator)	The person managing the OfficeScan server
Console	The user interface for configuring and managing OfficeScan server and client settings The console for the OfficeScan server program is called "Web console", while the console for the client program is called "client console".
Security risk	The collective term for virus/malware, spyware/grayware, and Web threats
Product service	Includes Antivirus, Damage Cleanup Services, and Web Reputation and Anti-spyware—all of which are activated during OfficeScan server installation
OfficeScan service	Services hosted by Microsoft Management Console (MMC). For example, ofcservice.exe, the OfficeScan Master Service.
Program	Includes the OfficeScan client, Cisco Trust Agent, and Plug-in Manager
Components	Responsible for scanning, detecting, and taking actions against security risks
Client installation folder	The folder on the computer that contains the OfficeScan client files. If you accept the default settings during installation, you will find the installation folder at any of the following locations: **C:\Program Files\Trend Micro\OfficeScan Client** **C:\Program Files (x86)\Trend Micro\OfficeScan Client**

TABLE P-3. OfficeScan terminology (Continued)

TERMINOLOGY	DESCRIPTION
Server installation folder	The folder on the computer that contains the OfficeScan server files. If you accept the default settings during installation, you will find the installation folder at any of the following locations: **C:\Program Files\Trend Micro\OfficeScan** **C:\Program Files (x86)\Trend Micro\OfficeScan** For example, if a particular file is found under \PCCSRV on the server installation folder, the full path to the file is: C:\Program Files\Trend Micro\OfficeScan\PCCSRV\<file_name>.
Smart scan client	An OfficeScan client that has been configured to use smart scan
Conventional scan client	An OfficeScan client that has been configured to use conventional scan

Chapter 1

Introducing Trend Micro Smart Protection Solutions

This topic describes Trend Micro™ smart protection solutions and the components that support these solutions.

Topics in this chapter:

About Smart Protection Solutions

The Trend Micro™ smart protection solutions 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 clients to access its unique in-the-cloud correlation of email, Web and file reputation technologies, as well as 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.

By incorporating in-the-cloud reputation, scanning, and correlation technologies, the Trend Micro smart protection solutions reduces reliance on conventional pattern file downloads and eliminates the delays commonly associated with desktop updates.

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 loads 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 Services

Smart protection solutions include services that provide anti-malware signatures, web reputations, and threat databases that are stored in-the-cloud. These services leverage file reputation technology to detect security risks and web reputation to proactively block malicious Web sites. File reputation technology works by off loading a large number of anti-malware signatures that were previously stored on endpoint computers to smart protection sources. Web reputation technology allows local smart protection sources to host URL reputation data that were previously hosted solely by Trend Micro. Both technologies ensure smaller bandwidth consumption when updating patterns or checking a URL's validity.

Additionally, Trend Micro continues to harvest information anonymously sent from Trend Micro products worldwide to proactively determine each new threat.

Smart protection services leverage the following technologies:

- *File Reputation* on page 1-3
- *Web Reputation* on page 1-4
- *Smart Feedback* on page 1-4

File Reputation

File reputation technology from Trend Micro 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 client footprint.

Web Reputation

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.

When a user accesses a URL, Trend Micro:

- Leverages the domain-reputation database to verify the credibility of the Web sites and pages
- Assigns reputation scores to Web domains and individual pages or links within sites
- Allows or blocks users from accessing sites

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 there are times that only portions of legitimate sites are hacked and reputations can change dynamically over time.

Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products and 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 of Trend Micro's threat databases, blocking any subsequent customer encounters of a given threat. For example, routine reputation checks are sent to the Smart Protection Network. 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. This is much like an automated neighborhood watch that involves the community in protection of others. The privacy of a customer's personal or business information is always protected because the threat information gathered is based on the reputation of the communication source.

Trend Micro Smart Feedback is designed to collect and transfer relevant data from Smart Protection Servers to the Smart Protection Network so that further analysis can be conducted, and consequently, advanced solutions can evolve and be deployed to protect clients.

Some samples of information sent to Trend Micro:

- File checksums
- Web sites accessed
- File information, including sizes and paths
- Names of executable files

You can terminate your participation to the program anytime from the Web console.

Tip: You do not need to participate in Smart Feedback to protect your computers. Your participation is optional and you may opt out at any time. Trend Micro recommends that you participate in Smart Feedback to help provide better overall protection for all Trend Micro customers.

For more information on the Smart Protection Network, visit:

http://www.smartprotectionnetwork.com

Smart Protection Sources

Trend Micro delivers smart protection services through smart protection sources. Smart protection sources host the majority of the virus/malware pattern definitions and web reputation data. Smart protection sources make these definitions available to other endpoints on the network for verifying potential threats. Queries are only sent to smart protection sources 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 sources as part of their regular system protection activities. In this solution, OfficeScan clients send identification information, determined by Trend Micro technology, to smart protection sources for queries. Clients never send the entire file when using file reputation technology. The risk of the file is determined using identification information.

The smart protection source to which a client connects depends on the client's location. Clients can connect to either of the following:

- **Trend Micro Smart Protection Network**: A globally scaled, Internet-based, infrastructure that provides reputation services to users who do not have immediate access to their corporate network.
- **Smart Protection Server**: Smart Protection Servers are for users who have access to their local corporate network. Local servers localize smart protection services to the corporate network to optimize efficiency.

TABLE 1-1. Comparison between smart protection sources

BASIS OF COMPARISON	SMART PROTECTION SERVER	TREND MICRO SMART PROTECTION NETWORK
Availability	Available for internal clients, which are clients that meet the location criteria specified on the OfficeScan Web console.	Available for external clients, which are clients that do not meet the location criteria specified on the OfficeScan Web console.
Purpose	Designed and intended to localize smart protection services to the corporate network to optimize efficiency	A globally scaled, Internet-based infrastructure that provides smart protection services to clients who do not have immediate access to their corporate network
Server administrator	OfficeScan administrators install and manage these servers	Trend Micro maintains this server
Pattern update source	Trend Micro ActiveUpdate server	Trend Micro ActiveUpdate server
Client connection protocols	HTTP and HTTPS	HTTPS

Trend Micro Smart Protection Network

The Smart Protection Network are the Trend Micro maintained servers and in-the-client technologies that provides unique in-the-cloud correlation of Web and file reputation technologies, as well as 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.

Smart Protection Servers

Smart Protection Servers localize smart protection services to the corporate network for efficiency. There are two types of Smart Protection Servers:

Integrated Smart Protection Server

The OfficeScan Setup program includes an integrated Smart Protection Server that installs on the same computer where the OfficeScan server is installed. After the installation, manage settings for this server from the OfficeScan Web console.

Standalone Smart Protection Server

A standalone Smart Protection Server installs on a VMware or Hyper-V server. The standalone server has a separate management console and is not managed from the OfficeScan Web console.

Smart Protection 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 or Trend Micro Smart Protection Network during the verification process. Smart Protection Servers use several algorithms to ensure 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 sources. This file is updated hourly. OfficeScan clients that use smart scan (which is part of the File Reputation Service) do not download the Smart Scan Pattern. Smart scan clients verify potential threats against the pattern by sending reputation queries to the smart protection source. In the smart protection solution, clients send identification information determined by Trend Micro technology to smart protection sources. Clients never send the entire file and the risk of the file is determined using the identification information.
- **Smart Scan Agent Pattern**: This is the other pattern used by smart scan clients. This pattern is hosted on the OfficeScan clients' update source (the OfficeScan server or a customized update source) and downloaded by clients. This pattern is for scans that do not require queries to smart protection sources. This pattern is updated daily.
- **Web Blocking List**: Smart protection sources download this pattern from Trend Micro ActiveUpdate servers. This pattern is used for Web Reputation queries. OfficeScan clients that use Web reputation do not download the Web Blocking List. Clients verify potentially malicious websites against the blocking list by sending queries to a smart protection source. If the smart protection source determines that the Web site is safe, OfficeScan allows the user to access the site. However, if the site is potentially malicious, OfficeScan blocks access to the site.

Pattern Update Process

Pattern updates are a response to security threats. The ActiveUpdate server hosts the smart protection pattern files. Smart protection sources download the Smart Scan Pattern and Web Blocking List, while the OfficeScan clients' update source (which is the OfficeScan server by default), downloads the Smart Scan Agent Pattern and deploys this pattern to clients.

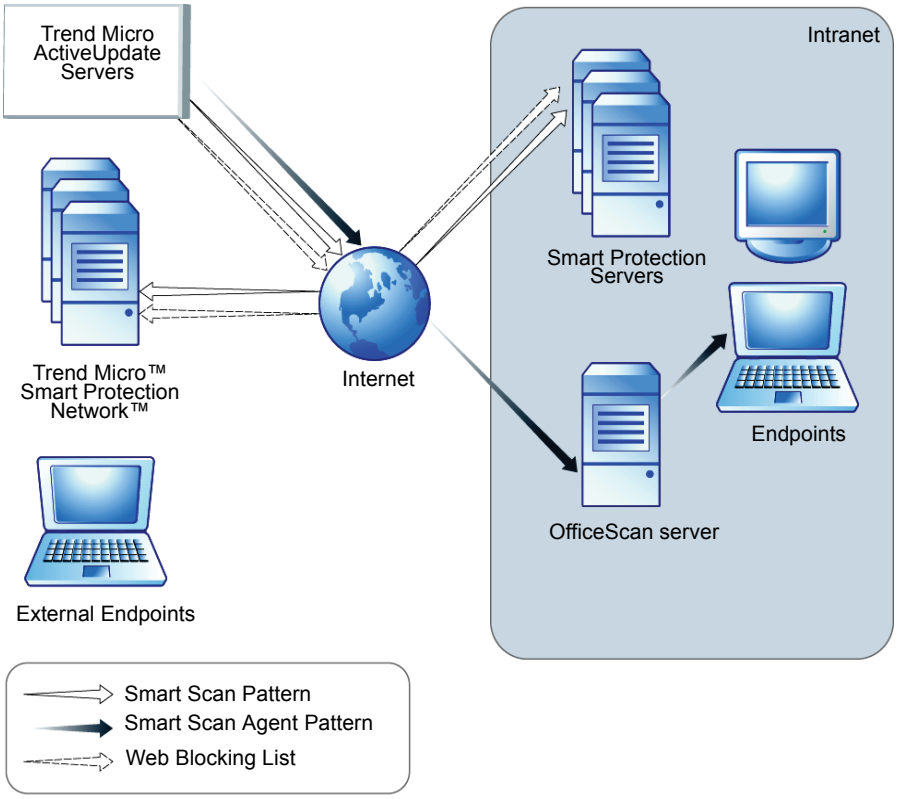


FIGURE 1-1. Pattern update process

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 the network still benefit from Trend Micro smart protection solutions through Smart Scan Agent Pattern and scan technology.

OfficeScan clients installed on endpoints first perform scanning on the endpoint. If the client cannot determine the risk of the file or URL, the client verifies the risk by sending a query to a Smart Protection Server. If Smart Protection Server cannot verify the risk of the file or URL, Smart Protection Server sends a query to Smart Protection Network.

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

LOCATION	PATTERN FILE AND QUERY BEHAVIOR
Access to intranet	• Pattern Files: Clients download the Smart Scan Agent Pattern file from the OfficeScan server. • File and Web Reputation Queries: Endpoints connect to Smart Protection Server for queries.
Without access to intranet but with connection to Smart Protection Network	• Pattern Files: Clients do not download the latest Smart Scan Agent Pattern file unless connection to an OfficeScan server is available. • File and Web Reputation Queries: Endpoints connect to Smart Protection Network for queries.
Without access to intranet and without connection to Smart Protection Network	• Pattern Files: Clients do not download the latest Smart Scan Agent Pattern file unless connection to an OfficeScan server is available. • File and Web Reputation Queries: Endpoints scan files using local resources such as the Smart Scan Agent Pattern.

Advanced filtering technology enables the client 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.

A client 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.

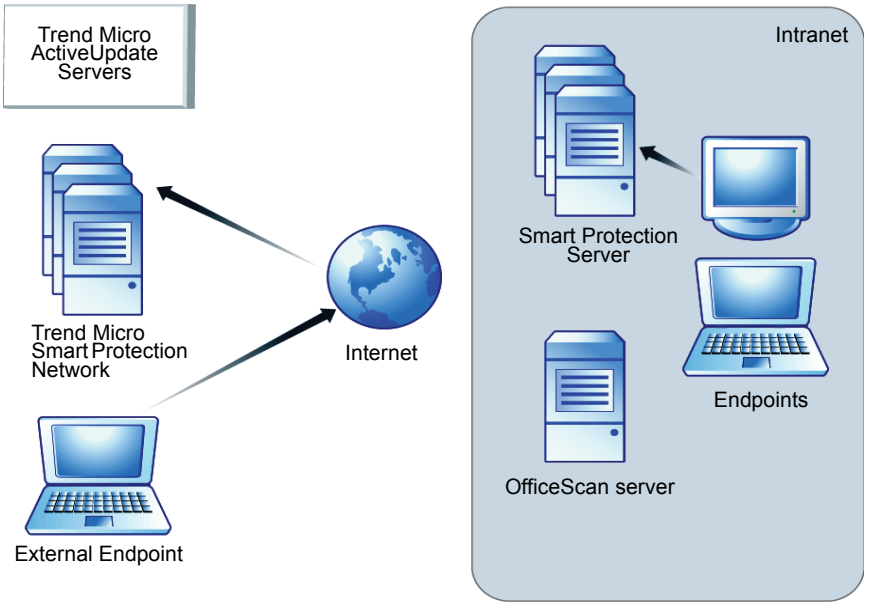


FIGURE 1-2. Query process

Features and Benefits

The following table lists the features and benefits.

TABLE 1-3. Features and benefits

FEATURES AND BENEFITS	
File Reputation Services	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 Services	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.

Chapter 2

Using Smart Protection Services

This chapter describes the necessary configurations and tasks to allow OfficeScan clients to use smart protection services.

Topics in this chapter:

Using File Reputation Services

The scan method that clients are using determines whether File Reputation Services can be leveraged.

OfficeScan clients must use **smart scan** as their scan method to leverage File Reputation Services.

Scan Methods

OfficeScan clients can use either conventional scan or smart scan when scanning for security risks.

Note: The default scan method in this release is smart scan. Change scan method settings from the **Scan Methods** screen at any time.

Conventional Scan

Conventional scan is the scan method used in all earlier OfficeScan versions. A conventional scan client stores all OfficeScan components on the client computer and scans all files locally.

Smart Scan

Smart scan is a next-generation, in-the-cloud based endpoint protection solution. At the core of this solution is an advanced scanning architecture that leverages threat signatures that are stored in-the-cloud.

Scan Methods Compared

The following table provides a comparison between these two scan methods:

TABLE 2-1. Comparison between conventional scan and smart scan

BASIS OF COMPARISON	CONVENTIONAL SCAN	SMART SCAN
Availability	Available in this and all earlier OfficeScan versions	Available starting from OfficeScan 10

TABLE 2-1. Comparison between conventional scan and smart scan (Continued)

BASIS OF COMPARISON	CONVENTIONAL SCAN	SMART SCAN

Scanning behavior	The conventional scan client performs scanning on the local computer.	• The smart scan client performs scanning on the local computer.
		• If the client cannot determine the risk of the file during the scan, the client verifies the risk by sending a scan query to a Smart Protection Server.
		• Using advanced filtering technology, the client "caches" the scan query result. The scanning performance improves because the client does not need to send the same scan query to the Smart Protection Server.
		• If a client cannot verify a file's risk locally and is unable to connect to any Smart Protection Server after several attempts:
		  • The client flags the file for verification.
		  • The client allows temporary access to the file.
		  • The client connects to the Trend Micro Smart Protection Network if the client's computer location is set to the default client connection status setting.
		• When connection to a Smart Protection Server is restored, all the files that have been flagged are re-scanned. The appropriate scan action is then performed on files that have been confirmed as infected.

TABLE 2-1. Comparison between conventional scan and smart scan (Continued)

BASIS OF COMPARISON	CONVENTIONAL SCAN	SMART SCAN
Components in use and updated	All components available on the update source, except the Smart Scan Agent Pattern	All components available on the update source, except the Virus Pattern and Spyware Active-monitoring Pattern
Typical update source	OfficeScan server	OfficeScan server

Scan Method as a Granular Setting

Scan method is a granular client tree setting, which means that it can be set on the root, domain, or individual client level.

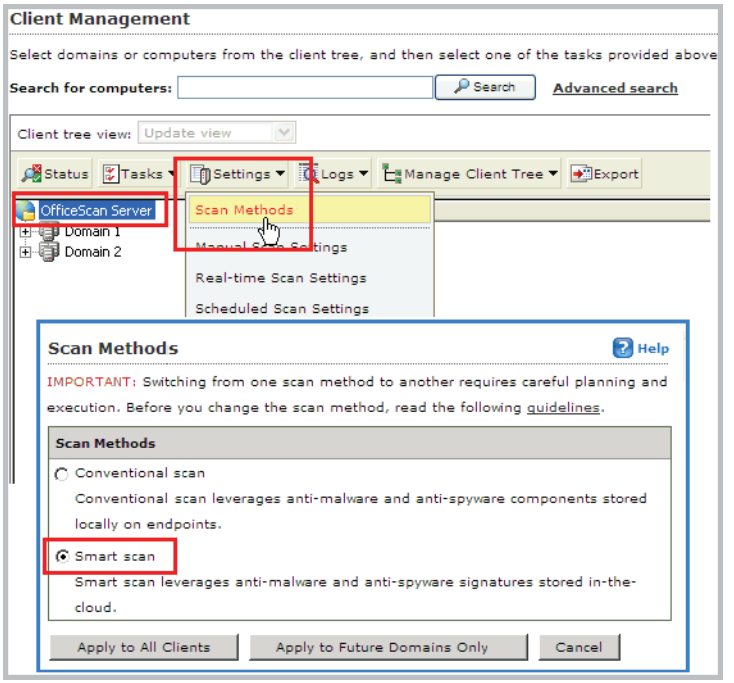


FIGURE 2-1. Smart scan as the root level scan method

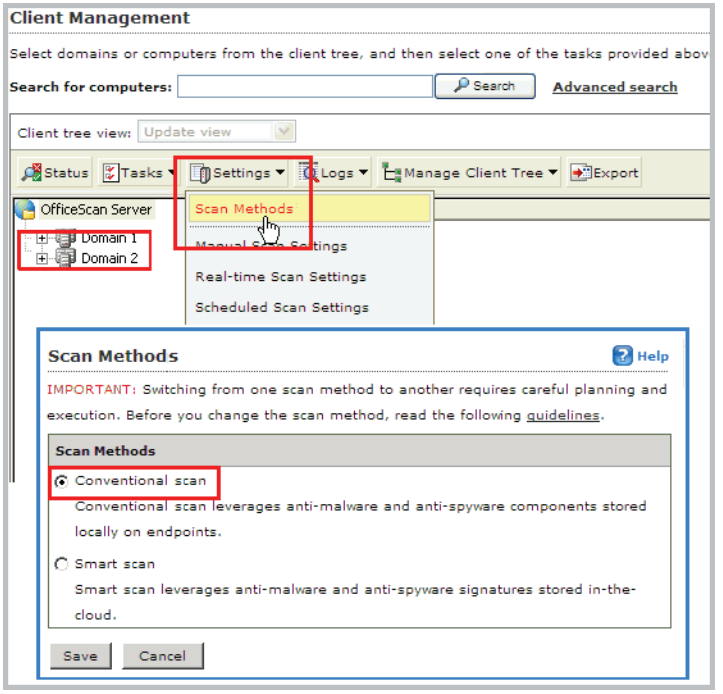


FIGURE 2-2. Conventional scan as the domain level scan method

When you configure the root level scan method, the setting automatically applies to all existing and future clients if you select **Apply to All Clients**. If you select **Apply to Future Domains Only**, the setting only affects domains (and the clients grouped under these domains) not yet added to the client tree.

