TREND MICRO

OfficeScan™ 10

For Enterprise and Medium Business

Smart Scan Getting Started Guide

Endpoint Security

Document Part No. OSEM104052/90318

Release Date: April 2009

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

Preface

Chapter 1: Introducing Trend Micro Smart Scan

Chapter 2: Smart Scan Deployment

Chapter 3: Smart Scan Environment

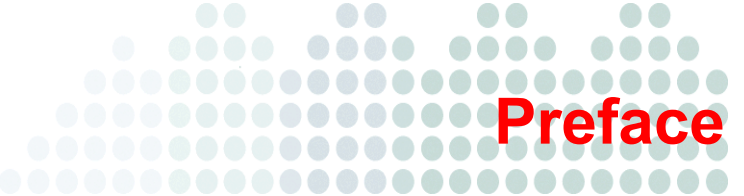
Chapter 4: Managing Smart Scan Clients and Servers

Chapter 5: Getting Help

Appendix A: Smart Scan Deployment Tasks

Appendix B: Command Line Interface (CLI) Commands

Index



Preface

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

Topics in this chapter:

OfficeScan Documentation

OfficeScan documentation includes the following:

TABLE P-1. OfficeScan documentation

DOCUMENTATION	DESCRIPTION
Trend Micro Smart Scan for OfficeScan Getting Started Guide	A PDF document that helps users understand smart scan concepts, prepare the environment needed to use smart scan, and manage smart scan clients
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 Scan

Topics in this chapter:

How Does Trend Micro Smart Scan Work?

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

Smart scan leverages file reputation technology to detect security risks. The technology works by off loading a large number of anti-malware signatures that were previously stored on endpoint computers to either local Smart Scan Servers or Global Smart Scan Servers.

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

The Need for a New Solution

In the current approach to file-based threat handling, patterns (or definitions) required to protect a computer are, for the most part, delivered on a scheduled basis in batches from Trend Micro to endpoint systems. When a new update is received, the virus/malware prevention software on the computer 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 user's computer to ensure continued protection.

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

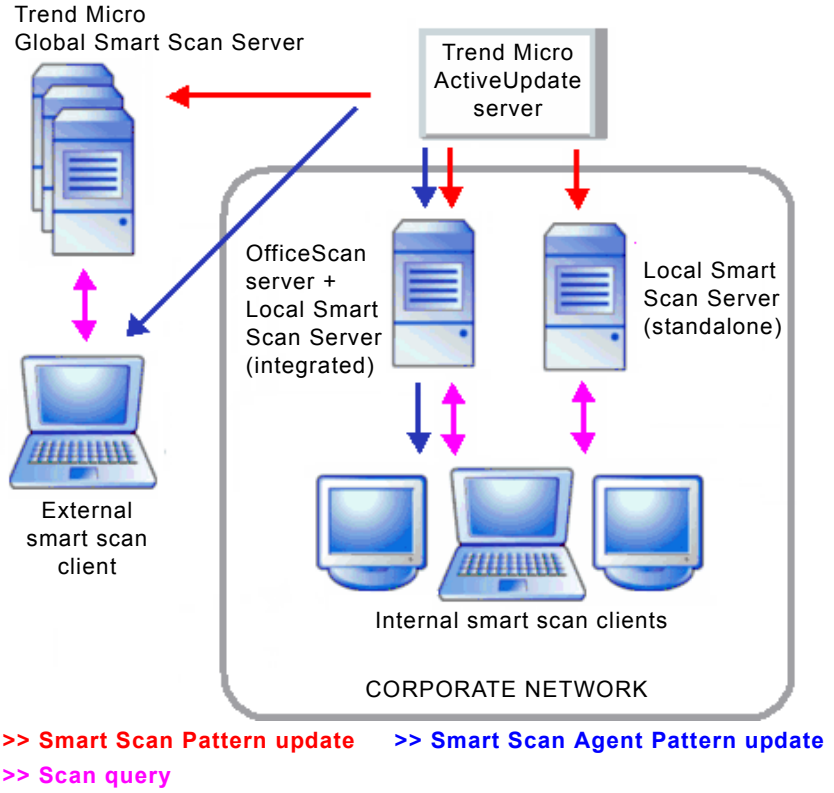
A new approach to handling the volume of threats has been pioneered by Trend Micro that aims to make Trend Micro customers immune to the threat of virus/malware volume. The technology and architecture used in this pioneering effort leverages technology that off load the storage of virus/malware signatures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

cloud. By off loading the storage of these virus/malware signatures to the cloud, Trend Micro is able to better protect customers against the future volume of emerging security risks.

The Trend Micro Smart Scan Solution

The smart scan solution makes use of lightweight patterns that work together to provide the same protection provided by conventional anti-malware and anti-spyware patterns. These patterns originate from the Trend Micro ActiveUpdate server and are made available to a Smart Scan Server and the OfficeScan client's update source (the OfficeScan Server or a custom update source).

FIGURE 1-1. The Trend Micro smart scan solution



Smart Scan Server

A Smart Scan Server hosts the **Smart Scan Pattern**. This pattern is updated hourly and contains the majority of pattern definitions. OfficeScan clients that use smart scan (referred to as "smart scan clients" in this document) do not download this pattern. Clients verify potential threats against the pattern by sending scan queries to the Smart Scan Server. In the smart scan solution, clients send identification information determined by Trend Micro technology to Smart Scan Servers. Clients never send the entire file and the risk of the file is determined using the identification information.

Smart Scan Server Types

The Smart Scan Server to which a client connects depends on the client's location. Internal smart scan clients connect to a *local Smart Scan Server*, while external smart scan clients connect to the *Trend Micro Global Smart Scan Server*. The following table provides a comparison between the two Smart Scan Server types:

TABLE 1-1. Comparison between Smart Scan Server types

BASIS OF COMPARISON	LOCAL SMART SCAN SERVER	GLOBAL SMART SCAN SERVER
Availability	Available for internal clients, which are clients that meet the location criteria specified on the OfficeScan Web console. See *Configuring Computer Location Settings* on page 3-32 for details on location criteria.	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 scan operations to the corporate network to optimize efficiency	A globally scaled Internet-based infrastructure that provides smart scan services to users who do not have immediate access to their corporate network

TABLE 1-1. Comparison between Smart Scan Server types (Continued)

BASIS OF COMPARISON	LOCAL SMART SCAN SERVER	GLOBAL SMART SCAN SERVER
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

OfficeScan Server

The OfficeScan server (or a custom update source if clients do not update directly from the OfficeScan server) hosts the **Smart Scan Agent Pattern**. This pattern is updated daily and contains all the other pattern definitions not found on the Smart Scan Pattern. Clients download this pattern from the OfficeScan server using the same methods for downloading other OfficeScan components.

Tip: You can configure clients to download the pattern from the Trend Micro ActiveUpdate server. Doing this enables external smart scan clients to keep protection current.

How a File's Reputation is Determined

The OfficeScan client, using the Smart Scan Agent Pattern and advanced filtering technology, can verify whether a file is infected without sending scan queries to the Smart Scan Server. The client only sends scan queries if it cannot determine the risk of the file during scanning. A client that cannot verify a file's risk locally and is unable to connect to a Smart Scan Server after several attempts:

- Flags the file for verification
- Temporarily allows access to the file

When connection to a Smart Scan 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.

Features and Benefits

Smart scan provides the following features and benefits:

- Provides fast, real-time security status lookup capabilities in the cloud
- Reduces the overall time it takes to deliver protection against emerging threats
- Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only need to be delivered to the cloud and not to many endpoints.
- Reduces the cost and overhead associated with corporate-wide pattern deployments
- Lowers kernel memory consumption on endpoints. Consumption increases minimally over time.

Trend Micro Smart Protection Network

The Trend Micro™ Smart Protection Network is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and Web threats. It powers both local and hosted solutions to protect users whether they are on the network, at home, or on the go, using light-weight 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.

File Reputation

File reputation technology from Trend Micro checks the reputation of each file against an extensive in-the-cloud database before permitting user access. Since the malware information is stored in the cloud, it is available instantly to all users. High performance content delivery networks and local caching servers ensure minimum latency during the checking process. The cloud-client architecture offers more immediate protection and eliminates the burden of pattern deployment besides significantly reducing the overall client footprint.

Chapter 2

Smart Scan Deployment

Topics in this chapter:

Scan Methods

In this OfficeScan version, you can configure clients to use either *smart scan* or *conventional scan*. 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 in this OfficeScan version

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 Scan 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 Scan Server.
		• If a client cannot verify a file's risk locally and is unable to connect to any Smart Scan Server after several attempts:
		  • The client flags the file for verification.
		  • The client allows temporary access to the file.

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

BASIS OF COMPARISON	CONVENTIONAL SCAN	SMART SCAN
		• When connection to a Smart Scan 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.
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

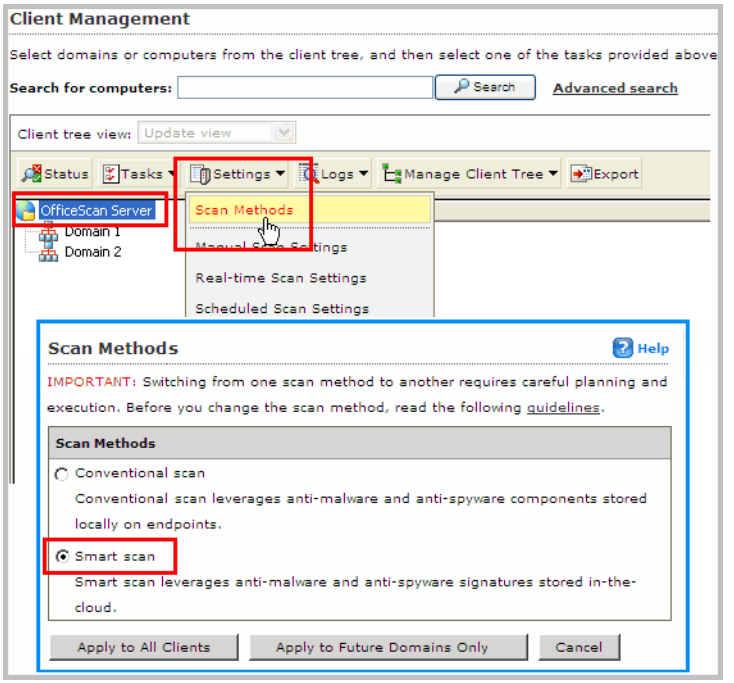
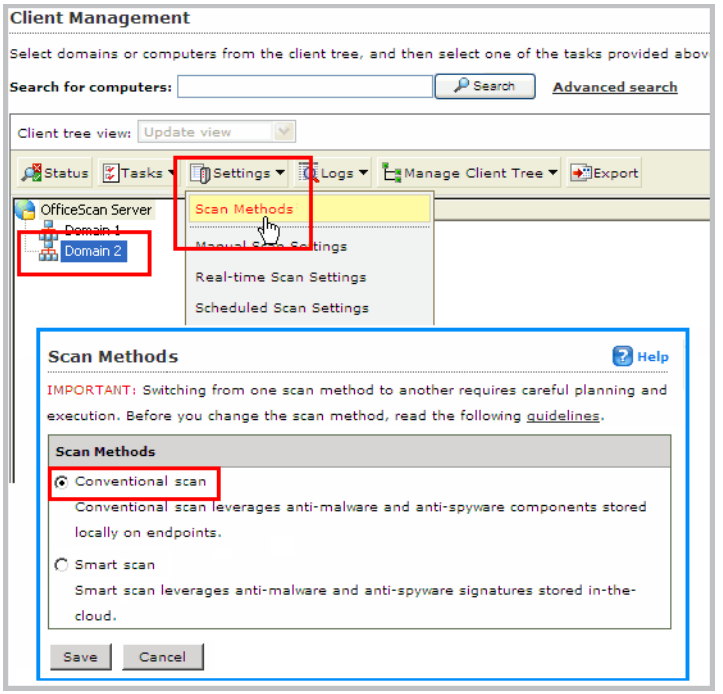


FIGURE 2-2. Conventional scan as the domain level scan method



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 is conventional 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 will manage will use conventional scan. Similarly, if you upgrade the OfficeScan server from an earlier version and automatic client upgrade is enabled, all clients managed by the server automatically use conventional scan after the upgrade.