After configuring the root level scan method, you can configure a client tree domain to use a different scan method. However, the domain level scan method will be overridden once you configure the root level scan method again and select **Apply to All Clients**. To avoid overriding the domain level scan method, select **Apply to Future Domains Only**.

You can also configure the scan method on an individual client. However, any changes to the domain or root level setting overrides the client's setting.

Default Scan Method

In this OfficeScan version, the default scan method for a fresh install is smart scan. This means that if you perform OfficeScan server fresh installation and did not change the scan method on the Web console, all clients that the server manages will use smart scan. However, if you upgrade the OfficeScan server from an earlier version and automatic client upgrade is enabled, all clients managed by the server will still use the scan method configured before the upgrade.

Scan Method Deployment Overview

This topic discusses how you can deploy smart scan to all or several clients.

To deploy smart scan efficiently, consider the following:

- The number of clients that will use smart scan. This affects how you configure smart scan settings on the Web console and the type/number of Smart Protection Servers to install.
- Features that are unavailable when clients use smart scan. If you have clients that need these features, do not configure the clients to use smart scan.

Number of Smart Scan Clients

The easiest way to deploy smart scan is by setting the root level scan method to smart scan and applying the setting to all existing and future clients. Use this deployment method if you want all clients to use smart scan.

If you have a client base that will use smart scan and conventional scan, determine which scan method will be used by a majority of clients.

Unavailable Features and Functions

The following OfficeScan features and functions are not available for smart scan clients:

- **Microsoft Outlook Mail Scan:** Microsoft Outlook email messages cannot be scanned if the client is using smart scan.
- **Policy Server for Cisco NAC:** smart scan clients cannot report Smart Scan Pattern and Smart Scan Agent Pattern information to the Policy Server.

Scan Method Deployment During Fresh Installation

On fresh installations, the default scan method for clients is smart scan. OfficeScan also allows you to customize the scan method for each domain after installing the server. Consider the following:

- If you did not change the scan method after installing the server, all clients that you install will use smart scan.
- If you want to use both conventional and smart scan, Trend Micro recommends retaining smart scan as the root level scan method and then changing the scan method on domains that you want to apply conventional scan.

Note: Refer to *Preparing the Smart Protection Solutions Environment* on page 3-2 for details on the environment required for clients to use smart scan.

- If you want to use conventional scan on all clients, change the root level scan method to conventional scan after installing the server.

Scan Method Deployment During Upgrade

If you upgrade OfficeScan from an earlier version, consider the following:

If Upgrading from OfficeScan 10.x

- If you plan to upgrade the OfficeScan 10.x server directly on the server computer, you do not need to make scan method changes from the Web console because clients will retain their scan method settings after they upgrade.

  For detailed upgrade instructions, see the *Installation and Upgrade Guide*.
- If you plan to upgrade OfficeScan 10.x clients by moving them to an OfficeScan10.5 server, follow these steps:
  - Prepare the OfficeScan 10.5 server. For details, see *Preparing the OfficeScan 10.5 Server* on page A-2.
  - Upgrade clients. For details, see *Upgrading OfficeScan 10.x Clients* on page A-4.

If Upgrading from OfficeScan 8.x/7.3

If you want all or most clients to use smart scan, deploy smart scan during the upgrade. The benefits of deploying smart scan during the upgrade are as follows:

- Reduces the deployment effort. You no longer need to switch clients from conventional scan to smart scan after clients upgrade.
- Reduces pattern updates and saves network bandwidth. If you deploy smart scan during client upgrade, the client downloads one new component needed for smart scan (Smart Scan Agent Pattern) but no longer needs to update the Virus Pattern and Spyware Active-monitoring Pattern. These two patterns are used only in conventional scan.

  If you did not deploy smart scan during the upgrade, the client updates the Virus Pattern and Spyware-active Monitoring Pattern. After you switch the client's scan method to smart scan, the client downloads the full version of the Smart Scan Agent Pattern.

Note: When switching to smart scan, the client only stops updating, but does not remove, the Virus Pattern and Spyware-active Monitoring Pattern. The client will update and use these patterns again if it switches back to conventional scan in the future.

When a smart scan client switches to conventional scan, the Smart Scan Agent Pattern is not removed.

The typical upgrade methods are as follows:

- *Upgrading the OfficeScan Server Directly on the Server Computer* on page 2-10
- *Moving Clients to an OfficeScan 10.5 server* on page 2-12

Upgrading the OfficeScan Server Directly on the Server Computer

If you plan to upgrade the OfficeScan 8.x/7.3 server directly on the server computer, deploy scan methods to clients during the upgrade by following these steps.

If all clients will use smart scan:

1. Prevent automatic updates and upgrade on clients.

   For details, see *Configuring Automatic Client Upgrade and Update Settings* on page A-9.

2. Upgrade the OfficeScan server.

   For details, see the *Installation and Upgrade Guide*.

3. Prepare the smart scan environment.

   For details, see *Preparing the Smart Protection Solutions Environment* on page 3-2.

4. Change the root level scan method to smart scan.

   For details, see *Configuring Scan Methods* on page A-1.

5. Upgrade clients.

   For details, see *Manually Upgrading Clients* on page A-7.

If most clients will use smart scan:

Trend Micro recommends performing the following tasks:

1. Prevent automatic updates and upgrade on clients.

   For details, see *Configuring Automatic Client Upgrade and Update Settings* on page A-9.

2. Upgrade the OfficeScan server.

   For details, see the *Installation and Upgrade Guide*.

3. Prepare the smart scan environment.

   For details, see *Preparing the Smart Protection Solutions Environment* on page 3-2.

4. Change the root level scan method to smart scan.

   For details, see *Configuring Scan Methods* on page A-1.

5. Upgrade clients (All clients will use smart scan).

   For details, see *Manually Upgrading Clients* on page A-7.

6. Change the scan method of clients that you want to use conventional scan.

   For details, see *Configuring Scan Methods* on page A-1.

If all clients will use conventional scan:

1. Upgrade the OfficeScan server.

   For details, see the *Installation and Upgrade Guide*.

2. Upgrade clients.

   For details, see *Manually Upgrading Clients* on page A-7.

Moving Clients to an OfficeScan 10.5 server

If you plan to upgrade clients by moving them to an OfficeScan 10.5 server, deploy scan methods to clients during the upgrade by following these steps.

If all clients will use smart scan:

1. Prepare the OfficeScan 10.5 server.

   For details, see *Preparing the OfficeScan 10.5 Server* on page A-2.

2. Prepare the smart scan environment.

   For details, see *Preparing the Smart Protection Solutions Environment* on page 3-2.

3. In the OfficeScan 8.x/7.3 server, move clients to the OfficeScan 10.5 server.

   For OfficeScan 8.x, see *Upgrading OfficeScan 8.x Clients* on page A-5.

   For OfficeScan 7.3, see *Upgrading OfficeScan 7.3 Clients* on page A-6.

If most clients will use smart scan:

1. Prepare the OfficeScan 10.5 server.

   For details, see *Preparing the OfficeScan 10.5 Server* on page A-2.

2. Prepare the smart scan environment.

   For details, see *Preparing the Smart Protection Solutions Environment* on page 3-2.

3. In the OfficeScan 8.x/7.3 server:
   - Identify which domains will apply smart scan and those that will apply conventional scan. For example, Domains A1, A2, and A3 will apply smart scan, and domains A4, A5, and A6 will apply conventional scan.
   - Ensure that OfficeScan 8.x/7.3 clients that you want to use smart scan are grouped under Domain A1, A2, or A3.
   - Ensure that OfficeScan 8.x/7.3 clients that you want to use conventional scan are grouped under Domain A4, A5, or A6.

4. In the OfficeScan 10.5 server:
   - Create Domains A1, A2, A3, A4, A5, and A6. Use the exact domain names.

     For details, see *Creating OfficeScan Domains* on page A-12.
   - Change the scan method of domains A4, A5, and A6 to conventional scan.

     For details, see *Configuring Scan Methods* on page A-1.
5. In the OfficeScan 8.x/7.3 server, move clients to the OfficeScan 10.5 server.

   For OfficeScan 8.x, see *Upgrading OfficeScan 8.x Clients* on page A-5.

   For OfficeScan 7.3, see *Upgrading OfficeScan 7.3 Clients* on page A-6.

If all clients will use conventional scan:

1. Prepare the OfficeScan 10.5 server.

   For details, see *Preparing the OfficeScan 10.5 Server* on page A-2.
2. In the OfficeScan 10.5 server, change the root level scan method to conventional scan.

   For details, see *Configuring Scan Methods* on page A-1.
3. In the OfficeScan 8.x/7.3 server, move clients to the OfficeScan 10.5 server.

   For OfficeScan 8.x, see *Upgrading OfficeScan 8.x Clients* on page A-5.

   For OfficeScan 7.3, see *Upgrading OfficeScan 7.3 Clients* on page A-6.

Using Web Reputation Services

To allow OfficeScan clients to use Web Reputation Services, ensure that the necessary environment has been set up properly. For details, see *Preparing the Smart Protection Solutions Environment* on page 3-2.

After setting up the environment, configure the following:

- *Web Reputation Policies* on page 2-14
- *Approved/Blocked URL Lists* on page 2-15

Web Reputation Policies

Web reputation policies dictate whether OfficeScan will block or allow access to a Web site. To determine the appropriate policy to use, OfficeScan checks the client's location. Location is based on either the client computer's gateway IP address or the client's connection status with the OfficeScan server or any reference server.

A client's location is "internal" if:

- The client's gateway IP address matches any of the gateway IP addresses specified on the Computer Location screen
- If the client can connect to the OfficeScan server or any of the reference servers. Otherwise, a client's location is "external".

To configure a Web reputation policy:

PATH: NETWORKED COMPUTERS > CLIENT MANAGEMENT > SETTINGS > WEB REPUTATION SETTINGS

1. Configure a policy for External Clients and Internal Clients.
2. Select the check box to enable/disable the Web reputation policy.

> **Tip:** Trend Micro recommends disabling Web reputation for internal clients if you already use a Trend Micro product with the Web reputation capability, such as InterScan Gateway Security Appliance.

3. Optionally enable the following:
   - **Assessment** (Internal/External): When in assessment mode, Web Reputation Service will allow all URLs but logs URLs that should have been blocked. Trend Micro provides assessment mode to allow you to evaluate URLs and then take appropriate action based on your evaluation.
   - **Use the Smart Protection Server Web Reputation Service** (Internal only): Internal clients connects to the Smart Protection Server and uses the Web Reputation Service to determine the status of the URL.

> **Note:** Ensure that there are several Smart Protection Servers on the smart protection source list to maintain Web reputation security. If the OfficeScan client is unable to connect to any Smart Protection Server, OfficeScan will allow access to the Website.

- **Use only Smart Protection Servers, do not send queries to Smart Protection Network** (Internal only): Internal clients connect only to the Smart Protection Servers and will not connect to the Smart Protection Network if the web reputation service is unable to determine the reputation of the URL.

4. Select from the available Web reputation security levels: **High**, **Medium**, or **Low**

   The security levels determine whether OfficeScan will allow or block access to a URL. For example, if you set the security level to Low, OfficeScan only blocks URLs that are known to be Web threats. As you set the security level higher, the Web threat detection rate improves but the possibility of false positives also increases.

5. Specify if you want to block Untested URLs.

   Untested URLs refer to URLs that have not been assessed by Trend Micro. While Trend Micro actively tests Web pages for safety, users may encounter untested pages when visiting new or less popular Web sites. Blocking access to untested pages can improve safety, but it also prevents access to safe pages.

6. Add URLs to the Approved/Blocked List, refer to page 2-16.

7. To submit Web reputation feedback, use the provided URL. The URL opens the Trend Micro Web Reputation Query system.

8. Select whether to allow the OfficeScan client to send Web Reputation Logs to the server. Allow clients to send logs if you want to analyze URLs being blocked by OfficeScan and take the appropriate action on URLs you think are safe to access.

9. Click Save.

Approved/Blocked URL Lists

Configure access to websites or block websites from being accessed. There are two kinds of URL lists that can be used:

- **Smart Protection Service Approved/Blocked List**: Smart Protection maintains this list from the Smart Protection Network. Trend Micro rates websites and determines if these should or should not be blocked, depending on the websites credibility. You can also export this .csv file to a Linux server.
- **Web Reputation Approved/Blocked URL List**: Specify websites that should or should not be accessed depending on the needs of your network. For example, you can block popular websites to ensure that users do not visit sites that do not pertain to work.

To import/export the Web Reputation Service Approved/Blocked list:

PATH: SMART PROTECTION > INTEGRATED SERVER

1. From the Web Service Approved/Blocked List section, do one of the following:
   - Export the list:
     i. Click **Export**. The Download page file appears.
     ii. Save the file.
   - Import the list:
     i. Click Import. The Import Web Reputation Service Approved/Blocked List screen appears.
     ii. Locate the .csv file.
     iii. Click Upload. The approved/blocked URLs display.

To add URLs to the Approved/Blocked URL list:

PATH: NETWORKED COMPUTERS > CLIENT MANAGEMENT > SETTINGS > WEB REPUTATION SETTINGS

Note: Separately add URLs to the External and Internal Clients.

1. Specify whether to enable the Approved or Blocked URL List feature.
2. Specify a URL in the text box.

   Note: Use the wildcard character (*) anywhere on the URL.

3. Select whether to approve or block the URL.
4. Repeat steps 2 to 3 until all the URLs you want to approve or block have been included in the list. The URL displays on the list.

Additional Tasks:

- To filter logs displayed, select either **Approved**, **Blocked**, or **Approved and Blocked**. The filtered URLs should immediately display.
- To export the list to a .csv file, click **Export** and then click **Save**.
- If you have exported a list from another server and want to import it to this screen, click **Import** and locate the .dat file. The list loads on the screen.

Chapter 3

Smart Protection Solutions Environment

This chapter describes how to set up the environment required to use Trend Micro™ smart protection solutions.

Topics in this chapter:

Preparing the Smart Protection Solutions Environment

Before clients can leverage smart protection solutions, ensure that the environment has been properly set up. Check the following:

1. Smart protection sources

   Clients connect to a smart protection source to send reputation queries and verify a file's risk against the Smart Scan Pattern. The smart protection source depends on the client's location. *Internal* clients connect to a Smart Protection Server, while *external* clients connect to the Trend Micro Smart Protection Network.

   Set up one or several Smart Protection Servers. See *Installing Smart Protection Servers* on page 3-3 for details.

2. Client connection proxy settings

   If connection to the Smart Protection Network requires proxy authentication, specify authentication credentials. For details, see *External Proxy Settings* on page 3-38.

   Configure internal proxy settings clients will use when connecting to a Smart Protection Server. See *Internal Proxy Settings* on page 3-38 for details.

3. Smart Protection Server list

   Add the Smart Protection Servers you have set up to the Smart Protection Server list. Clients refer to the list to determine which Smart Protection Server to connect to for scan or web reputation queries. See *Smart Protection Server List* on page 3-39 for details.

4. Computer location settings

   OfficeScan includes a location awareness feature that identifies the client computer's location and determines whether the client connects to the Smart Protection Network or Smart Protection Server. This ensures that clients remain protected regardless of their location.

   To configure location settings, see *Computer Location Settings* on page 3-44.

5. Other Trend Micro products

   If you have Trend Micro™ Network VirusWall™ Enforcer installed:

   - Install a hot fix (build 1047 for Network VirusWall Enforcer 2500 and build 1013 for Network VirusWall Enforcer 1200).
   - Update the OPSWAT engine to version 2.5.1017 to enable the product to detect a client's scan method.

Installing Smart Protection Servers

There are two types of Smart Protection Servers.

Integrated Smart Protection Server

The OfficeScan Setup program includes an integrated Smart Protection Server that installs on the same computer where the OfficeScan server is installed. After the installation, manage settings for this server from the OfficeScan Web console.

Standalone Smart Protection Server

A standalone Smart Protection Server installs on a VMware server. The standalone server has a separate management console and is not managed from the OfficeScan Web console.

Recommendations

Install several Smart Protection Servers for failover purposes. Clients that are unable to connect to a particular server will try to connect to the other servers you have set up. Assign a standalone Smart Protection Server as the primary scan source and the integrated server as a backup. This reduces the reputation query traffic directed to the computer that hosts the OfficeScan server and integrated server. The standalone server can also process more reputation queries. See *Performance Considerations* on page 3-4 for details.

Installation Guidelines

Consider the following when setting up Smart Protection Servers:

- Smart Protection Server is a CPU-bound application. This means that increasing CPU resources increases the number of simultaneous requests handled.
- Network bandwidth may become a bottleneck depending on network infrastructure and the number of simultaneous update requests or connections.
- Additional memory might be required if there is a large number of concurrent connections between Smart Protection Servers and endpoints.