Deployment Overview

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 local Smart Scan 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.

See *All Clients Use Smart Scan* on page 2-7 for details.

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.

See the following topics for details:

- *Most Clients Use Smart Scan* on page 2-8
- *Most Clients Use Conventional Scan* on page 2-16

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.

All Clients Use Smart Scan

There are two ways to deploy smart scan to all clients.

If you are performing fresh installations of the OfficeScan 10 server and clients, or if you are upgrading clients by moving them to an OfficeScan 10 server, perform the following tasks:

1. Perform a fresh installation of the OfficeScan server.

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

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

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

3. Prepare the smart scan environment.

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

4. Install the OfficeScan client.

   For details, see the *Administrator's Guide*.

5. If upgrading clients from a previous version:

   a. Record the server name and listening port. Specify this information on the OfficeScan 8.x/7.x server when moving clients.

      For details, see *Recording OfficeScan Server Information* on page A-2.

   b. Upgrade the clients by moving them to the OfficeScan 10 server.

      For details, see *Upgrading Clients by Moving Them to an OfficeScan 10 Server* on page A-2.

If upgrading the OfficeScan server directly on the host computer, perform the following tasks:

1. Prevent automatic updates and upgrade on clients.

   For details, see *Configuring Automatic Client Upgrade and Update Settings* on page A-6.

2. Upgrade the OfficeScan server.

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

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

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

4. Prepare the smart scan environment.

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

5. Upgrade clients.

   For details, see *Manually Upgrading Clients* on page A-4.

Most Clients Use Smart Scan

If most clients will use smart scan, set the root level scan method to smart scan. After setting the root level scan method:

- If you are upgrading the OfficeScan server and clients, check the client tree domains to determine the extent of the changes you need to make to the client tree structure. See *Deploying Smart Scan During an Upgrade* on page 2-9 for details.
- If you are performing server and client fresh installations, there are no domains in the client tree yet. These domains will be created in the client tree when you install clients. See *Deploying Smart Scan During Fresh Installations* on page 2-14 for details.

Deploying Smart Scan During an Upgrade

If you are upgrading the OfficeScan server and clients and want most clients to use smart scan, deploy smart scan during the upgrade.

The benefits of using this deployment method 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.

Before upgrading the server and clients, check the existing client tree domains. If you already have a well-defined structure (for example, domains represent client computers grouped by functions or geographical locations), it may not be reasonable to change the existing structure significantly.

Below are some guidelines that may help minimize changes to the current client tree structure:

- If all clients under a domain will use conventional scan, set the scan method for that domain to conventional scan.

  Note: If all clients under a domain will use smart scan, you do not need to modify the domain's scan method anymore because the root level scan method is smart scan.

- If clients under a particular domain will use both scan methods, perform any of the following tasks:
  - Since only a small the number of clients will use conventional scan, configure individual clients to use conventional scan.
  - Split the domain into two, with one domain applying one scan method and another applying the other scan method. For example, if the domain "US_Office" has 100 clients and 80 clients will use smart scan, rename the domain "US_Office - Smart Scan". Keep the 80 smart scan clients under this domain.

    For the other 20 clients, create a new domain named "US_Office - Conventional Scan". Set the domain's scan method to conventional scan, and then move clients to this domain.

Typical Upgrade Methods

This section discusses how you can upgrade the server/clients and deploy smart scan at the same time. The most common methods of upgrading the OfficeScan server and clients are as follows:

1. Perform a fresh installation of the latest OfficeScan server version on a computer and then move clients running an earlier OfficeScan version to this server. Clients that move to a new parent server automatically upgrade to that server's version.

   For details, see *Upgrade Method 1* on page 2-11.

2. Prevent automatic updates and upgrade on clients, upgrade the server directly on the host computer, and then manually upgrade clients individually or in groups.

   This upgrade method is effective if the server manages a large number of clients.

   For details, see *Upgrade Method 2* on page 2-13.

Note: You cannot deploy smart scan during the upgrade if you allow automatic client updates and upgrade. This is because clients automatically upgrade after server upgrade is complete and then use conventional scan, the default scan method.

Upgrade Method 1

Part 1: Steps to perform on the OfficeScan 8.x/7.x server:

1. Add a new client tree domain.
2. Move clients that will use conventional scan to this domain.

   For details on steps 1 and 2, see *Managing OfficeScan Domains* on page A-7.

Part 2: Steps to perform on the OfficeScan 10 server:

3. Perform fresh installation of the OfficeScan server.

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

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

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

5. Add a new client tree domain. This domain and the domain you just created on the OfficeScan 8.x/7.x console should have the same name.

   For details, see *Managing OfficeScan Domains* on page A-7.

   Note: If the domain names are not identical and clients move to the OfficeScan 10 server, the domain name in OfficeScan 8.x/7.x will be created in the OfficeScan 10 console. The root level scan method (smart scan) will be applied to clients belonging to the domain.

6. For the domain created in step 5, change the scan method to conventional scan.

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

7. Record the server name and server listening port. Specify this information on the OfficeScan 8.x/7.x server when moving clients.

   For details, see *Recording OfficeScan Server Information* on page A-2.

8. Prepare the smart scan environment.

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

Part 3: Steps to perform on the OfficeScan 8.x/7.x server:

9. Move clients to the OfficeScan 10 server.

   For details, see *Upgrading Clients by Moving Them to an OfficeScan 10 Server* on page A-2.

Upgrade Method 2

Part 1: Steps to perform on the OfficeScan 8.x/7.x server:

1. Add a new client tree domain.
2. Move clients that will use conventional scan to this domain.

   For details on steps 1 and 2, see *Managing OfficeScan Domains* on page A-7.
3. Prevent automatic updates and upgrade on clients.

   For details, see *Configuring Automatic Client Upgrade and Update Settings* on page A-6.
4. Upgrade the OfficeScan server.

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

Part 2: Steps to perform on the OfficeScan 10 server:

5. Change the root level scan method to smart scan.
6. For the domain created in step 1, change the scan method to conventional scan.

   For details, see *Configuring Scan Methods* on page A-1.
7. Prepare the smart scan environment.

   For details, see *Preparing the Smart Scan Environment* on page 3-2.
8. Upgrade clients.

   For details, see *Manually Upgrading Clients* on page A-4.

Deploying Smart Scan During Fresh Installations

If you are performing fresh installations of the OfficeScan server and clients and want most clients to use smart scan, the typical smart scan deployment workflow is as follows:

1. Perform a fresh installation of the OfficeScan server.

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

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

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

3. Identify the target computer to which you will install the first OfficeScan client, and the network domain to which it belongs.

4. Check the client grouping setting by navigating to **Networked Computers > Global Client Settings > Client Grouping**. This setting determines the name of the network domain that will be created in the client tree when the first OfficeScan client is installed.

5. Install the OfficeScan client.

   For details, see the *Administrator's Guide*.

   The client automatically uses smart scan after the installation.

   The network domain name appears on the client tree and becomes the first client tree domain. The scan method for this domain is smart scan.

6. Install the OfficeScan client to another target computer belonging to the same network domain.

   The client will be grouped under the same client tree domain and will use smart scan.

   If you want this client to use conventional scan, you have two options:

   Option 1: Change the client's scan method directly

   a. Select the client from the client tree.

   b. Change its scan method to conventional scan.

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

   Option 2: Add a new client tree domain

   a. From the Web console, add a new client tree domain.

For details, see *Managing OfficeScan Domains* on page A-7.

b. Assign conventional scan as the domain's scan method.

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

c. Move the client to the new domain.

For details, see *Managing OfficeScan Domains* on page A-7.

When a client switches to conventional scan for the first time, the client downloads the full versions of the Virus Pattern and Spyware-active Monitoring Pattern.

- Consider moving the client during off-peak hours to ensure the download process finishes within a short amount of time.
- Also consider switching when the client is not scheduled to update from the server.
- You can also temporarily disable "Update Now" on the client and re-enable it after the client has changed its scan method.

7. Install more clients. When installing clients, always check the network domain to which the target computer belongs.

If the network domain does not exist on the client tree, a new domain with the same name as the network domain will be created in the client tree. The client will be grouped under this domain. This new domain will apply smart scan.

If you do not want the client to use smart scan, see the options provided in step 6. You can also perform the following steps before installing the client:

a. Check the network domain to which the target computer belongs.

b. Add a new domain in the client tree with the same name as the network domain.

For details, see *Managing OfficeScan Domains* on page A-7.

c. Change the domain's scan method to conventional scan.

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

d. Install the client.

For details, see the *Administrator's Guide*.

Most Clients Use Conventional Scan

If most clients will use conventional scan, you can postpone smart scan deployment until the server and all clients have been installed or upgraded. Perform the following tasks:

1. Install or upgrade the server and clients without configuring scan method settings.

   If you are upgrading OfficeScan, ensure that clients have up-to-date components before upgrading. If client components are up-to-date, clients only need to download incremental versions of pattern files. This reduces the network bandwidth consumed during the upgrade.

   For details on installing the server, or upgrading the server and clients, see the *Installation and Upgrade Guide*.

   For details on installing clients, see the *Administrator's Guide*.

2. Switch clients to smart scan after the fresh installation or upgrade.

   For details, see the *Administrator's Guide* topic on switching from one scan method to another.

   A client that switches to smart scan for the first time downloads a new pattern called Smart Scan Agent Pattern. The client also stops updating but does not remove the Virus Pattern and Spyware-active Monitoring Pattern, the two components used only during conventional scan. The client will update and use these patterns again if it switches back to conventional scan in the future.

Note: The Smart Scan Agent Pattern is not removed when a smart scan client switches to conventional scan.

Chapter 3

Smart Scan Environment

Topics in this chapter:

Preparing the Smart Scan Environment

Before deploying smart scan to clients, ensure that the smart scan environment has been properly set up. Check the following:

1. Smart Scan Servers

   Smart scan clients connect to a Smart Scan Server to send scan queries and verify a file's risk against the Smart Scan Pattern. The Smart Scan Server to which a client connects depends on the client's location. *Internal* clients connect to a *local* Smart Scan Server, while *external* clients connect to the Trend Micro Global Smart Scan Server.

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

2. Client connection proxy settings

   If connection to the Global Smart Scan Server requires proxy authentication, specify authentication credentials. For details, see *Configuring External Proxy Settings* on page 3-27.

   Configure internal proxy settings clients will use when connecting to a local Smart Scan Server. See *Configuring Internal Proxy Settings* on page 3-28 for details.

3. Smart Scan Server list

   Add the Smart Scan Servers you have set up to the Smart Scan Server list. Clients refer to the list to determine which Smart Scan Server to connect to. See *Configuring the Smart Scan Server List* on page 3-29 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 global or a local Smart Scan Server. This ensures that clients remain protected regardless of their location.

   To configure location settings, see *Configuring Computer Location Settings* on page 3-32.

5. OfficeScan server

   Ensure that clients can connect to the OfficeScan server. Only online clients will be notified to switch to smart scan. Offline clients are notified when they become

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

Also verify that the OfficeScan server has the latest components because smart scan clients need to download the Smart Scan Agent Pattern from the server. See the *Administrator's Guide* for details on updating components on the server.

6. 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 Local Smart Scan Servers

OfficeScan provides two types of local Smart Scan Servers.

Integrated Smart Scan Server

The OfficeScan Setup program includes an integrated Smart Scan 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 Scan Server

A standalone Smart Scan 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 Scan 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 Scan 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 scan queries. See *Recommended Capacity Examples* on page 3-8 for details.