Performance Considerations

- Because the integrated Smart Protection Server and the OfficeScan server run on the same computer, the computer's performance may reduce significantly during peak traffic for the two servers. Consider using standalone Smart Protection Servers as the primary smart protection source for clients and the integrated server as a backup.
- OfficeScan clients registered to the same OfficeScan server use the corresponding Smart Protection Server.
- If you install the integrated Smart Protection Server, consider disabling the OfficeScan firewall. The OfficeScan firewall is intended for client computer use and may affect performance when enabled on server computers. See the *Administrator's Guide* for information on disabling the OfficeScan firewall.

Note: Consider the effects of disabling the firewall and ensure that it adheres to your security plans.

Best Practices

- Avoid performing Manual scans and Scheduled scans simultaneously. Stagger the scans in groups.
- Avoid configuring all endpoints from performing Scan Now simultaneously. (For example, the "Perform scan now after update" option.)
- Install multiple Smart Protection Servers to ensure the continuity of protection in the event that connection to a Smart Protection Server is unavailable.
- Customize Smart Protection Server for slower network connections, about 512Kbps, by making changes to the `ptngrowth.ini` file.

  For the standalone server:

  a. Open the `ptngrowth.ini` file in `/var/tmcss/conf/`.

  b. Modify the `ptngrowth.ini` file using the recommended values below:

  ```
  [COOLDOWN]
  ENABLE=1
  MAX_UPDATE_CONNECTION=1
  UPDATE_WAIT_SECOND=360
  ```

  c. Save the `ptngrowth.ini` file.

  d. Restart the `lighttpd` service by typing the following command from the Command Line Interface (CLI):

  ```
  service lighttpd restart
  ```

  For the integrated server:

  a. Open the `ptngrowth.ini` file in <Server installation folder>`\PCCSRV\WSS\`.

  b. Modify the `ptngrowth.ini` file using the recommended values below:

  ```
  [COOLDOWN]
  ENABLE=1
  MAX_UPDATE_CONNECTION=1
  UPDATE_WAIT_SECOND=360
  ```

  c. Save the `ptngrowth.ini` file.

  d. Restart the `Trend Micro Smart Protection Server` service.

Installing the Standalone Smart Protection Server

The standalone Smart Protection Server installation process formats your existing system for program installation. VMware or Hyper-V installation requires the creation of a virtual machine before installation.

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

You need the following information for the installation:

- Proxy server information
- A virtual machine server that fulfills the requirements for your network

What's New in the Standalone Smart Protection Server

The following table is a list of new features in this release of the standalone Smart Protection Server:

TABLE 3-1. What's new in this release

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.
Logs	This version of Smart Protection Server includes logs for monitoring activity.
Notifications	This version of Smart Protection Server includes notifications for events.

Standalone Smart Protection Server Requirements

For the standalone Smart Protection Server, the following are required:

TABLE 3-1. Standalone Smart Protection Server requirements

HARDWARE / SOFTWARE	REQUIREMENTS
Hardware	• 2.0GHz Intel® Core2Duo™ 64-bit processor supporting Intel® Virtualization Technology™ or equivalent • 1GB RAM (1.5GB RAM recommended) • 10GB disk space for minimum virtualization requirements (20GB recommended for virtualization requirements if fewer than 1000 endpoints. Add 15GB for every 1000 endpoints.) **Note:** Smart Protection Server automatically partitions the detected disk space as required. • Monitor with 800 x 600 or greater resolution with 256 colors or higher
Virtualization	• Microsoft® Windows Server® 2008 R2 Hyper-V™ (Legacy Network Adapter is required to detect the network device for Hyper-V installations.) **Note:** After installing Smart Protection Server, use the Command Line Interface (CLI) to enable Hyper-V Integration Components to increase capacity. • VMware® ESXi™ Server 4.0 or 3.5 • VMware® ESX™ Server 4.0, 3.5, or 3.0 • VMware® Server 2.0 **Note:** A purpose-built, hardened, performance-tuned 64-bit Linux operating system is included with Smart Protection Server.

TABLE 3-1. Standalone Smart Protection Server requirements (Continued)

HARDWARE / SOFTWARE	REQUIREMENTS
Virtual Machine	• Red Hat® Enterprise Linux® 5 64-bit (Guest Operating System) • 1GB RAM (1.5GB RAM recommended) • 2.0GHz processor • 10GB disk space (20GB recommended for fewer than 1000 endpoints. Add 15GB for every 1000 endpoints.) • 1 network device • 2 virtual processors • Network Device **Note:** Install VMware Tools after successfully installing Smart Protection Server. If installing with minimum requirements, disable Web Access Log from the Command Line Interface (CLI).
Web Console	• Microsoft® Internet Explorer® 7.0 or later with the latest updates • Mozilla® Firefox® 3.6.0 or later • Adobe® Flash® Player 8.0 or above is required for viewing graphs in widgets • 1024 x 768 or greater resolution with 256 colors or higher

Performing a Fresh Installation

After preparing the requirements for installation, run the installation program to begin installation.

To install Smart Protection Server:

1. Create a virtual machine on your VMware or Hyper-V server and specify the virtual machine to boot from the Smart Protection Server ISO image. Refer to the Virtual Machine section in *Standalone Smart Protection Server Requirements* on page 3-7 for more information about the type of virtual machine required for installation.

   Note: A Legacy Network Adapter is required to detect the network device for Hyper-V installations.

2. Power on the virtual machine. The Installation Menu displays with the following options:
   - **Install Smart Protection Server**: Select this option to install Smart Protection Server to the new virtual machine.
   - **System Memory Test**: Select this option to perform memory diagnostic tests to rule out any memory issues.
   - **Exit Installation**: Select this option to exit the installation process and to boot from other media.

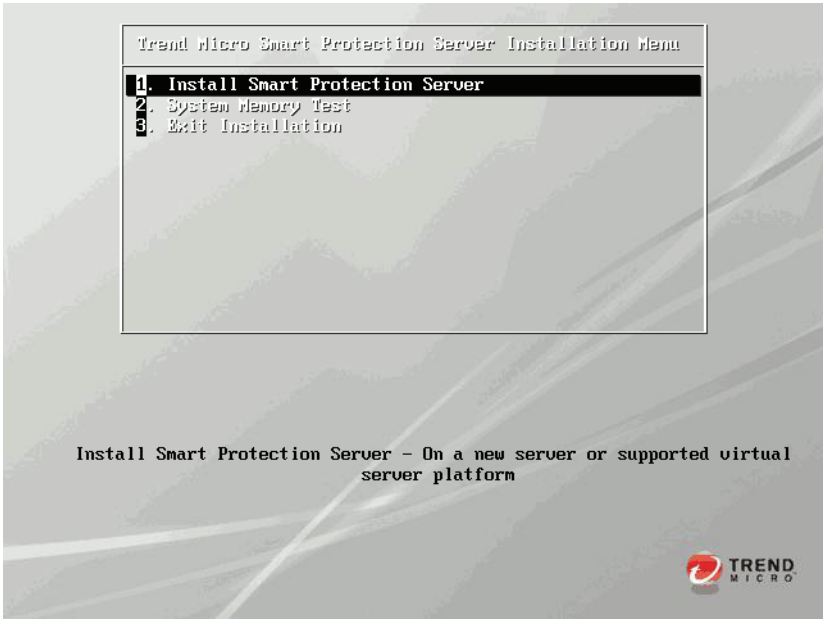


FIGURE 3-1. Installation Menu screen

3. Select **Install Smart Protection Server**. The Select language screen appears.
4. Select the language for this installation of Smart Protection Server and click **Next**. The License Agreement screen appears.

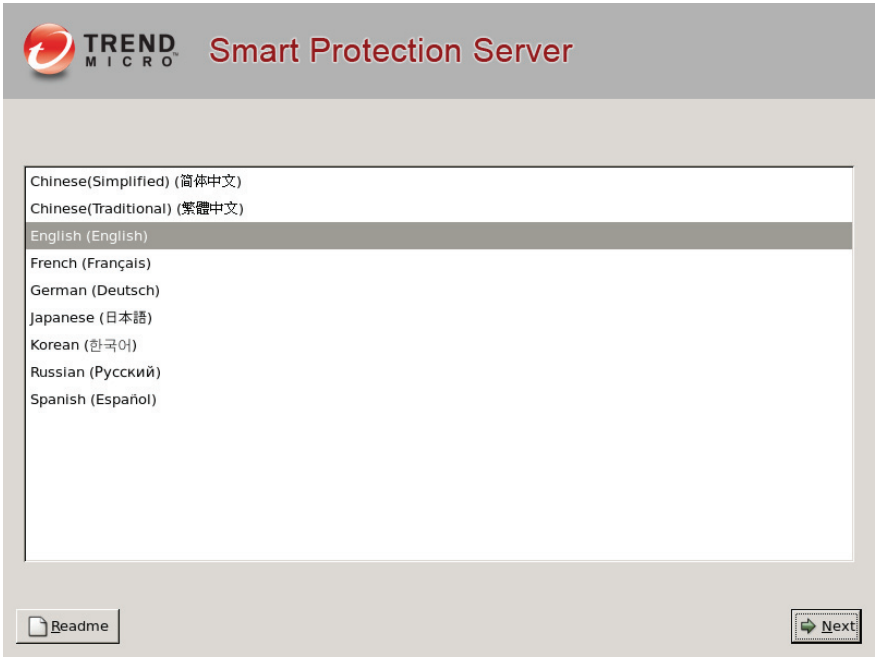


FIGURE 3-2. Select language screen

Note: From this screen on, you can access the readme from a button in the lower left hand corner of the installation screen.

5. Click **Accept** to continue. The Keyboard Selection screen appears.

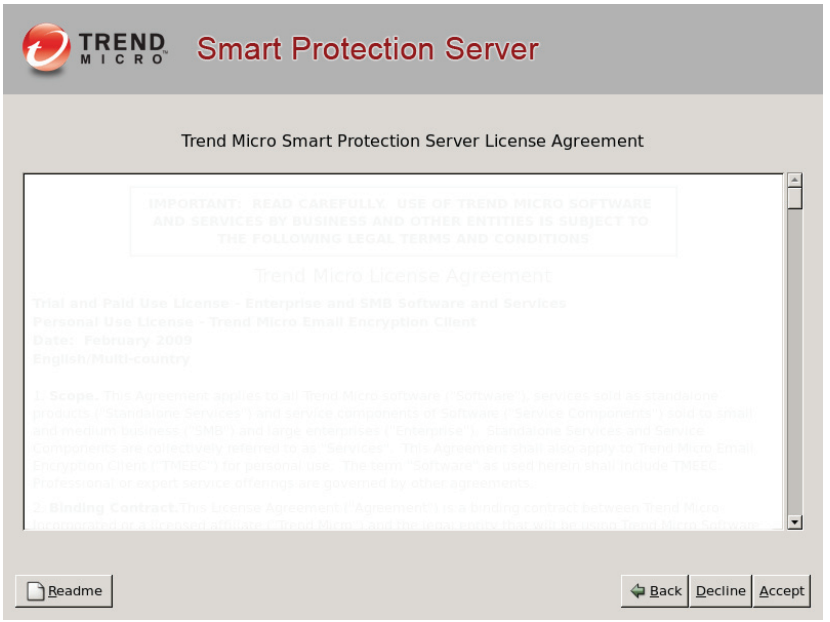


FIGURE 3-3. License Agreement screen

6. Select the keyboard language and click **Next** to continue. The Hardware Components Summary screen appears.

   The installation program performs a scan to determine if the system specifications have been met and displays the results. If the hardware contains components that do not meet the system requirements, the installation program highlights those components. Installation can proceed as long as there is a hard drive and network device. If there is no hard drive or no network device, installation cannot continue.

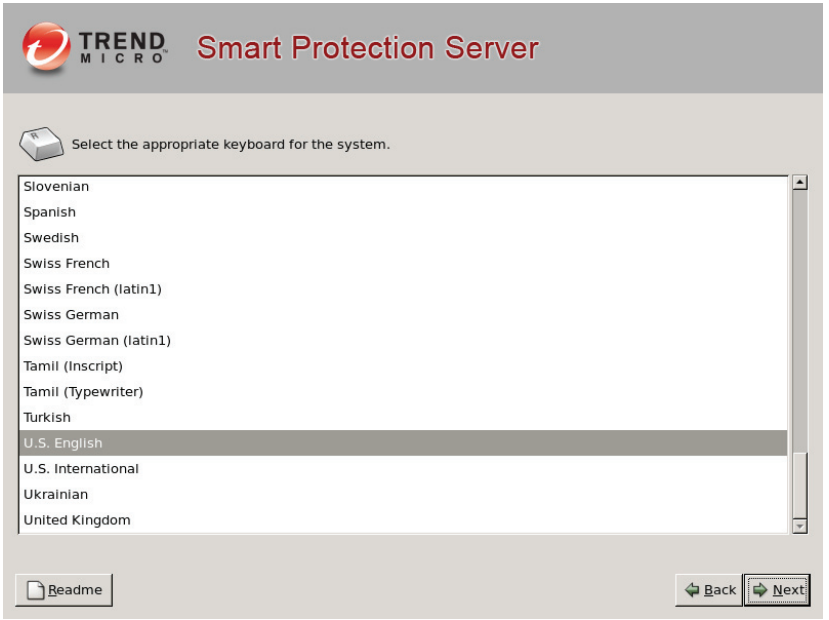


FIGURE 3-4. Keyboard Selection screen

7. Click **Next** to continue. The Network Settings screen appears.

   If there are multiple network devices, configure settings for all devices. (Only one device can be active on boot.)

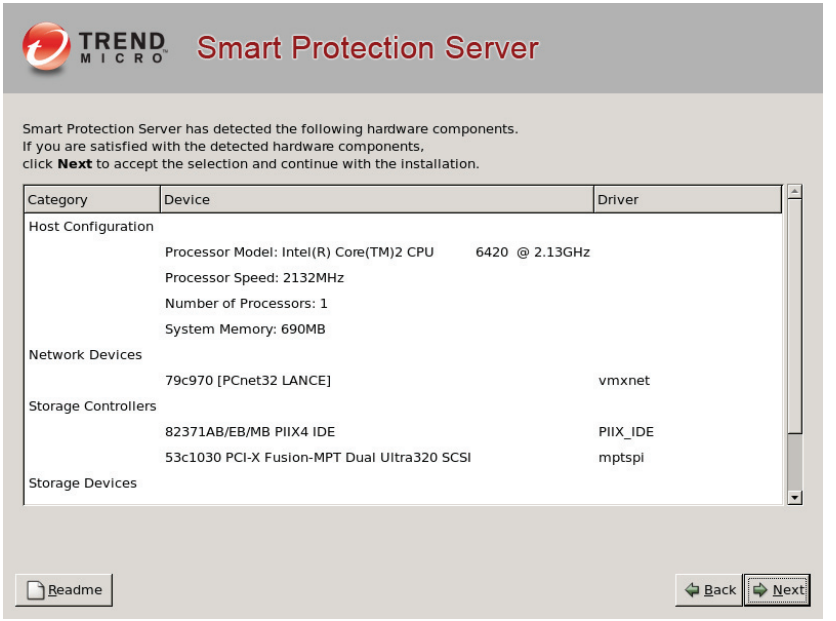


FIGURE 3-5. Hardware Components Summary screen

8. Configure network settings.

   a. Specify the Active on Boot network devices, host name, and miscellaneous settings.

      The **Edit** button allows you to configure IPv4 settings, the default setting is DHCP. Click **Edit** to select manual configuration and configure miscellaneous settings.

   b. Click **Next** to continue. The Time Zone screen appears.

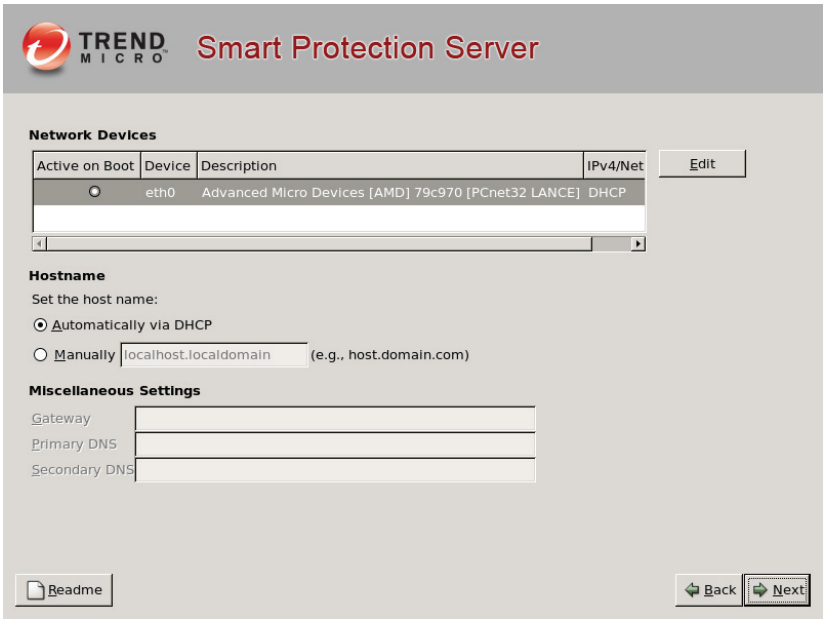


FIGURE 3-6. Network Settings screen

Note: To change the active on boot device after installation, log on to the Command Line Interface (CLI).

---

9. Specify the time zone and click **Next** to continue. The Authentication screen appears.

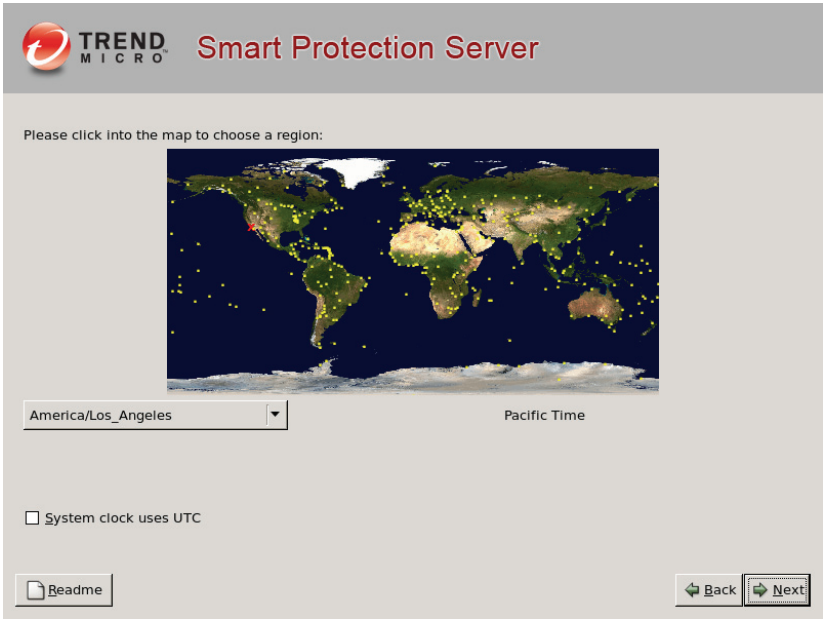


FIGURE 3-7. Time Zone screen

10. Specify passwords. Smart Protection Server uses two different levels of administrator types to secure the server.
    a. Type the "root" and "admin" passwords. The password must be a minimum of 6 characters and a maximum of 32 characters.