Recommended System Requirements

The following are required to install the integrated Smart Scan Server and OfficeScan server:

TABLE 3-1. OfficeScan server and integrated Smart Scan server requirements

RESOURCE	REQUIREMENTS
Operating system	**Windows 2000** • Microsoft™ Windows™ 2000 Server with Service Pack 4 • Windows 2000 Advanced Server with Service Pack 4 • Microsoft Cluster Server 2000 **Windows 2003** • Windows Server™ 2003 (Standard, Enterprise, and Datacenter Editions) with Service Pack 2 or later, 32-bit and 64-bit versions • Windows Server 2003 R2 (Standard, Enterprise, and Datacenter Editions) with Service Pack 2 or later, 32-bit and 64-bit versions • Windows Storage Server 2003 R2, 32-bit and 64-bit versions • Microsoft Cluster Server 2003 **Windows 2008** • Windows Server 2008 (Standard, Enterprise, Datacenter and Web Editions) with Service Pack 1 or later, 32-bit and 64-bit versions • Microsoft Cluster Server 2008 OfficeScan cannot be installed if Windows 2008 runs on the Server Core or Hyper-V™ environment.

TABLE 3-1. OfficeScan server and integrated Smart Scan server requirements

RESOURCE	REQUIREMENTS
Virtualization	OfficeScan supports server installation on guest Windows 2000/2003/2008 operating systems hosted on the following virtualization applications: • VMware™ ESX™/ESXi Server 3.5 (Server Edition) • VMware Server 1.0.3 or later (Server Edition) • VMware Workstation and Workstation ACE Edition 6.0 The server can also be installed on guest Windows 2000 and 2003 (32-bit) operating systems hosted on Microsoft Virtual Server 2005 R2 with Service Pack 1.
Hardware	**Processor** • At least 1.86GHz Intel™ Core2Duo™ **RAM** • 1GB minimum **Available disk space** • 2.8GB minimum if installing locally • 3.2GB minimum if installing remotely **Others** • Gigabit Network Interface Card (NIC) • Monitor that supports 800 x 600 resolution at 256 colors or higher

TABLE 3-1. OfficeScan server and integrated Smart Scan server requirements

RESOURCE	REQUIREMENTS

Web server	• Microsoft Internet Information Server (IIS)
	  • on Windows 2000: version 5.0
	  • on Windows Server 2003: version 6.0
	  • on Windows Server 2008: version 7.0
	• Apache™ Web server 2.0.x
	Note: If Apache Web server exists on the computer but the version is not 2.0.x, OfficeScan will install and use version 2.0.63. The existing Apache Web server is not removed.

Others	• Administrator or Domain Administrator access on the server computer • File and printer sharing for Microsoft Networks installed on the server computer

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

TABLE 3-2. Standalone Smart Scan Server requirements

RESOURCE	REQUIREMENTS
Virtualization	• VMware ESXi Server 3.5 Update 2 • VMware ESX Server 3.5 or 3.0 • VMware Server 2.0 **Note:** A purpose-built, hardened, performance-tuned 64-bit Linux operating system is included with Trend Micro Smart Scan Server.

TABLE 3-2. Standalone Smart Scan Server requirements (Continued)

RESOURCE	REQUIREMENTS
Hardware	• 2.0GHz Intel Core2Duo 64-bit processor supporting Intel Virtualization Technology™ or equivalent • 512MB of RAM • 10GB of available disk space **Note:** Smart Scan Server automatically partitions the detected disk space as required. • Monitor that supports 800 x 600 resolution with 256 colors or higher
Virtual machine	• Red Hat™ Enterprise Linux™ 5 64-bit for VMware ESX 3.5, VMware ESXi 3.5, or VMware Server 2.0 • Red Hat Enterprise Linux 4 64-bit for VMware ESX 3.0 • 512MB RAM • 2.0GHz processor • 10GB available disk space • 1 network device **Note:** Install VMware Tools after successfully installing Smart Scan Server.
Browser	Microsoft Internet Explorer 6.0 or later (For access to the Web console)

Environment Considerations

Consider the following when setting up local Smart Scan Servers:

- Smart Scan Server is a CPU-bound application. This means that increasing CPU resources increases the number of simultaneous client connections handled. For standalone servers, the number of processors allocated to the virtual machine will affect the performance of the server.
- Network bandwidth may become a bottleneck depending on network infrastructure and the number of simultaneous connections.
- Additional memory might be required if there is a large number of concurrent connections between Smart Scan Servers and OfficeScan clients.

Recommended Capacity Examples

A standalone Smart Scan Server installed on a virtual machine with the specifications described in *Table 3-1* can support up to 50,000 clients.

TABLE 3-1. Hardware used in example (standalone server)

HARDWARE	SPECIFICATIONS
Server Model	Dell™ PowerEdge™ 2950
Processor	Intel Quad Core Xeon™ E5320 x 2, 2 x 4MB Cache
Memory	DDR-2 667MHz ECC 4GB
Hard Disk	73GB, 15K RPM SAS, RAID-1
Network Card	Broadcom™ NetXtreme™ II 5708 Gigabit Ethernet Card

An integrated Smart Scan Server installed on a computer with the specifications described in *Table 3-2* can support up to 1,000 clients.

TABLE 3-2. Hardware used in example (integrated server)

HARDWARE	SPECIFICATIONS
Operating system	Windows Server 2003 (32-bit) with Service Pack 2
Processor	1.86GHz Intel Core2Duo
Memory	4GB

Performance Considerations

- Because the integrated Smart Scan 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 Scan Servers as the primary smart scan source for clients and the integrated server as a backup.
- Avoid running Scheduled Scan on OfficeScan clients simultaneously. Stagger the scan in groups.
- Avoid configuring all OfficeScan clients from performing Scan Now simultaneously. For example, you can disable the "Perform scan now after update" option on the Web console.
- OfficeScan clients registered to the same OfficeScan server use the corresponding Smart Scan Server.
- If you install the integrated Smart Scan 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.

Installing the Standalone Smart Scan Server

The standalone Smart Scan Server installation process formats your existing system for program installation. VMware installation requires the creation of a virtual machine before installation.