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.

- **Root account**: This account is used to gain access to the operating system shell and has all rights to the server. This account includes the most privileges.
- **Admin account**: This account is the default administration account used to access the Smart Protection Server web and CLI product consoles. This account includes all rights to the Smart Protection Server application, but does not include access rights to the operating system shell.

b. Click **Next** to continue. The Installation Summary screen appears.

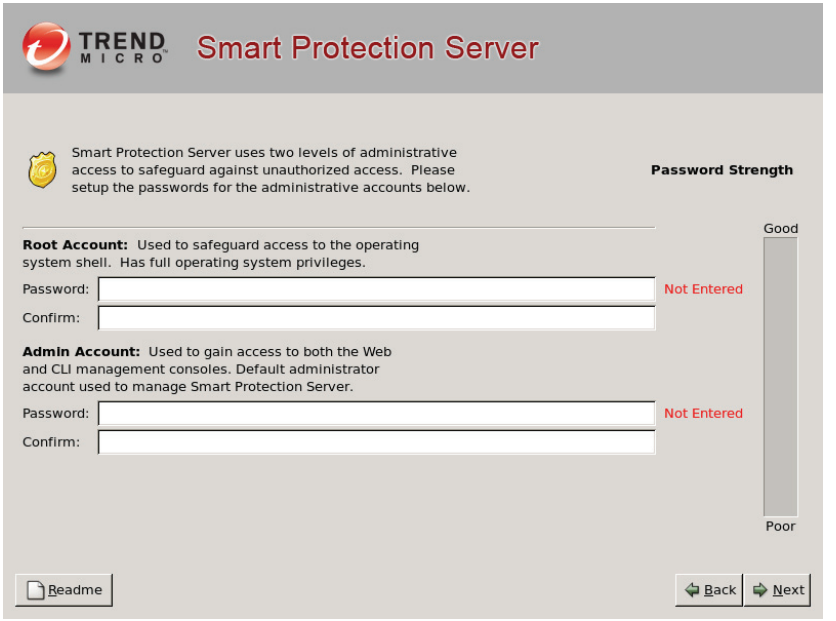


FIGURE 3-8. Authentication screen

11. Confirm the summary information.

a. Review the summary information on this screen.

Note: Continuing with the installation formats and partitions the necessary disk space and installs the operating system and application. If there is any data on the hard disk that cannot be erased, cancel the installation and back up the information before proceeding.

---

b. If any of the information on this screen requires a different configuration, click **Back**. Otherwise, click **Next** to continue and click **Continue** at the confirmation message. The Installation Progress screen appears.

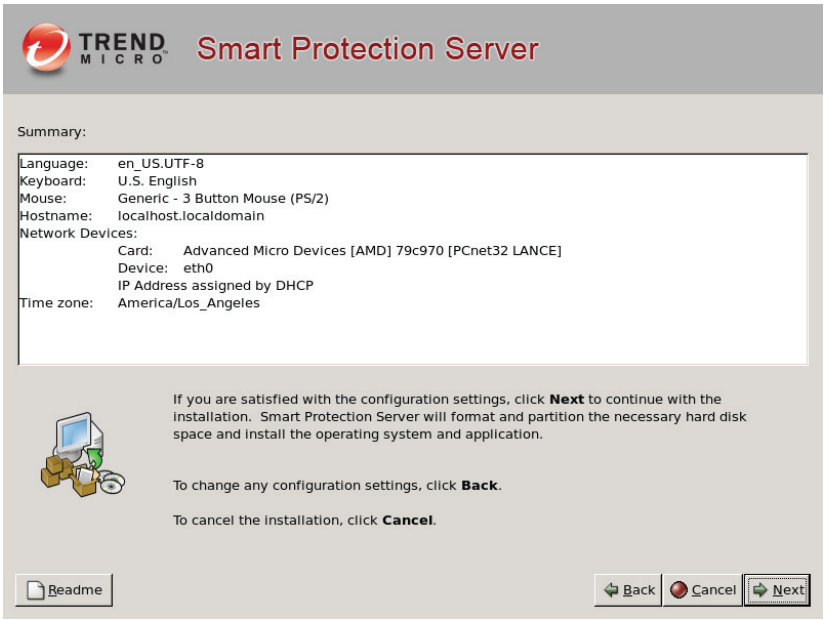


FIGURE 3-9. Installation Summary screen

12. A message appears when the installation completes. The installation log is saved in the `/root/install.log` file for reference.

FIGURE 3-10. Installation Progress screen

13. Click **Reboot** to restart the virtual machine. The initial product Command Line Interface (CLI) logon screen appears and displays the client connection addresses and the web console URL.

Tip: Trend Micro recommends disconnecting the CD ROM device from the virtual machine after Smart Protection Server is installed.

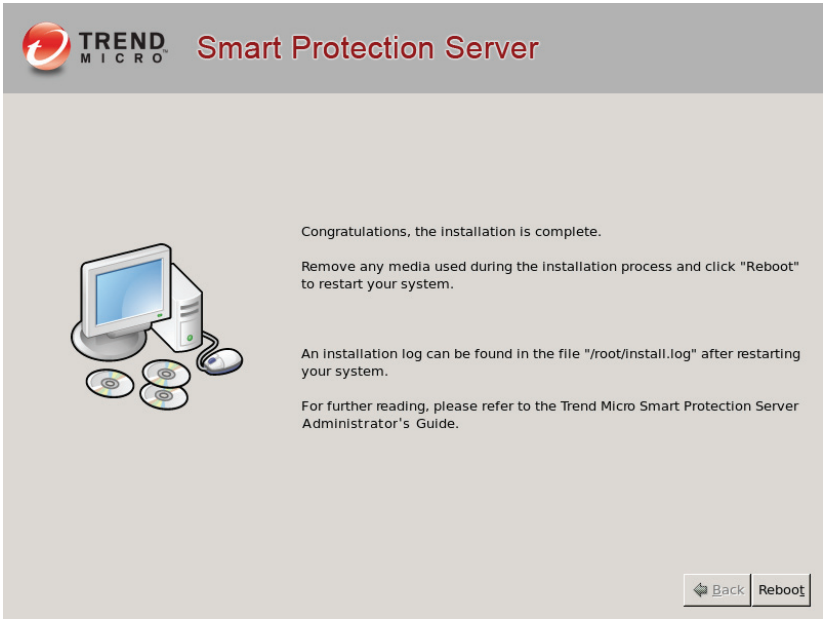


FIGURE 3-11. Installation Complete screen

14. Use `admin` to log on to the product CLI or the web console to manage Smart Protection Server. Log on to the web console to perform post installation tasks such as configuring proxy settings. Log on to the CLI shell if you need to perform additional configuration, troubleshooting, or maintenance tasks.

Note: Use `root` to log on to the operating system shell with full privileges.

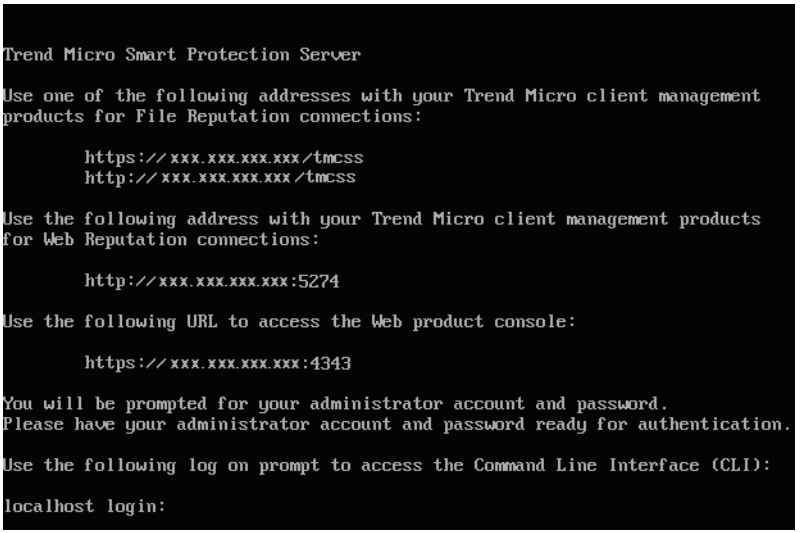


FIGURE 3-12. CLI logon screen

15. Perform post installation tasks. See Post Installation on page 3-24.

Upgrading the Standalone Smart Protection Server

Upgrade to this version of Smart Protection Server from Smart Scan Server 1.0 or Smart Scan Server 1.0 with Service Pack 1.

TABLE 3-2. Version upgrade details

VERSION	REQUIREMENTS
Upgrading to Smart Protection Server 2.0	• Ensure that System Requirements are met before installation. See *Installation Guidelines* on page 3-4. • Smart Scan Server 1.1 Build 8888 • Clear the browsers temporary Internet files before logging on to the web console.
Upgrading to Smart Scan Server 1.1 to Build 8888	• Upgrade to Smart Scan Server 1.1 Build 8888 from previous build versions of Smart Scan Server 1.1 and Smart Scan Server 1.0. • Wait 40 seconds while the web service restarts after installation before logging on. **Note:** When upgrading from Smart Scan Server 1.0, change the port number and clear the browser cache to connect to the web console.

Note: The web service is disabled for about 5 minutes during the upgrade process. During this time, endpoints will not be able to send queries to Smart Protection Server. Trend Micro recommends redirecting endpoints to another Smart Protection Server for the duration of the upgrade. If there is only one Smart Protection Server installed on your network, Trend Micro recommends planning the upgrade for off-peak times. Suspicious files will be logged and scanned immediately once connection to Smart Protection Server is restored.

To upgrade Smart Protection Server:

1. Log on to the web console.
2. Click **Updates** from the main menu. A drop down menu appears.
3. Click **Program**. The Program screen appears.
4. Under Upload Component, click **Browse**. The Choose File to Upload screen appears.
5. Select the upgrade file from the Choose File to Upload screen.
6. Click **Open**. The Choose File to Upload screen closes and the file name appears in the **Upload program package** text box.
7. Click **Update**.

After upgrading to Smart Protection Server 2.0, perform post installation tasks. See *Post Installation* on page 3-24.

Post Installation

Trend Micro recommends performing the following post-installation tasks:

- After installing Smart Protection Server, install VMware™ Tools. Refer to VMware documentation for more information.
- After installing Smart Protection Server with Hyper-V, enable Hyper-V Integration Components to increase capacity. Ensure that a Network Adapter is available before enabling Hyper-V Integration Components. Enable Hyper-V Integration Components from the Command Line Interface (CLI) with your admin account by typing:

  ```
  enable
  ```

  ```
  enable hyperv-ic
  ```

- If you installed with minimum system requirements, disable the Web Access Log from the Command Line Interface (CLI) with your admin account by typing:

  ```
  enable
  ```

  ```
  disable adhoc-query
  ```

- Perform initial configuration. See Client Proxy Settings on page 3-38.
- Configure Smart Protection Server settings on other Trend Micro products that support smart protection solutions.

Note: The Real Time Status widget and Smart Protection Server CLI console display Smart Protection Server addresses.

Initial Configuration

Perform the following tasks after installation or upgrading:

1. Log on to the web console. The first time installation wizard appears.
2. Select the **Enable File Reputation Service** check box to use File reputation.

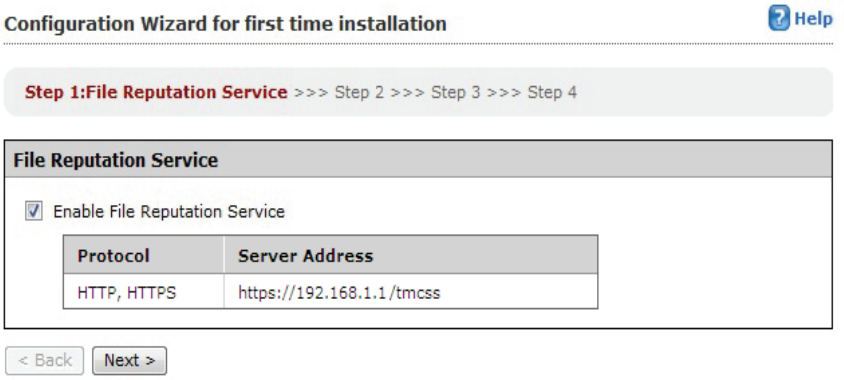


FIGURE 3-13. Configure File Reputation Settings

3. Click **Next**. The Web Reputation Service screen appears.

4. Select the **Enable Web Reputation Service** check box to enable Web Reputation.

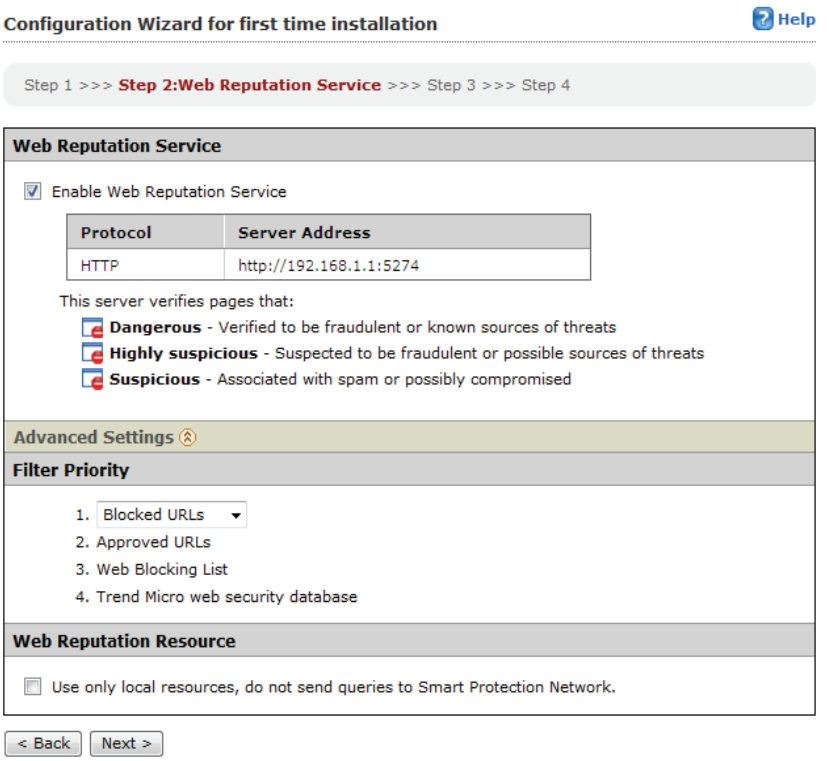


FIGURE 3-14. Configure Web Reputation Settings

5. (Optional) Click **Advanced Settings** to configure the filter priority and resource settings. The filter priority settings allow you to specify the filter order for URL queries. The resource setting option allows you to prevent queries from being sent outside of your network.

6. Click **Next**. The Smart Feedback screen appears.

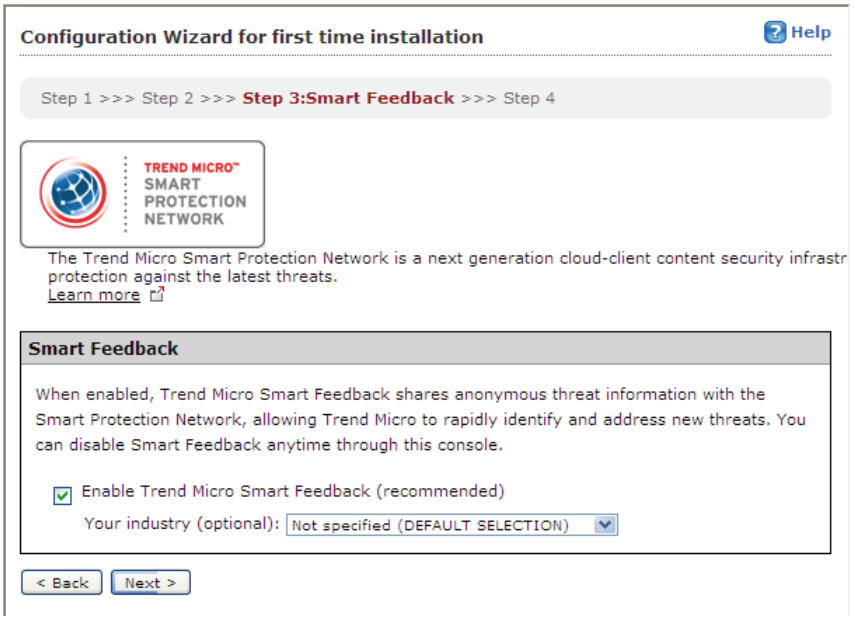


FIGURE 3-15. Smart Feedback

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

8. Click **Next**. The Proxy Settings screen appears.

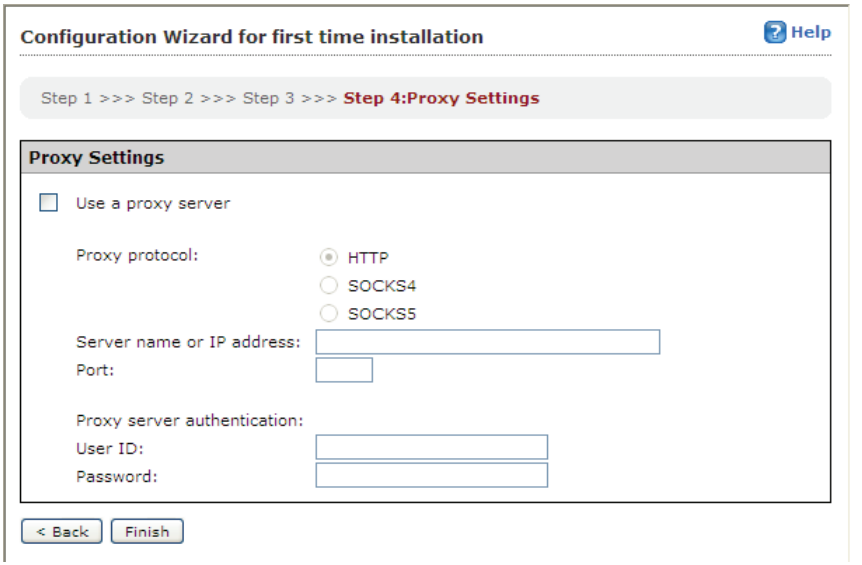


FIGURE 3-16. Proxy Settings

9. Specify proxy settings if your network uses a proxy server.
10. Click **Finish** to complete the initial configuration of Smart Protection Server. The Summary screen of the web console displays.

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

Using Smart Protection Services

This version of standalone 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. A brief description of the available options is below.

- **Enable File Reputation Service**: Select to support File Reputation queries from endpoints.
- **Server Address**: Used by other Trend Micro products that support File Reputation queries.

To enable File Reputation:

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 OfficeScan servers.

Web Reputation

Enable Web Reputation to support URL queries from endpoints. A brief description of the available options is below.

- **Enable Web Reputation Service**: Select to support Web Reputation queries from endpoints.
- **Server Address**: Used by other Trend Micro products for Web Reputation queries.
- **Edit Proxy Settings**: Click to navigate to the Administration > Proxy Settings screen to configure proxy settings if your network uses a proxy server.
- **Advanced Settings**: Click to display the Approved/Blocked URL List and Resource settings.
- **Filter Priority**: Select to specify the priority when filtering URLs.
- **Use only local resources, do not send queries to Smart Protection Network**: Select to keep all queries in the company network.

To enable Web Reputation:

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 Approved/Blocked URL List when filtering URLs.
5. (Optional) Select **Use only local resources, do not send queries to Smart Protection Network** to keep all queries within the local intranet.
6. Click **Save**.

Using the Approved/Blocked URL List

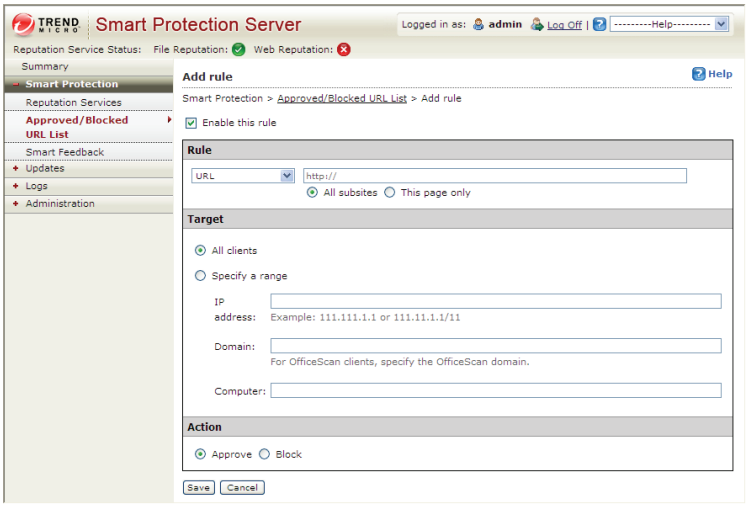
The Approved/Blocked URL List allows you to specify a custom list of approved and/or blocked URLs. This list is used for Web Reputation. A brief description of the available options is below.

- **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://`.

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

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**.

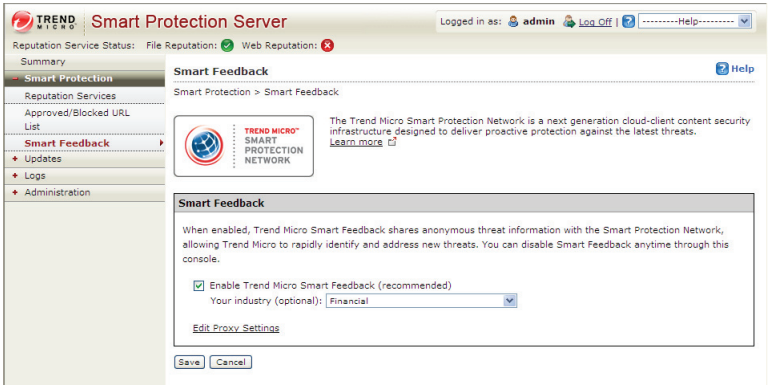
Using Smart Feedback

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:

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**.

Installing the Integrated Smart Protection Server

The integrated Smart Protection Server installs with the OfficeScan server. For installation requirements and instructions, see the *OfficeScan Installation and Upgrade Guide*.

Take note of the following when installing the integrated server:

Licenses

During the installation, activate the licenses for the following services to use smart protection services in the integrated Smart Protection Server:

- Antivirus
- Web Reputation and Anti-spyware

If you do not activate the licenses, you can still install the integrated Smart Protection Server but clients will not be able to use smart protection or connect to any Smart Protection Server. Contact your Trend Micro representative for license and activation concerns.

Number of Clients

You can use the integrated or standalone Smart Protection Server if the number of clients connecting to the server is 1,000 or less. However, Trend Micro recommends using the standalone Smart Protection Server if there are more than 1,000 smart scan clients.

Client Connection Protocols

Clients can connect to the integrated server using HTTP and HTTPS protocols, depending on the services. HTTPS allows for a more secure connection while HTTP uses less bandwidth.

File Reputation Services can connect to both HTTP and HTTPS, while Web Reputation Services can only connect to HTTP protocols.

The SSL port number used for secure connections depends on the Web server (Apache or IIS) used by the OfficeScan server. See the *OfficeScan Installation and Upgrade Guide* for more information on OfficeScan Web servers.

TABLE 3-3. SSL port numbers for the OfficeScan server and integrated Smart Protection Server

OFFICESCAN WEB SERVER SETTINGS	OFFICESCAN SERVER SSL PORT	INTEGRATED SMART PROTECTION SERVER SSL PORT
Apache Web server with SSL enabled	4343	4343
Apache Web server with SSL disabled	N/A	4345
IIS default Web site with SSL enabled	443	443
IIS default Web site with SSL disabled	N/A	443
IIS virtual Web site with SSL enabled	4343	4345
IIS virtual Web site with SSL disabled	N/A	4345

Verifying Integrated Smart Protection Server Installation

OfficeScan automatically installs the integrated Smart Protection Server during a fresh installation.

To verify the integrated Smart Protection Server installation:

1. On the OfficeScan server Web console, navigate to **Smart Protection > Smart Protection Sources**.
2. Click the **standard list** link.
3. On the screen that opens, click **Integrated Smart Protection Server**.
4. On the screen that displays, click **Test Connection**. Connection with the integrated server should be successful.

Using Smart Protection Services

By default, OfficeScan installs the integrated Smart Protection Server during OfficeScan server fresh installation. For upgrades, you can enable the File Reputation Services and Web Reputation Services if you want to use the integrated Smart Protection Server in your smart protection environment.

To enable the Smart Protection Services:

1. On the OfficeScan server Web console, navigate to **Smart Protection > Integrated Server**.
2. Select the **Use the Integrated File Reputation Service** option to enable the smart scan technology.
3. Select the **Use the Integrated Web Reputation Service** option to enable the URL Filtering technology.
4. Click **Save**.

Integrated Smart Protection Server Reactivation

If you are upgrading from OfficeScan 10.x and you did not install the integrated Smart Protection Server but now want to use it in your smart protection environment, reactivate the server by performing the following steps.

To reactivate the integrated Smart Protection Server:

1. Open Microsoft Management Console and stop the OfficeScan Master Service.
2. Open a command prompt and navigate to <Server installation folder>\PCCSRV.
3. Run the following command:

   ```
   SVRSVCSETUP.EXE -uninstall
   ```

   This command uninstalls OfficeScan-related services but does not remove configuration files and the OfficeScan database.
4. Navigate to <Server installation folder>\PCCSRV\private and open **ofcserver.ini**. Modify the following settings as follows:

   ```
   WSS_INSTALL=1
   WSS_ENABLE=1
   WSS_URL=https://<computer_name>:<SSL port>/tmcss/
   WSS_HTTP_URL=http://<computer_name>:<HTTP port>/tmcss/
   ```
5. Navigate to <Server installation folder>\PCCSRV and open **OfUninst.ini.** Modify the following lines as follows:
   - If using IIS Web server:

     ```
     [WSS_VIRDIR_INFO]
     ROOT=/tmcss,<Server installation
     folder>\PCCSRV\WSS\isapi,,5
     [WSS_WEB_SERVER]
     ServerPort=8082
     IIS_VhostName=Smart Protection Server (Integrated)
     IIS_VHostIdx=<VALUE>
     ```

     Note: The value for IIS_VHostidx should be the same as the "isapi" value indicated on the following line:

     ROOT=/tmcss,<Server installation folder>\PCCSRV\WSS\isapi,,<value>

     ```
     [WSS_SSL]
     SSLPort=<SSL port number>
     ```

- If using Apache Web server:

```
[WSS_VIRDIR_INFO]
ROOT=/tmcss,<Server installation folder>\PCCSRV\WSS\isapi,,5
[WSS_WEB_SERVER]
ServerPort=8082
[WSS_SSL]
SSLPort=<SSL port number>
```

6. Open a command prompt and navigate to <Server installation folder>\PCCSRV.
7. Run the following commands:

```
SVRSVCSETUP.EXE -install
SVRSVCSETUP.EXE -enablessl
SVRSVCSETUP.EXE -setprivilege
```

8. Verify the reactivation.
   a. On Microsoft Management Console, the Trend Micro Smart Protection Server service has been started and its startup type is manual.
   b. On the OfficeScan server Web console, navigate to **Smart Scan > Scan Source**.
   c. Click the **standard list** link.
   d. On the screen that opens, click **Integrated Smart Protection Server**.
   e. On the screen that displays, click **Test Connection**. Connection with the integrated server should be successful.

Client Proxy Settings

Configure OfficeScan clients to use proxy settings when connecting to internal and external servers.

External Proxy Settings

Clients can use the proxy settings configured in Internet Explorer to connect to the Trend Micro Smart Protection Network. If proxy server authentication is required, clients will use the authentication credentials (user ID and password) specified on the Web console.

Note: Clients also use the same credentials when connecting to the Trend Micro Web reputation servers to verify if a URL is safe to access.

To configure proxy server authentication credentials:

PATH: ADMINISTRATION > PROXY SETTINGS > EXTERNAL PROXY

1. On the **Client Connection with Trend Micro Servers** section, type the user ID and password needed for proxy server authentication.

   The following proxy authentication protocols are supported:

   - Basic access authentication
   - Digest access authentication
   - Integrated Windows Authentication

2. Confirm the password.
3. Click **Save**.

Internal Proxy Settings

Clients can use internal proxy settings to connect to the following servers on the network:

OfficeScan Server

The server hosts the OfficeScan server and the integrated Smart Protection Server. Clients connect to the OfficeScan server to update components, obtain configuration settings, and send logs. Clients connect to the integrated Smart Protection Server to send reputation queries.

Smart Protection Servers

Smart Protection Servers include all standalone Smart Protection Servers and the integrated Smart Protection Server of other OfficeScan servers. Clients connect to the servers to send reputation queries.

To configure internal proxy settings:

PATH: ADMINISTRATION > PROXY SETTINGS > INTERNAL PROXY TAB

1. Select the check box to enable the use of a proxy server.
2. Specify the proxy server name or IP address, and port number.
3. If the proxy server requires authentication, type the user name and password in the fields provided.
4. Click **Save**.

Smart Protection Server List

Add the Smart Protection Servers you have set up to the Smart Protection Server list. Clients refer to the list to determine which Smart Protection Server to connect to. The client tries connecting to other servers on the list if it cannot connect to a particular server.

Tip: If you have set up multiple Smart Protection Servers, assign a standalone Smart Protection Server as the primary scan source and the integrated server as a backup. This reduces the scan query traffic directed to the computer that hosts the OfficeScan server and integrated server. The standalone server can also process more reputation queries.

To configure the Smart Protection Server list:

PATH: SMART PROTECTION > SMART PROTECTION SOURCE > INTERNAL CLIENTS

1. Select whether clients will use the standard list or custom lists.
2. Click **Notify All Clients**. smart scan clients automatically refer to the list you have configured.

Standard List

The standard list is used by all internal smart scan clients.

To configure the standard list:

PATH: SMART PROTECTION > SMART PROTECTION SOURCE > INTERNAL CLIENTS

1. Click the **standard list** link.
2. In the screen that opens, click **Add**.
3. Specify the Smart Protection Server name, Web Reputation Server name or IP address. Smart Protection Services supports HTTP or HTTPS, while Web Reputation Services supports only HTTP connection.

   Clients can connect to the Smart Protection Sources using HTTP and HTTPS protocols. HTTPS allows for a more secure connection while HTTP uses less bandwidth.

   To obtain the Smart Protection Server address:

   - For the integrated Smart Protection Server, open the OfficeScan Web console and go to **Smart Protection > Integrated Server**.
   - For the standalone Smart Protection Server, open the standalone server's console and go to the Summary page.

   Tip: Because the integrated Smart Protection Server and the OfficeScan server run on the same computer, the computer's performance may reduce significantly during peak traffic for the two servers. To reduce the traffic directed to the OfficeScan server computer, assign a standalone Smart Protection Server as the primary scan source and the integrated server as a backup source.

4. Select whether this server will be used for File Reputation services, Web reputation services, or both.

5. Specify the port number for secure connection.
6. Optionally enable SSL if the connection specified is HTTPS. HTTPS allows for a more secure connection while HTTP uses less bandwidth.
7. Click **Test Connection** to verify if connection to the server can be established.
8. Click **Save** when the test connection is successful. The Smart Protection Source screen displays.

Recommended Tasks:

1. Click the server name to do one of the following:
   - To view or edit server information.
   - View the full server address for Web or File Reputation Services.

   Smart Protection Services supports HTTP or HTTPS, while Web Reputation Services supports only HTTP connection. HTTPS allows for a more secure connection while HTTP uses less bandwidth.
2. To open the console of a Smart Protection Server, click **Launch console**.
   - For the integrated Smart Protection Server, the server's configuration screen displays.
   - For standalone Smart Protection Servers and the integrated Smart Protection Server of another OfficeScan server, the console logon screen displays.
3. To delete an entry, select the check box for the server and click **Delete**.
4. To export the list to a .dat file, click **Export** and then click **Save**.
5. If you have exported a list from another server and want to import it to this screen, click **Import** and locate the .dat file. The list loads on the screen.
6. On top of the screen, select whether clients will refer to the servers in the order in which they appear on the list or randomly. If you select **Order**, use the arrows under the **Order** column to move servers up and down the list.
7. Click **Save**.

Custom Lists

If you select custom lists, specify a range of IP addresses for a custom list. If a client's IP address is within the range, the client uses the custom list.

To configure custom lists:

PATH: SMART PROTECTION > SMART PROTECTION SOURCE > INTERNAL CLIENTS

1. Optionally enable the **Use the standard list if all servers on the custom lists are unavailable** option.
2. Click **Add**.
3. In the screen that opens, specify the following:
   - IP address range
   - Proxy settings clients will use to connect to the local Smart Protection Servers
4. Specify the Smart Protection Server name, Web Reputation Server name or IP address. Smart Protection Services supports HTTP or HTTPS, while Web Reputation Services supports only HTTP connection.

   To obtain the Smart Protection Server address:
   - For the integrated Smart Protection Server, open the OfficeScan Web console and go to **Smart Protection > Integrated Server**.
   - For the standalone Smart Protection Server, open the standalone server's console and go to the Summary page.

   Tip: Because the integrated Smart Protection Server and the OfficeScan server run on the same computer, the computer's performance may reduce significantly during peak traffic for the two servers. To reduce the traffic directed to the OfficeScan server computer, assign a standalone Smart Protection Server as the primary scan source and the integrated server as a backup source.

5. Select whether this server will be used for File Reputation services, Web reputation services, or both.
6. Specify the port number for secure connection.
7. Optionally enable SSL if the connection specified is HTTPS. HTTPS allows for a more secure connection while HTTP uses less bandwidth.

8. Click **Test Connection** to verify if connection to the server can be established.
9. Click **Save** when the test connection is successful. The Smart Protection Source list screen displays.

Recommended Tasks:

1. Click the server name to do one of the following:
   - To view or edit server information.
   - View the full server address for Web or File Reputation Services.

   Smart Protection Services supports HTTP or HTTPS, while Web Reputation Services supports only HTTP connection. HTTPS allows for a more secure connection while HTTP uses less bandwidth.
2. To open the console of a Smart Protection Server, click **Launch console**.
   - For the integrated Smart Protection Server, the server's configuration screen displays.
   - For standalone Smart Protection Servers and the integrated Smart Protection Server of another OfficeScan server, the console logon screen displays.
3. To delete an entry, click the icon under **Delete**.
4. Select whether clients will refer to the servers in the order in which they appear on the list or randomly. If you select **Order**, use the arrows under the **Order** column to move servers up and down the list.
5. Click **Save**.
6. Back in the Smart Protection Source screen, select whether to refer to the standard list if the client is unable to connect to any server on the custom list.
7. To modify an IP address range and its corresponding custom list, click the link under **IP Range**.
8. To export the custom lists to a .dat file, click **Export** and then click **Save**.
9. If you have exported custom lists from another server and want to import them to this screen, click **Import** and locate the .dat file. The lists load on the screen.

Computer Location Settings

OfficeScan provides a location awareness feature that determines the Web reputation policy applied to clients and the Smart Protection Server clients connect to. OfficeScan clients that can connect to the OfficeScan server or any of the reference servers are located internally, which means:

- These clients will apply the Web reputation policy for internal clients.
- If these clients use smart scan, they will connect to a Smart Protection Server.

If connection cannot be established, clients will apply the Web reputation policy for external clients. If clients use smart scan, these clients will connect to the Trend Micro Smart Protection Network.

Tip: Trend Micro recommends enforcing a stricter Web reputation policy on external clients.

Specify whether location is based on the client computer's gateway IP address or the client's connection status with the OfficeScan server or any reference server.

Gateway IP address

If the client computer's gateway IP address matches any of the gateway IP addresses you specified on the Computer Location screen, the computer's location is internal. Otherwise, the computer's location is external.

Client connection status

If the OfficeScan client can connect to the OfficeScan server or any of the assigned reference servers on the intranet, the computer's location is internal. Additionally, if a computer outside the corporate network can establish connection with the OfficeScan server/reference server, its location is also internal. If none of these conditions apply, the computer's location is external.