You need the following information for the installation:

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

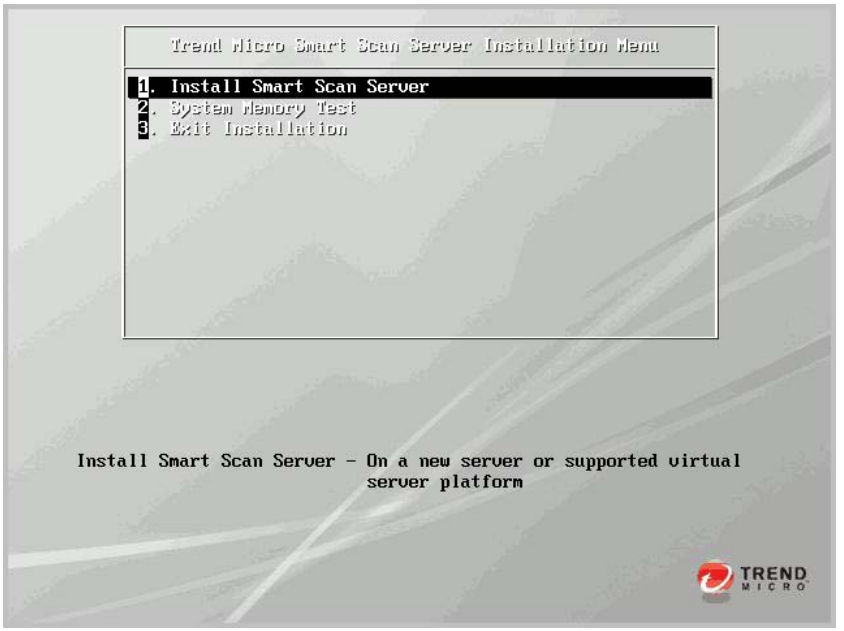
Running the Installation Program

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

To install the standalone Smart Scan Server:

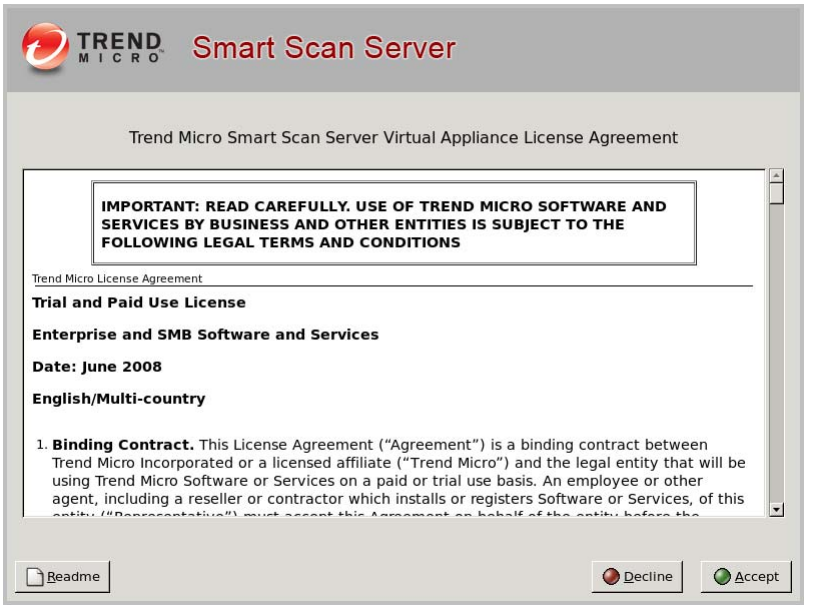
1. Create a virtual machine on your VMware ESX server and specify the virtual machine to boot from the Smart Scan Server ISO.
2. Power on the virtual machine. The Installation Menu displays with the following options:
   - **Install Smart Scan Server**—Select this option to install Smart Scan Server 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 Scan Server**. The License Agreement screen appears.

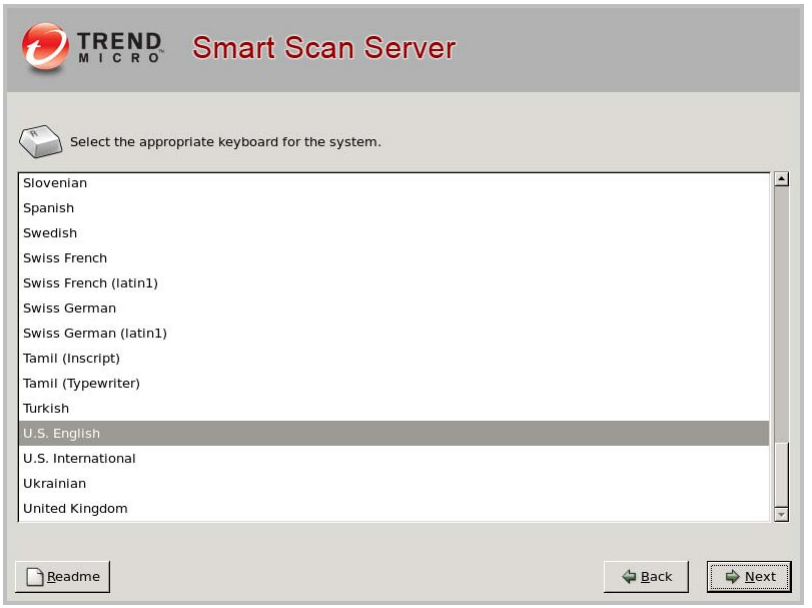
FIGURE 3-2. License Agreement screen



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

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

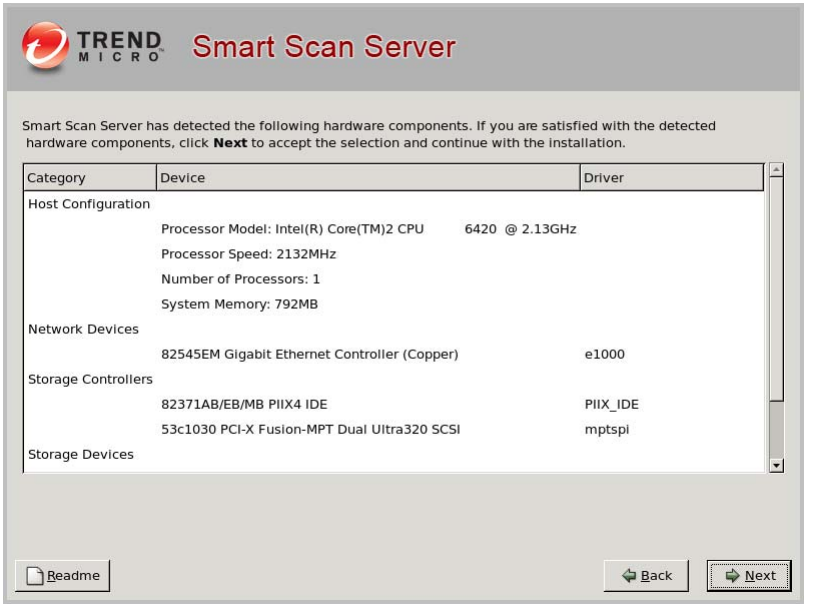
FIGURE 3-3. Keyboard Selection screen



5. 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 and no network device, installation cannot continue.