To configure location settings:

PATH: NETWORKED COMPUTERS > COMPUTER LOCATION

1. Choose whether location is based on **Client connection status** or **Gateway IP and MAC address**.
2. If you choose Client connection status, decide if you want to use a reference server. See *Reference Servers* on page 3-46 for details.
   a. If you did not specify a reference server, the client checks the connection status with the OfficeScan server when the following events occur:
      - Client switches from roaming to normal (online/offline) mode.
      - Client switches from one scan method to another.
      - Client detects IP address change in the computer.
      - Client restarts.
      - Server initiates connection verification.
      - Web reputation location criteria changes while applying global settings.
      - Outbreak prevention policy is no longer enforced and pre-outbreak settings are restored.

   b. If you specified a reference server, the client checks its connection status with the OfficeScan server first, and then with the reference server if connection to the OfficeScan server is unsuccessful. The client checks the connection status every 1 hour and when any of the events occur.
3. If you choose Gateway IP and MAC address:
   a. Type the gateway IP address in the text box provided.
   b. Optionally type the MAC address. If you do not type a MAC address, OfficeScan will include all the MAC addresses belonging to the specified IP address.
   c. Click **Add**.
   d. Repeat step a to step c until you have all the gateway IP addresses you want to add.

   You can also use the Gateway Settings Importer tool to import a list of gateway settings. See the *Administrator's Guide* for instructions on using the tool.
4. Click **Save**.

Reference Servers

One of the ways the OfficeScan client determines which of the firewall profiles or Web Reputation Policies to use is by checking its connection status with the OfficeScan server. If an internal client (or a client within the corporate network) cannot connect to the server, the client status becomes offline. The client then applies a firewall profile or Web reputation policy intended for external clients. Reference servers address this issue.

A client that loses connection with the OfficeScan server will try connecting to reference servers. If the client successfully establishes connection with a reference server, it applies the firewall profile or Web reputation policy for internal clients.

Take note of the following:

- Assign computers with server capabilities, such as a Web server, SQL server, or FTP server, as reference servers. You can specify a maximum of 32 reference servers.
- Clients connect to the first reference server on the reference server list. If connection cannot be established, the client tries connecting to the next server on the list.
- OfficeScan clients only use reference servers when determining the firewall profile or the Web reputation policy to use. Reference servers do not manage clients or deploy updates and client settings. The OfficeScan server performs these tasks.
- A client cannot send logs to reference servers or use them as update sources

To manage the reference server list:

PATH: NETWORKED COMPUTERS > FIREWALL > PROFILES > EDIT REFERENCE SERVER LIST

NETWORKED COMPUTERS > COMPUTER LOCATION > EDIT REFERENCE SERVER LIST

1. Select **Enable the Reference Server list**.
2. To add a computer to the list, click **Add**.
   a. Specify the computer's IP address, name, or fully qualified domain name (FQDN), such as:
      - computer.networkname
      - 12.10.10.10
      - mycomputer.domain.com
   b. Type the port through which clients communicate with this computer. Specify any open contact port (such as ports 20, 23 or 80) on the reference server.

Note: To specify another port number for the same reference server, repeat steps 2a and 2b. The client uses the first port number on the list and, if connection is unsuccessful, uses the next port number.

c. Click **Save**.

3. To edit the settings of a computer on the list, click the computer name. Modify the computer name or port, and then click **Save**.
4. To remove a computer from the list, select the computer name and then click **Delete**.
5. To enable the computers to act as reference servers, click **Assign to Clients**.

Chapter 4

Managing OfficeScan Clients and Smart Protection Servers

This chapter describes how to manage OfficeScan clients that use Trend Micro smart protection solutions and the Smart Protection Servers that provide the reputation services to these clients.

Topics in this chapter:

Managing Clients

This section discusses maintenance tasks after installing or upgrading clients and configuring them to use smart protection.

Client Information

View details about smart scan clients on the Web console's Summary screen and in the client tree.

Summary Screen

The **Smart Scan** tab on the Summary screen displays the following information:

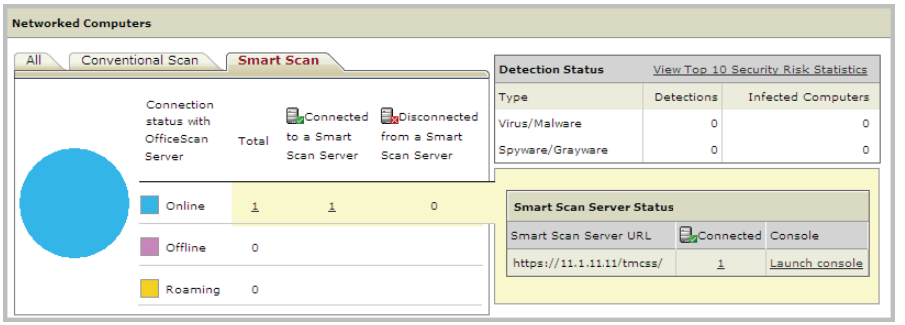


FIGURE 4-1. Smart Scan tab on the OfficeScan Summary screen

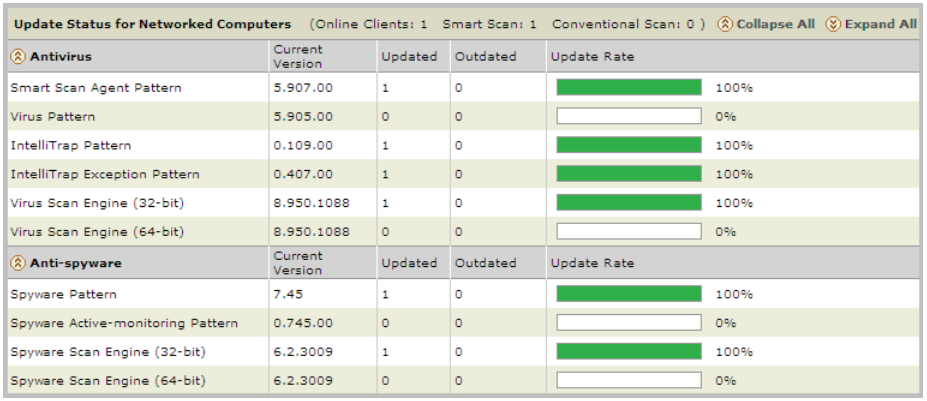
- The connection status of smart scan clients with the OfficeScan server
- The connection status of online smart scan clients with Smart Protection Servers

> **Note:** Only online clients can report their connection status with Smart Protection Servers.
>
> If clients are disconnected from a Smart Protection Server, restore the connection by performing the steps in *A Client Cannot Connect to a Smart Protection Server* on page 5-3.

- The number of detected security risks

- The computers where the security risks were detected
- A list of Smart Protection Servers
- The number of clients connected to each Smart Protection Server. Clicking the number opens the client tree where you can manage client settings.
- For each Smart Protection Server, a link that launches the server's console
- A **More** link (if you have clients connecting to more than two Smart Protection Servers) that opens a screen where you can:
  - View all the local Smart Protection Servers to which clients connect and the number of clients connected to each server. Clicking the number opens the client tree where you can manage client settings.
  - Launch a server's console by clicking the link for the server

View smart scan component information on the **Components and Programs** section.



Update Status for Networked Computers (Online Clients: 1 Smart Scan: 1 Conventional Scan: 0) Collapse All Expand All

Antivirus	Current Version	Updated	Outdated	Update Rate
Smart Scan Agent Pattern	5.907.00	1	0	100%
Virus Pattern	5.905.00	0	0	0%
IntelliTrap Pattern	0.109.00	1	0	100%
IntelliTrap Exception Pattern	0.407.00	1	0	100%
Virus Scan Engine (32-bit)	8.950.1088	1	0	100%
Virus Scan Engine (64-bit)	8.950.1088	0	0	0%
Anti-spyware	Current Version	Updated	Outdated	Update Rate
Spyware Pattern	7.45	1	0	100%
Spyware Active-monitoring Pattern	0.745.00	0	0	0%
Spyware Scan Engine (32-bit)	6.2.3009	1	0	100%
Spyware Scan Engine (64-bit)	6.2.3009	0	0	0%

FIGURE 4-2. Components and Programs section of the Summary screen

Smart scan clients download all the components, except the Virus Pattern and Spyware Active-monitoring Pattern. Check if you have clients with outdated components and use any of the client update methods to update clients. For details on client update methods, see the *OfficeScan Administrator's Guide*.

Client Tree

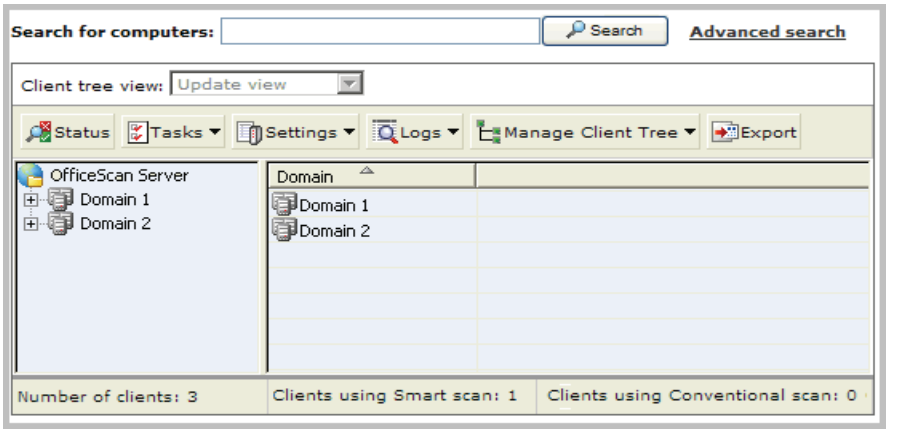


FIGURE 4-3. OfficeScan Web console client tree

The lower part of the screen displays the number of clients using smart scan.

On the client tree view, select **Smart scan view** to display smart scan information, which includes:

- Whether a Smart Protection Server is available for a client
- The URL of the Smart Protection Server to which a client currently connects. If a client is currently disconnected, the URL indicates the last server the client connected to.
- Smart scan component versions. If no component version displays and the cell is shaded, the component is not used by the client.

Click **Status** on top of the client tree to view detailed information about a client or group of clients.

Client Icons

Icons on the client computer's system tray indicate the client's connection status with the OfficeScan server and a Smart Protection Server.

Users need to take action when the icon indicates any of the following conditions:

- Pattern has not been updated for a while.
- Real-time Scan is disabled.
- Real-time Scan service was stopped. OfficeScan uses the Real-time Scan Service not only for Real-time Scan, but also for Manual Scan and Scheduled Scan. This means that if the Real-time Scan service stops, the client computer becomes unprotected.
- The client cannot connect to the Smart Protection Server hosting the Web Reputation Service.
- A smart scan client is not connected to any Smart Protection Server.

See *Troubleshooting* on page 5-2 for steps that users can take when any of these conditions arise.

Online Clients

Online clients maintain a continuous connection with the server. The OfficeScan server can initiate tasks and deploy settings to these clients.

TABLE 4-1. Online client icons

ICON	DESCRIPTION
CONVENTIONAL SCAN	
	All components are up-to-date and services work properly.
	The pattern file has not been updated for a while. Real-time Scan is enabled.
	The pattern file has not been updated for a while. Real-time Scan is enabled. The client can connect to the Smart Protection Server hosting the Web Reputation Service.

TABLE 4-1. Online client icons (Continued)

ICON	DESCRIPTION
	The pattern file has not been updated for a while. Real-time Scan is enabled. The client cannot connect to the Smart Protection Server hosting the Web Reputation Service.
	Real-time Scan is disabled.
	The pattern file has not been updated for a while. Real-time Scan is disabled.
	The pattern file has not been updated for a while. Real-time Scan is disabled. The client can connect to the Smart Protection Server hosting the Web Reputation Service.
	The pattern file has not been updated for a while. Real-time Scan is disabled. The client cannot connect to the Smart Protection Server hosting the Web Reputation Service.
	Real-time Scan Service was stopped.
	The pattern file has not been updated for a while. Real-time Scan Service was stopped.
	The pattern file has not been updated for a while. Real-time Scan Service was stopped. The client can connect to the Smart Protection Server hosting the Web Reputation Service.

TABLE 4-1. Online client icons (Continued)

ICON	DESCRIPTION
	The pattern file has not been updated for a while. Real-time Scan Service was stopped. The client cannot connect to the Smart Protection Server hosting the Web Reputation Service.
SMART SCAN	
	The client can connect to a Smart Protection Server and/or the Smart Protection Network. All services work properly.
	The client can connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan is disabled.
	The client can connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan Service was stopped.
	The client cannot connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan is enabled.
	The client cannot connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan is disabled.
	The client cannot connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan Service was stopped.

Offline Clients

Offline clients are disconnected from the server. The OfficeScan server cannot manage these clients.

TABLE 4-2. Offline client icons

ICON	DESCRIPTION
CONVENTIONAL SCAN	
	Real-time Scan is enabled.
	The pattern file has not been updated for a while. Real-time Scan is enabled.
	The pattern file has not been updated for a while. Real-time Scan is enabled. The client can connect to the Smart Protection Server hosting the Web Reputation Service.
	The pattern file has not been updated for a while. Real-time Scan is enabled. The client cannot connect to the Smart Protection Server hosting the Web Reputation Service.
	Real-time Scan is disabled.
	The pattern file has not been updated for a while. Real-time Scan is disabled.
	The pattern file has not been updated for a while. Real-time Scan is disabled. The client can connect to the Smart Protection Server hosting the Web Reputation Service.

TABLE 4-2. Offline client icons (Continued)

ICON	DESCRIPTION
	The pattern file has not been updated for a while. Real-time Scan is disabled. The client cannot connect to the Smart Protection Server hosting the Web Reputation Service.
	Real-time Scan Service was stopped.
	The pattern file has not been updated for a while. Real-time Scan Service was stopped.
	The pattern file has not been updated for a while. Real-time Scan Service was stopped. The client can connect to the Smart Protection Server hosting the Web Reputation Service.
	The pattern file has not been updated for a while. Real-time Scan Service was stopped. The client cannot connect to the Smart Protection Server hosting the Web Reputation Service.
SMART SCAN	
	The client can connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan is enabled.
	The client can connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan is disabled.
	The client can connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan Service was stopped.

TABLE 4-2. Offline client icons (Continued)

ICON	DESCRIPTION
	The client cannot connect to a Smart Protection Server and/or the Smart Protection Network.
	The client cannot connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan is disabled.
	The client cannot connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan Service was stopped.

Roaming Clients

Roaming clients can update components from the OfficeScan server but cannot send logs to the OfficeScan server. The OfficeScan server also cannot initiate tasks and deploy client settings to roaming clients. Depending on various factors such as a client computer's location or network connection status, a roaming client may or may not be able to communicate with the OfficeScan server.

Users with the roaming privilege may enable roaming mode when OfficeScan server intervention (such as server-initiated scanning) prevents them from fulfilling a task, such as when doing a presentation. Roaming clients with an Internet connection can still update components if configured to get updates from an Update Agent or the Trend Micro ActiveUpdate server.

Assign roaming privileges to clients that lose connection with the OfficeScan server for an extended period of time. To assign the privilege, go to **Networked Computers > Client Management > Settings > Privileges and Other Settings > Privileges** tab.

Updates to roaming clients occur only on the following occasions:

- When the client user performs manual update
- When you set an automatic update deployment that includes roaming clients
- When you grant clients the privilege to enable scheduled update

TABLE 4-3. Roaming client icons

ICON	DESCRIPTION
CONVENTIONAL SCAN	
	Real-time Scan is enabled.
	The pattern file has not been updated for a while. Real-time Scan is enabled.
	The pattern file has not been updated for a while. Real-time Scan is enabled. The client can connect to the Smart Protection Server hosting the Web Reputation Service.
	The pattern file has not been updated for a while. Real-time Scan is enabled. The client cannot connect to the Smart Protection Server hosting the Web Reputation Service.
	Real-time Scan is disabled.
	The pattern file has not been updated for a while. Real-time Scan is disabled.
	The pattern file has not been updated for a while. Real-time Scan is disabled. The client can connect to the Smart Protection Server hosting the Web Reputation Service.

TABLE 4-3. Roaming client icons (Continued)

ICON	DESCRIPTION
	The pattern file has not been updated for a while. Real-time Scan is disabled. The client cannot connect to the Smart Protection Server hosting the Web Reputation Service.
	Real-time Scan Service was stopped.
	The pattern file has not been updated for a while. Real-time Scan Service was stopped.
	The pattern file has not been updated for a while. Real-time Scan Service was stopped The client can connect to the Smart Protection Server hosting the Web Reputation Services.
	The pattern file has not been updated for a while. Real-time Scan Service was stopped The client cannot connect to the Smart Protection Server hosting the Web Reputation Services.
SMART SCAN	
	The client can connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan is enabled.
	The client can connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan is disabled.
	The client can connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan Service was stopped.

TABLE 4-3. Roaming client icons (Continued)

ICON	DESCRIPTION
	The client cannot connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan is disabled.
	The client cannot connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan is disabled.
	The client cannot connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan Service was stopped.

Managing the Standalone Smart Protection Server

This section discusses maintenance tasks you need to perform after installing the standalone Smart Protection Server.

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.

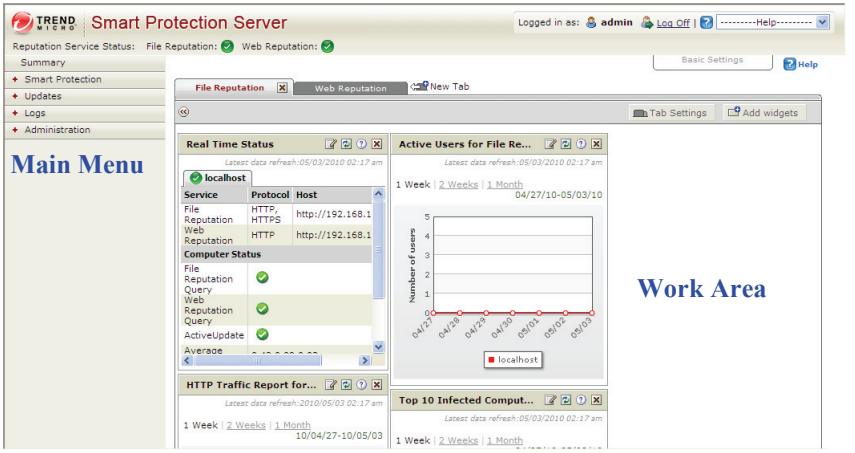


FIGURE 4-4. Summary Screen

TABLE 4-4. Contents of Smart Protection Server 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 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.