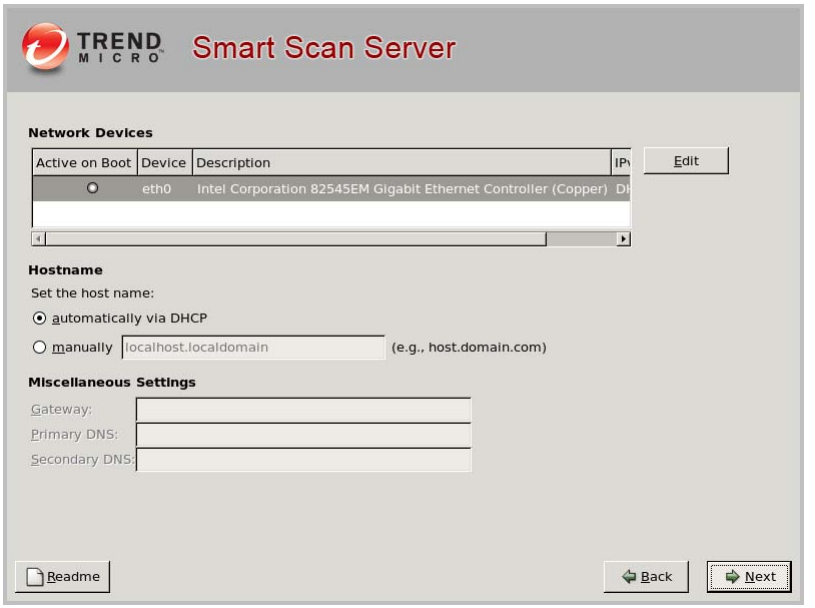
FIGURE 3-4. Hardware Components Summary screen



6. 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.)

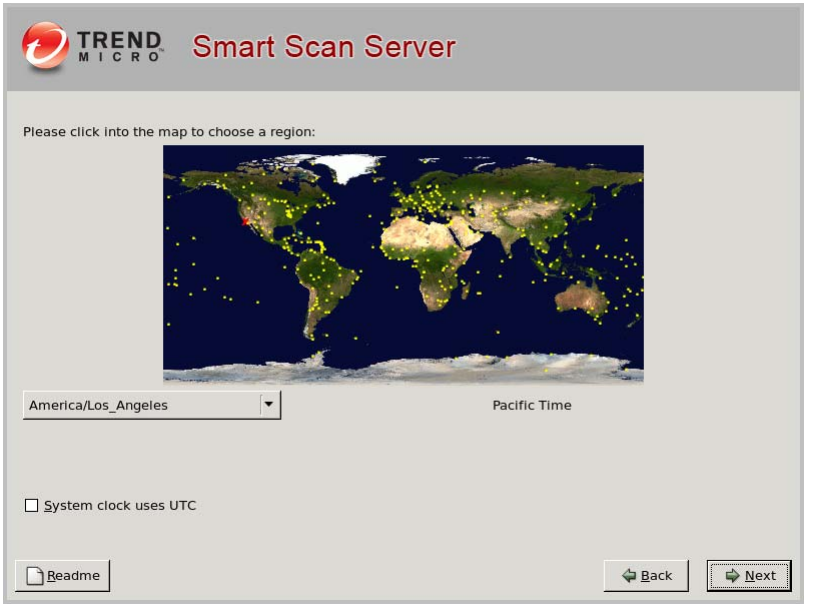
FIGURE 3-5. Network Settings screen



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

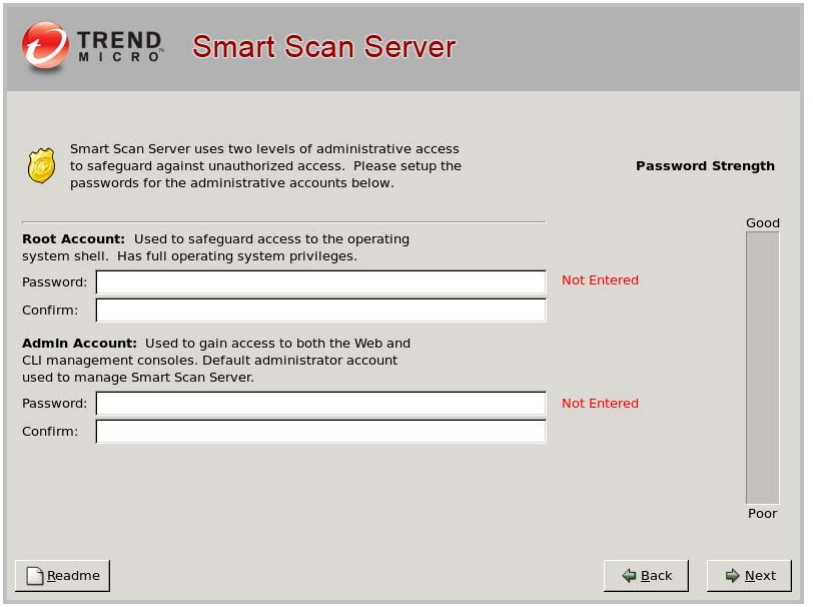
7. Configure network settings.
   a. Specify the Active on Boot network devices, host name, and miscellaneous settings. If you specify the host name manually, the miscellaneous settings are also configurable.
   b. Click **Next** to continue. The Time Zone screen appears.

FIGURE 3-6. Time Zone screen



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

FIGURE 3-7. Authentication screen



9. Specify passwords for the " root" and "admin" accounts. Smart Scan Server uses two different levels of administrator types to secure the server.