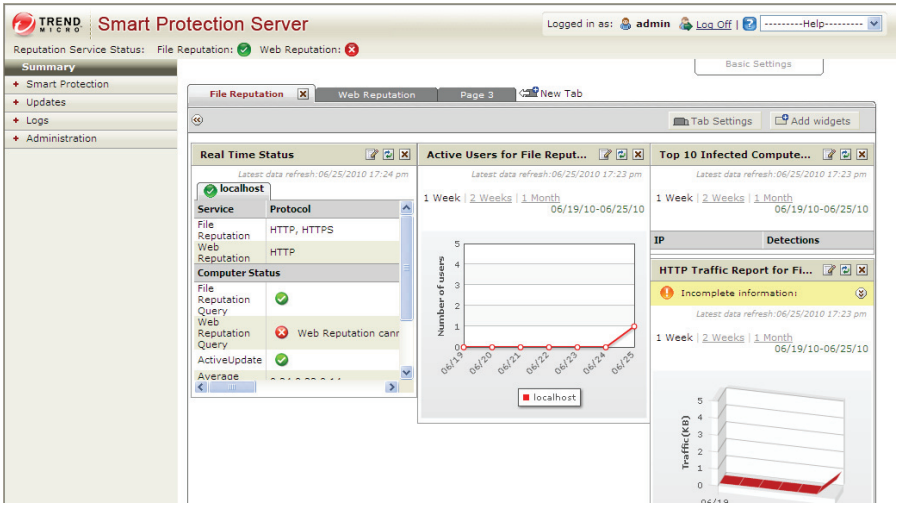


FIGURE 4-5. Summary Screen

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

A brief description of the available options is below.

- **Basic Settings**: Click to display the drop down menu.
- **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.
- **New Tab**: Click to add a new tab. Specify the title and layout of the tab. The layout can be one column, two columns, or three columns.
- **Tab Settings**: Click to edit the tab title and layout.
- **Add Widgets**: Click to add widgets to the Summary screen.

Using Tabs

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

To add a new tab:

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

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

4. 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:

PATH: SUMMARY

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

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:

PATH: SUMMARY

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.

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:

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:

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.

A brief description of the available options is below.

- **Operating System**: Select to update operating system components.
- **Smart Protection Server**: Select to update the product server program file.
- **Widget Pool**: 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.

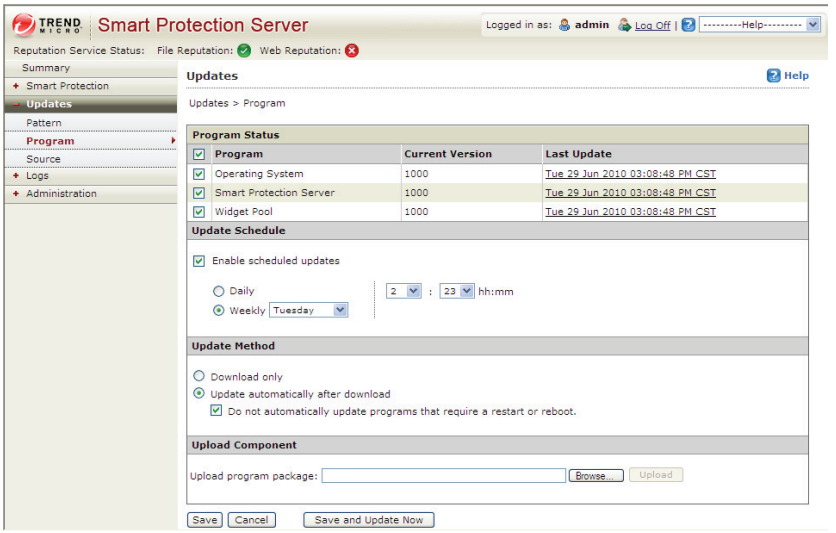
Performing Updates

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

To configure a scheduled update:

PATH: UPDATES > PROGRAM

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



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:

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:

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. The default update source is Trend Micro ActiveUpdate Server.

A brief description of the available options is below.

- **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.

Specifying an Update Source

To configure an update source:

PATH: UPDATES > SOURCE

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.

A brief description of the available options is below.

- **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.

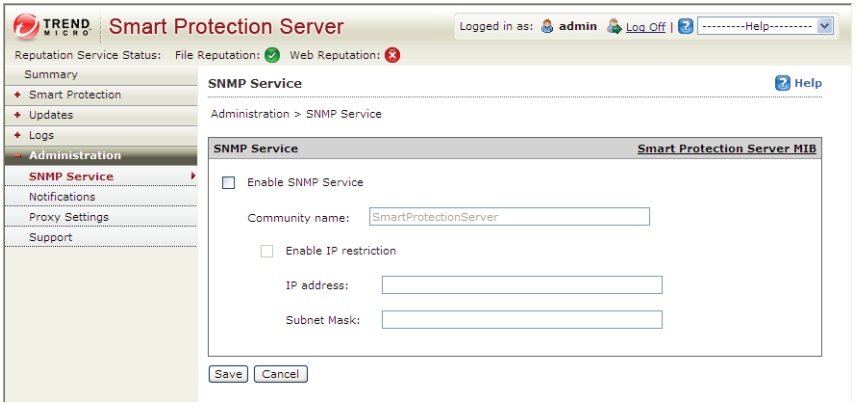
Configuring SNMP Service

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

To configure SNMP Service:

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:

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 4-5. 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:: 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.

TABLE 4-5. Description of Smart Protection Server MIB

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.

Logs

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

Web Access Log

The Web Access Log screen displays information for Web Reputation queries. A brief description of the available options is below.

- **Keyword**: Specify keywords to use when searching for URLs.
- **More Search Filters**: Click to display additional search filters.
- **Date Range**: Select a date range.
- **Product Entity**: Select the product that responded to the URL query from endpoints.
- **Details**: Click to see additional details about a log entry.

Viewing Web Access Log Entries

To view Web Access Log entries:

PATH: LOGS > WEB ACCESS LOG

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

Details

A brief description of the items on this screen is available below.

- **Date and time**: The date and time of the blocked URL event.
- **URL**: The URL that was blocked by Web Reputation.
- **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. This could be Smart Protection Server or Smart Protection Network.
- **Filter**: The list that filtered the URL. This could be the custom blocked URL list, custom approved URL list, or the Trend Micro Web Blocking List.

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:

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. A brief description of the available options is below.

- Pattern Update Log: Select to purge pattern update log entries.
- Program Update Log: Select to purge update log entries.
- Web Access Log: Select to purge URL query 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.

Performing Log Maintenance

To perform log maintenance:

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**.

Viewing Notifications

You can configure Smart Protection Server to send email message or Small 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.

A brief description of the options available on this screen is available below.

- **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.

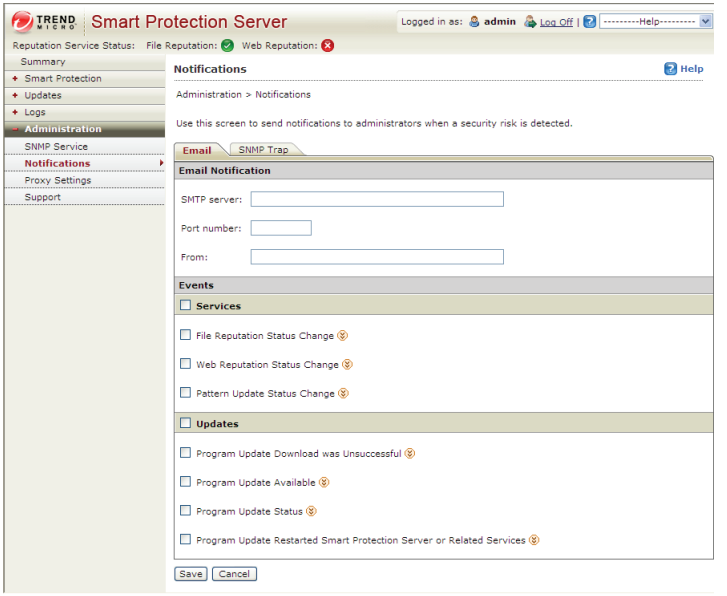
- **Pattern Update Status Change**: Select to send a notification for status changes and specify the recipient for this notification.
- **Updates**: Select to send notifications for all program related notifications.
- **Program Update Download was Unsuccessful**: Select to send a notification if the 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

To configure email notifications:

PATH: ADMINISTRATION > NOTIFICATIONS

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



2. Select the **Services** check box or select from the following check boxes:
   - **File Reputation Status Change**: Select to send a notification for status changes and specify the recipient, subject, and message.
   - **Web Reputation Status Change**: Select to send a notification for status changes and specify the recipient, subject, and message.
   - **Pattern Update Status Change**: Select to send a notification for status changes and specify the recipient, subject, and message.

3. Select **Update** 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.

A brief description of the options available on this screen is available below.

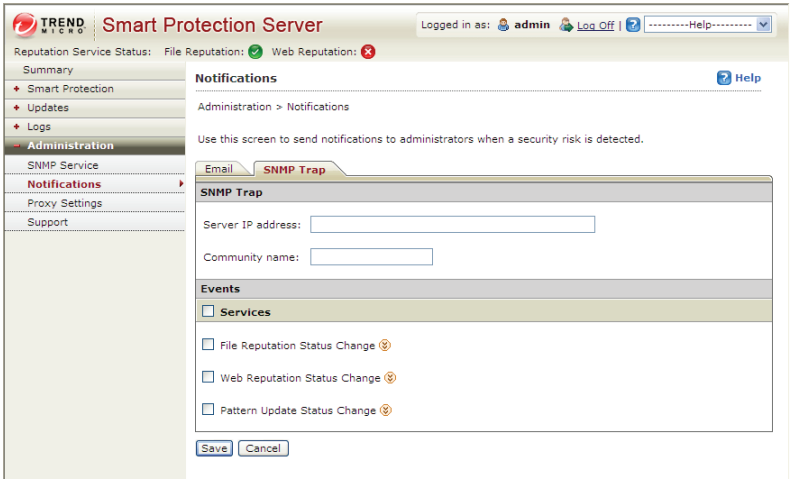
- **Server IP address**: Specify the SNMP trap receiver IP address
- **Community name**: Specify the SNMP community name.
- **Services**: Select to send an SNMP notification for status changes in File Reputation, Web Reputation, and pattern updates.
- **Message**: Type a new message or use the default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

Configuring SNMP Trap Notifications

To configure SNMP trap notifications:

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**.

Downloading System Information for Support

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

A brief description of the available options is below.

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

Downloading the System Information File

To download diagnostic information:

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**.

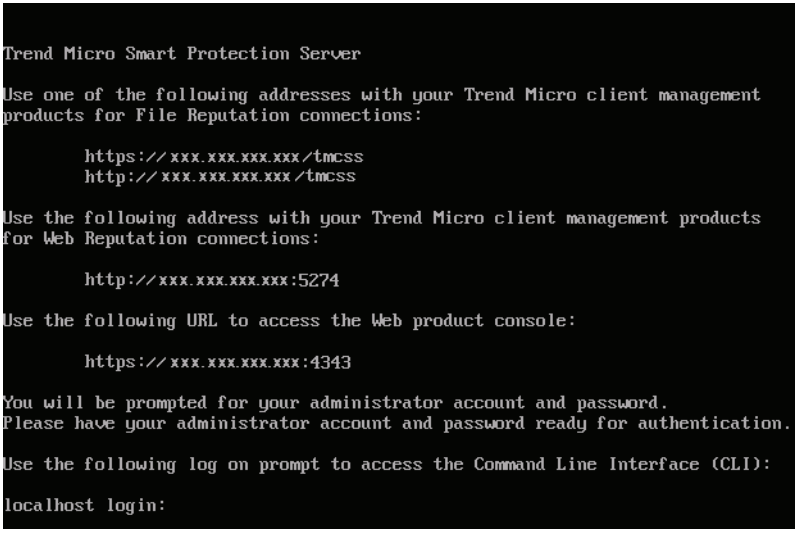
Changing the Product Console Password

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.



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.

Managing the Integrated Smart Protection Server

This section discusses maintenance tasks you need to perform after installing the integrated Smart Protection Server.

Updating Components

The Smart Protection Server downloads the Smart Scan Pattern and Web Blocking List. Clients verify potential threats against the pattern by sending reputation queries to the Smart Protection Server. Clients do not download the Smart Scan Pattern.

Note: The other pattern used in the smart protection solution, called Smart Scan Agent Pattern, is hosted on the client update source (the OfficeScan server or a customized update source) and downloaded by clients.

Trend Micro updates the Smart Scan Pattern hourly. Like the OfficeScan server, the Smart Protection Server also uses a mechanism called *component duplication* that allows faster downloads of the pattern file. See the *Administrator's Guide* for more information on component duplication.

Configure the Smart Protection Server to download the Smart Scan Pattern from the Trend Micro ActiveUpdate server or from another source. You can manually update the pattern or configure an update schedule.

To configure server update settings:

PATH: SMART PROTECTION > INTEGRATED SERVER

1. Select to use the Integrated File Reputation Service, Web Reputation Service, or both. If you do not select the check box:
   - The integrated server stops updating components from the ActiveUpdate server.
   - Clients will not be able to send reputation queries to the integrated server.
2. Use the information under **Server Address** when configuring the Smart Protection Server list.

Clients can connect to the integrated server using HTTP and HTTPS protocols. HTTPS allows for a more secure connection while HTTP uses less bandwidth. When clients connect using a specific protocol, they identify the integrated server by its server address.

Tip: Clients managed by another OfficeScan server can also connect to the integrated server. On the other OfficeScan server's Web console, add the integrated server's address to the Smart Protection Server list.

3. View the Smart Scan Pattern version. To update the pattern manually, click **Update Now**. The update result displays on top of the screen.
4. **Import** or **Export** the Web Reputation Service Approved/Blocked List.

Note: This list can only be imported or exported.

5. To update the pattern automatically, enable scheduled updates and configure the update schedule.
6. Select the location from where you want to download component updates for file reputation service or web reputation service.

   If you choose ActiveUpdate server, ensure that the server has Internet connection and, if you are using a proxy server, test if Internet connection can be established using the proxy settings. See *Proxy for Server Update* on page 4-38 for details.

   If you choose a custom update source, set up the appropriate environment and update resources for this update source. Also ensure that there is functional connection between the server computer and this update source. If you need assistance setting up an update source, contact your support provider.
7. Click **Save**.

Proxy for Server Update

You can configure the integrated Smart Protection Server to use proxy settings when downloading updates from the Trend Micro ActiveUpdate server.

The OfficeScan server also uses these settings when downloading components from the ActiveUpdate server.

To configure proxy settings:

PATH: ADMINISTRATION > PROXY SETTINGS > EXTERNAL PROXY TAB

1. On the **OfficeScan Server Computer Updates** section, select the check box to enable the use of a proxy server.
2. Specify the proxy protocol, server name or IP address, and port number.
3. If the proxy server requires authentication, type the user name and password in the fields provided.
4. Click **Save**.

Component Rollback

Rollback refers to reverting to the previous version of the Virus Pattern, Smart Scan Agent Pattern, and Virus Scan Engine. If these components do not function properly, roll them back to their previous versions. OfficeScan retains the current and the previous versions of the Virus Scan Engine, and the last five versions of the Virus Pattern and Smart Scan Agent Pattern.

Note: Only the above-mentioned components can be rolled back.

OfficeScan uses different scan engines for clients running 32-bit and 64-bit platforms. You need to roll back these scan engines separately. The rollback procedure for all types of scan engines is the same.

To roll back the Virus Pattern, Smart Scan Agent Pattern, and Virus Scan Engine:

PATH: UPDATES > ROLLBACK

1. Click **Synchronize with Server** under the appropriate section.
   a. In the client tree that displays, select the clients with components that need to be rolled back.
   b. Click **Roll back**. Click **Back** at the bottom of the screen to return to the Rollback screen.
2. If an older version pattern file exists on the server, roll back the pattern file for both the client and the server by clicking **Rollback Server and Client Versions.**

Chapter 5

Getting Help

This chapter describes troubleshooting issues that may arise and how to contact support.

Topics in this chapter:

Troubleshooting

Perform the necessary tasks when the client icon on the system tray indicates any of the following conditions:

Real-time Scan Service was Stopped

Users can manually start the service (OfficeScanNT RealTime Scan) from Microsoft Management Console by clicking **Start > Run** and typing **services.msc**.

Real-time Scan was Disabled

Enable Real-time Scan from the Web console (**Networked Computers > Client Management > Settings > Real-time Scan Settings**).

Real-time Scan was Disabled and Client is in Roaming Mode

Users need to disable roaming mode first. After disabling roaming mode, enable Real-time Scan from the Web console.

A Client Within the Corporate Network is Disconnected from the Server

Verify the connection from the Web console (**Networked Computers > Connection Verification**) and then check connection verification logs (**Logs > Networked Computer Logs > Connection Verification**).

If the client is still disconnected after verification:

1. If the connection status on both the server and client is offline, check the network connection.
2. If the connection status on the client is offline but online on the server, the server's domain name may have been changed and the client connects to the server using the domain name (if you select domain name during server installation). Register the OfficeScan server's domain name to the DNS or WINS server or add the domain name and IP information into the "hosts" file in the client computer's <Windows folder>\system32\drivers\etc folder.
3. If the connection status on the client is online but offline on the server, check the OfficeScan firewall settings. The firewall may block server-to-client communication, but allow client-to-server communication.

4. If the connection status on the client is online but offline on the server, the client's IP address may have been changed but its status does not reflect on the server (for example, when the client is reloaded). Try to redeploy the client.

A Client Cannot Connect to a Smart Protection Server

1. Check if the following settings have been configured properly:
   - Reference servers and port numbers
   - Gateway IP addresses

   For details, see *Computer Location Settings* on page 3-44.
2. Check if the Smart Protection Server address on the standard or custom list of scan servers is correct.

   For details, see *Smart Protection Server List* on page 3-39.
3. Test if connection using the server address can be established. Also ensure that you click **Notify All Clients** after configuring the list.
4. Check if the following configuration files on the Smart Protection Server and OfficeScan client are synchronized:
   - sscfg.ini
   - ssnotify.ini
5. Verify from the registry whether or not a client is connected to the corporate network.

   Key:
   HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\iCRC Scan\Scan Server
   - If LocationProfile=1, the client is connected to the network and should connect to a local Smart Protection Server.
   - If LocationProfile=2, the client is not connected to the network and should connect to the Global Smart Protection Server. From Internet Explorer, check if the client computer can browse Internet Web pages.
6. Check internal and external proxy settings used to connect to Smart Protection Servers (local and global).

   For details, see *External Proxy Settings* on page 3-38 and *Internal Proxy Settings* on page 3-38.

Contacting Trend Micro

Technical Support

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

Trend Micro Incorporated provides worldwide support to all registered users.

- Get a list of the worldwide support offices at:

  http://www.trendmicro.com/support

- Get the latest Trend Micro product documentation at:

  http://www.trendmicro.com/download

In the United States, you can reach the Trend Micro representatives through phone, fax, or email:

Trend Micro, Inc.

10101 North De Anza Blvd., Cupertino, CA 95014

Toll free: +1 (800) 228-5651 (sales)

Voice: +1 (408) 257-1500 (main)

Fax: +1 (408) 257-2003

Web address:

http://www.trendmicro.com

Email: support@trendmicro.com

Speeding Up Your Support Call

When you contact Trend Micro, to speed up your problem resolution, ensure that you have the following details available:

- Product build version
- Virtualization platform (VMware™ or Hyper-V™) and version

- Exact text of the error message, if any
- Steps to reproduce the problem
- Collect Diagnostic Information.

The Trend Micro Knowledge Base

The Trend Micro Knowledge Base, maintained at the Trend Micro Web site, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:

http://esupport.trendmicro.com

Trend Micro updates the contents of the Knowledge Base continuously and adds new solutions daily. If you are unable to find an answer, however, you can describe the problem in an email and send it directly to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

TrendLabs

TrendLabs^{SM} is the global antivirus research and support center of Trend Micro. Located on three continents, TrendLabs has a staff of more than 250 researchers and engineers who operate around the clock to provide you, and every Trend Micro customer, with service and support.

You can rely on the following post-sales service:

- Regular virus pattern updates for all known "zoo" and "in-the-wild" computer viruses and malicious codes
- Emergency virus outbreak support
- Email access to antivirus engineers
- Knowledge Base, the Trend Micro online database of technical support issues

TrendLabs has achieved ISO 9002 quality assurance certification.

Security Information Center

Comprehensive security information is available at the Trend Micro Web site.

http://www.trendmicro.com/vinfo/

Information available:

- List of viruses and malicious mobile code currently "in the wild," or active
- Computer virus hoaxes
- Internet threat advisories
- Virus weekly report
- Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- Glossary of terms

Sending Suspicious Files to Trend Micro

If you think you have an infected file but the scan engine does not detect it or cannot clean it, Trend Micro encourages you to send the suspect file to us. For more information, refer to the following site:

http://subwiz.trendmicro.com/subwiz

You can also send Trend Micro the URL of any Web site you suspect of being a phish site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and viruses).

- Send an email to the following address and specify "Phish or Disease Vector" as the subject.

  virusresponse@trendmicro.com

- You can also use the Web-based submission form at:

  http://subwiz.trendmicro.com/subwiz

Documentation Feedback

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

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

Appendix A

Scan Method Deployment Tasks

This appendix discusses the tasks involved in various stages of smart method deployment. For details about deployment, see *Scan Method Deployment During Fresh Installation* on page 2-9 and *Scan Method Deployment During Upgrade* on page 2-9.

Configuring Scan Methods

OfficeScan clients can use either conventional scan or smart scan when scanning for security risks.

To change the scan method:

PATH: NETWORKED COMPUTERS > CLIENT MANAGEMENT > SETTINGS > SCAN METHODS

1. Select to use conventional scan or smart scan.
2. If you selected domain(s) or client(s) on the client tree, click **Save** to apply settings to the domain(s) or client(s).

   If you selected the root icon  , choose from the following options:

   - **Apply to All Clients:** Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configure the settings.

- **Apply to Future Domains Only:** Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Recording OfficeScan Server Information

Record the following OfficeScan 10.5 server information. Specify this information on the OfficeScan 8.x/7.3 server when moving clients:

- Server computer name or IP address
- Server listening port. To view the server listening port, navigate to **Administration > Connection Settings**. The port number displays on the screen.

Preparing the OfficeScan 10.5 Server

One of the upgrade methods involves preparing an OfficeScan 10.5 server and then moving online OfficeScan 10.x/8.x/7.3 clients to this server. When clients move, they automatically upgrade.

To prepare the OfficeScan 10.5 server:

1. Perform a fresh installation of the OfficeScan 10.5 server. For details, see the *Installation and Upgrade Guide*.
2. Open the OfficeScan 10.5 Web console and go to **Updates > Networked Computers > Automatic Update**.
3. Enable the following options:
   - Initiate component update on clients immediately after the OfficeScan server downloads a new component.
   - Let clients initiate component update when they restart and connect to the OfficeScan server (roaming clients are excluded)
4. Go to **Networked Computers > Client Management**.
5. From the client tree, select the root icon.
6. Click **Settings > Privileges and Other Settings** and go to the **Other Settings** tab.
7. Disable **Clients can update components but not upgrade the client program or deploy hot fixes**.
8. Click **Apply to All Clients**.

9. Record the following OfficeScan 10.5 server information. Specify this information on the OfficeScan 10.x/8.x/7.3 server when moving clients:
   - Server computer name or IP address
   - Server listening port. To view the server listening port, navigate to **Administration > Connection Settings**. The port number displays on the screen.
10. Go to **Networked Computers > Client Grouping**.
11. Choose a manual client grouping method (by NetBIOS domain, Active Directory Domain, or DNS domain). Any of these client grouping methods allows you to create new domains.

Note: If you plan to use custom client grouping, enable it only after all clients have upgraded to ensure that all scan method settings are retained during client upgrade.

Upgrading Clients by Moving Them to An OfficeScan 10.5 Server

One of the upgrade methods involves preparing an OfficeScan 10.5 server and then moving online OfficeScan 10.x/8.x/7.3 clients to this server. When clients move, they automatically upgrade.

After preparing the OfficeScan 10.5 server (see *Preparing the OfficeScan 10.5 Server* on page A-2), follow these steps to upgrade clients:

Upgrading OfficeScan 10.x Clients

1. Duplicate the client tree domain structure and scan method settings in the OfficeScan 10.x server into the OfficeScan 10.5 server. If the domain structure and scan method settings on the two servers are not identical, some clients that move to the OfficeScan 10.5 server may not apply their original scan method settings.

   WARNING! **Perform the succeeding steps immediately. If the server notification queue gets updated before you move clients, clients might not move successfully.**

2. On the OfficeScan 10.x Web console:
   a. Navigate to **Updates > Summary**.
   b. Click **Cancel Notification**. This function clears the server notification queue, which will prevent problems moving clients to the OfficeScan 10.5 server.
   c. Navigate to **Networked Computers > Client Management**.
   d. From the client tree, select the clients you want to upgrade. Select only online clients because offline and roaming clients cannot be moved.

   Tip: Upgrade online Update Agents first. Update Agents help reduce traffic directed to the OfficeScan server by acting as an update source for other clients.

3. Click **Manage Client Tree > Move Client**.
4. Specify the OfficeScan 10.5 server computer name/IP address and server listening port under **Move selected client(s) to another OfficeScan server**.
5. Click **Move**. See *Upgrade Results* on page A-6.

Upgrading OfficeScan 8.x Clients

1. Open the OfficeScan 8.x Web console.
2. Navigate to **Updates > Summary**.
3. Click **Cancel Notification**. This function clears the server notification queue, which will prevent problems moving clients to the OfficeScan 10.5 server.

   WARNING! **Perform the succeeding steps immediately. If the server notification queue gets updated before you move clients, clients might not move successfully.**

4. Navigate to **Networked Computers > Client Management**.
5. From the client tree, select the clients you want to upgrade. Select only online clients because offline and roaming clients cannot be moved.

   Tip: Upgrade online Update Agents first. Update Agents help reduce traffic directed to the OfficeScan server by acting as an update source for other clients.

6. Click **Manage Client Tree > Move Client**.
7. Specify the OfficeScan 10.5 server computer name/IP address and server listening port under **Move selected client(s) online to another OfficeScan Server**.
8. Click **Move**. See *Upgrade Results* on page A-6.

Upgrading OfficeScan 7.3 Clients

1. Open the OfficeScan 7.3 Web console.
2. Click **Clients** on the main menu.
3. From the client tree, select the clients you want to upgrade. Select only online clients because offline and roaming clients cannot be moved.

Tip: Upgrade online Update Agents first. Update Agents help reduce traffic directed to the OfficeScan server by acting as an update source for other clients.

4. Click **Move**.
5. Specify the OfficeScan 10.5 server computer name/IP address and server listening port under **Move selected client(s) online to another OfficeScan Server**.
6. Click **Move**. See *Upgrade Results* on page A-6.

Upgrade Results

- Online clients start to move and upgrade.
- Tips for managing offline and roaming clients:
  - Disable roaming mode on clients so you can upgrade them.
  - For offline clients, instruct users to connect to the network so that the client can become online. For clients that are offline for an extended period of time, instruct users to uninstall the client from the computer and then use a suitable client installation method (such as client packager) discussed in the OfficeScan Administrator's Guide to install the OfficeScan 10.5 client.

Note: Restart computers to finish upgrading the clients. You can uninstall the OfficeScan 10.x, 8.x, or 7.3 server after all clients have been upgraded.

Manually Upgrading Clients

One of the ways you can upgrade clients is by upgrading them manually after the OfficeScan server upgrades to version 10.5. Do this if you have a large number of clients.

Perform the following tasks on the OfficeScan 10.5 Web console:

To manually upgrade clients after the OfficeScan server upgrades to version 10.5:

1. Navigate to **Networked Computers > Client Management**.
2. On the client tree, select the clients you want to upgrade. You can select one or several domains, or individual/all clients within a domain.

   Tip: Upgrade Update Agents first. Update Agents help reduce traffic directed to the OfficeScan server by acting as an update source for other clients.

3. Click **Settings > Privileges and Other Settings** and navigate to the **Other Settings** tab.
4. Disable **Clients can update components but not upgrade the client program or deploy hot fixes**.
5. Navigate to **Updates > Networked Computers > Automatic Update**.
6. Enable the following options:
   - Initiate component update on clients immediately after the OfficeScan server downloads a new component.
   - Let clients initiate component update when they restart and connect to the OfficeScan server (roaming clients are excluded)
7. Check the upgrade results.
   - *Upgrade Results (Online Clients)* on page A-8
   - *Upgrade Results (Offline Clients)* on page A-9
   - *Upgrade Results (Roaming Clients)* on page A-9
8. Restart computers to finish upgrading the clients.

Upgrade Results (Online Clients)

Automatic upgrade

Online clients start to upgrade when any of the following events occur:

- The OfficeScan server downloads a new component and notifies clients to update.
- The client reloads.
- The client restarts and then connects to the OfficeScan server.
- A client computer running Windows 2003 and XP Professional logs on to a server whose login script you modified using Login Script Setup (AutoPcc.exe).
- Scheduled update runs on the client computer (only for clients with scheduled update privileges).

Manual upgrade

If none of the above events have occurred, perform any of the following tasks to upgrade clients immediately:

- Create and deploy an EXE or MSI client package.

  Note: See the *Administrator's Guide* for instructions on creating a client package.

- Instruct client users to run **Update Now** on the client computer.
- If the client computer runs Windows 2003, XP Professional, 2008, or Vista™ (all editions except Vista Home), instruct the user to perform the following steps:
  - Connect to the server computer.
  - Navigate to \\<server computer name>\ofcscan.
  - Launch **AutoPcc.exe**.
- If the client computer runs Windows XP Home or Vista Home, instruct the user to right-click **AutoPcc.exe**, and select **Run as administrator**.
- Initiate manual client update.

To initiate manual client update:

1. Navigate to **Updates > Networked Computers > Manual Update**.
2. Select **Manually select clients** and click **Select**.
3. In the client tree that opens, choose the clients to upgrade.
4. Click **Initiate Component Update** on top of the client tree.

Upgrade Results (Offline Clients)

Offline clients upgrade when they become online.

Upgrade Results (Roaming Clients)

Roaming clients upgrade when they become online or, if the client has scheduled update privileges, when scheduled update runs.

Configuring Automatic Client Upgrade and Update Settings

OfficeScan clients automatically upgrade after the server upgrades. If you have a large number of clients, you can upgrade the server first and then manually upgrade clients individually or in groups. Before upgrading the server, configure settings that prevent clients from upgrading. After the server upgrades, re-enable the settings.

Tip: It may take a while to deploy the settings to online clients if you have a complex network environment and a large number of clients. Before the upgrade, allocate sufficient time for settings to deploy to all clients. Clients that do not apply the settings will automatically upgrade.

To configure automatic client upgrade and update settings:

For OfficeScan 10.x/8.x:

1. Navigate to **Networked Computers > Client Management**.
2. From the client tree, select the root icon to select all clients.
3. Click **Settings > Privileges and Other Settings** and navigate to the **Other Settings** tab.
4. Check the setting **Clients can update components but not upgrade the client program or deploy hot fixes**.
   - Enable this setting to prevent clients from upgrading after the server upgrades.
   - Disable this setting to upgrade clients automatically.
5. Click **Apply to All Clients**.
6. Navigate to **Updates > Networked Computers > Automatic Update**.
7. If you disabled the **Clients can update components but not upgrade the client program or deploy hot fixes** setting in step 4, enable the following settings:
   - Initiate component update on clients immediately after the OfficeScan server downloads a new component.
   - Let clients initiate component update when they restart and connect to the OfficeScan server (roaming clients are excluded).

   If you enabled the **Clients can update components but not upgrade the client program or deploy hot fixes** setting in step 4, disable the following settings:
   - Initiate component update on clients immediately after the OfficeScan server downloads a new component.
   - Let clients initiate component update when they restart and connect to the OfficeScan server (roaming clients are excluded).
8. Click **Save**.

For OfficeScan 7.3:

1. Click **Clients** on the main menu.
2. From the client tree, select the root icon to select all clients.
3. Click **Client Privileges/Settings**.
4. Under Update Settings, check the setting **Forbid program upgrade and hot fix deployment**.

a. Enable this setting to prevent clients from upgrading after the server upgrades.

b. Disable this setting to upgrade clients automatically.

5. Click **Apply to All**.
6. Navigate to **Updates > Client Deployment > Automatic Deployment**.
7. If you disabled the **Forbid program upgrade and hot fix deployment** setting in step 4, enable the following settings:
   - Deploy to clients immediately after the OfficeScan server downloads a new component.
   - Deploy to clients for OfficeScan clients only and excluding roaming clients when they are restarted.

   If you enabled the **Forbid program upgrade and hot fix deployment** setting in step 4, disable the following settings:
   - Deploy to clients immediately after the OfficeScan server downloads a new component.
   - Deploy to clients for OfficeScan clients only and excluding roaming clients when they are restarted.
8. Click **Save**.

Creating OfficeScan Domains

A domain in OfficeScan is a group of clients that share the same configuration and run the same tasks. By grouping clients into domains, you can configure, manage, and apply the same configuration to all domain members.

To create domains:

PATH: NETWORKED COMPUTERS > CLIENT MANAGEMENT > MANAGE CLIENT TREE > ADD DOMAINS

1. Type a name for the domain you want to add.
2. Click **Add**. The new domain appears in the client tree.
3. Optionally, create subdomains:
   a. Select the parent domain.
   b. Click **Manage Client Tree** > **Add domain**.
   c. Specify the sub domain name.
   d. Repeat steps a to c to create additional subdomains.

Appendix B

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

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 B-1. Command Line Interface (CLI) Commands

COMMAND	SYNTAX	DESCRIPTION
configure date	configure date <date> <time>	Configure date and save to CMOS *date* DATE_FIELD [DATE_FIELD] *time* TIME_FIELD [TIME_FIELD]
configure dns	configure dns <dns1> [dns2]	Configure DNS settings *dns1* IP_ADDR Primary DNS server *dns2* IP_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

TABLE B-1. Command Line Interface (CLI) Commands

COMMAND	SYNTAX	DESCRIPTION
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 ja_JP	configure locale ja_JP	Configure system locale to Japanese
configure locale pl_PL	configure locale pl_PL	Configure system locale to Polish
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 ip dhcp	configure ip dhcp [vlan]	Configure the default Ethernet interface to use DHCP vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure ip static	configure ip static <ip> <mask> <gateway> [vlan]	Configure the default Ethernet interface to use the static IP configuration

TABLE B-1. Command Line Interface (CLI) Commands

COMMAND	SYNTAX	DESCRIPTION
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
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

TABLE B-1. Command Line Interface (CLI) Commands

COMMAND	SYNTAX	DESCRIPTION
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
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

TABLE B-1. Command Line Interface (CLI) Commands

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

TABLE B-1. Command Line Interface (CLI) Commands

COMMAND	SYNTAX	DESCRIPTION
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
configure timezone Asia Tokyo	configure timezone Asia Tokyo	Configure timezone to Asia/Tokyo location

TABLE B-1. Command Line Interface (CLI) Commands

COMMAND	SYNTAX	DESCRIPTION
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 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/
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

TABLE B-1. Command Line Interface (CLI) Commands

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

TABLE B-1. Command Line Interface (CLI) Commands

COMMAND	SYNTAX	DESCRIPTION
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 lwcs-access-log	disable lwcs-accesslog	Disable lwcs_access.log to write to Smart Protection Server: /var/log/lighttpd/ folder
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

TABLE B-1. Command Line Interface (CLI) Commands

COMMAND	SYNTAX	DESCRIPTION
enable lwcs-access-log	enable lwcs-accesslog	Enable lwcs_access.log to write to Smart Protection Server: /var/log/lighttpd/ folder
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
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 ip address	show ip address	Display network address.
show ip dns	show ip dns	Display network DNS servers.
show ip gateway	show ip gateway	Display network gateway

TABLE B-1. Command Line Interface (CLI) Commands

COMMAND	SYNTAX	DESCRIPTION
show ip route	show ip route	Display network routing table
show timezone	show timezone	Display network timezone
show uptime	show uptime	Display current system uptime
show url FileReputationService	show url FileReputationService	Display endpoint connection addresses for File Reputation Service

Index

T

U

V

W