Tip: For best security, create a highly unique password known only to you. Use both upper and lower case alpha characters, numerals, and special characters on your keyboard to create your password. The password must be a minimum of 6 characters and a maximum of 32 characters.

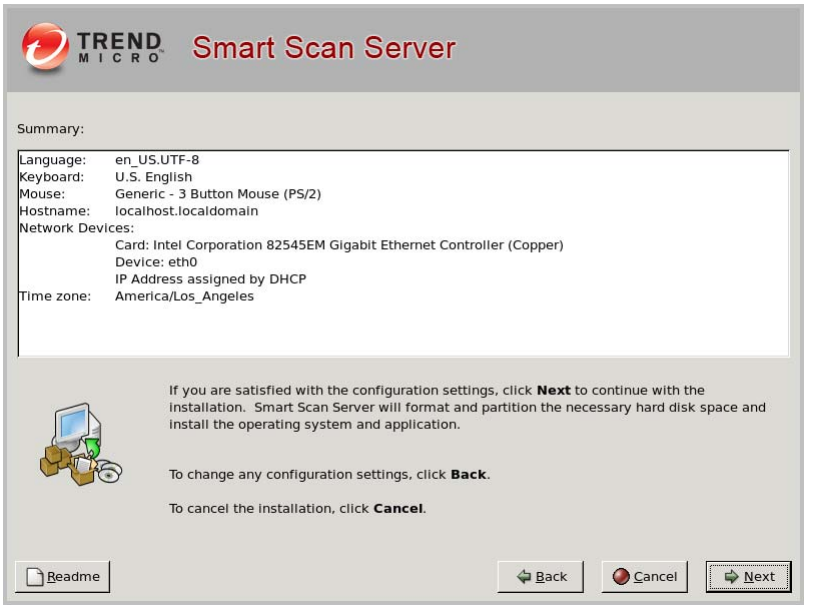
- **Root account**—This account is used to gain access to the operating system shell and has all rights to the server. This account includes the most privileges.
- **Admin account**—This account is the default administration account used to access the Smart Scan Server Web and CLI product consoles. This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

Tip: Trend Micro recommends using a strong, unique password.

a. Type the "root" and "admin" passwords.

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

FIGURE 3-8. Installation Summary screen



10. 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.

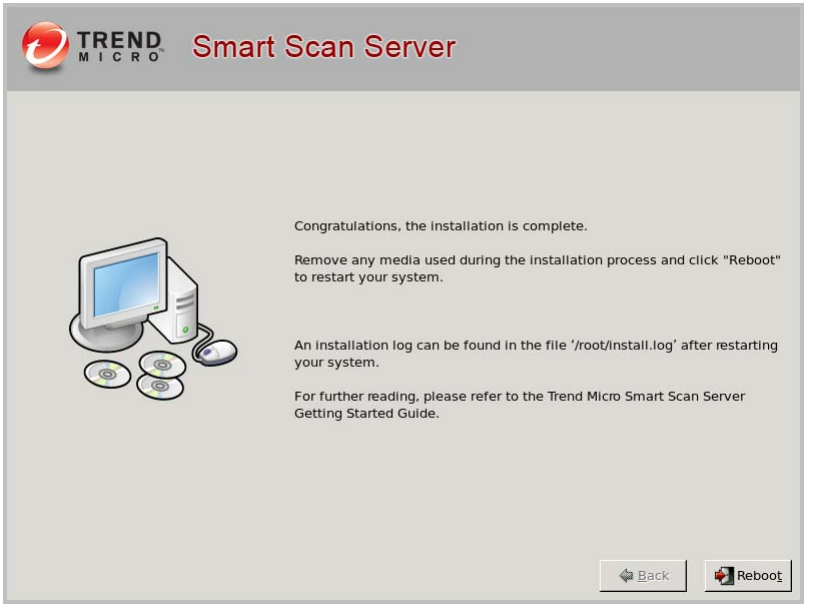
---

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 Progress screen

11. A message appears when the installation is complete. The installation log is saved in the /root/install.log file for reference.

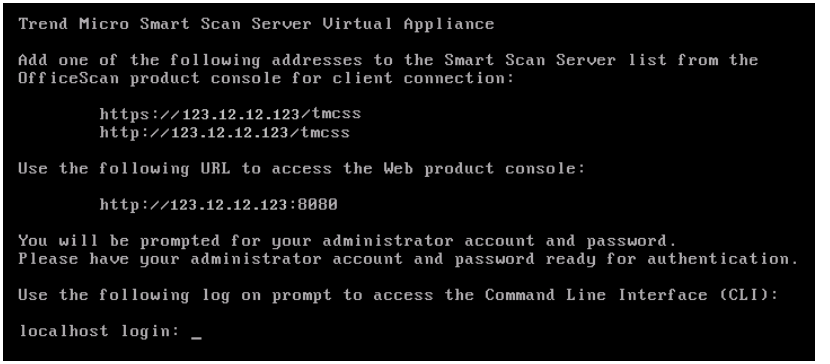
FIGURE 3-10. Installation Complete screen



12. Click **Reboot** to restart the virtual machine. The initial 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 Scan Server is installed.

FIGURE 3-11. CLI logon screen



13. Use `admin` to log on to the CLI or the Web console to manage Smart Scan 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 housekeeping tasks.

Post-installation

The following are recommended post-installation tasks:

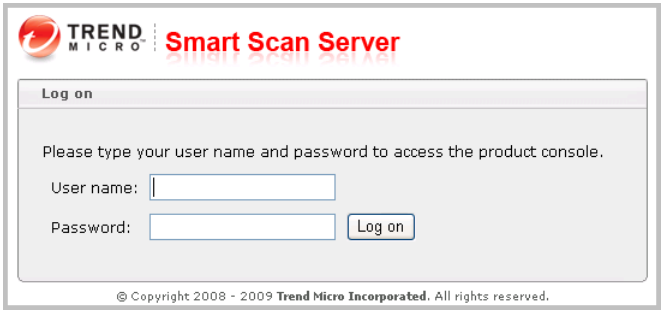
- After successfully installing Smart Scan Server, install VMware™ Tools. Refer to VMware documentation for more information.
- If your network uses a proxy server, configure proxy settings first. See *Configuring Proxy Settings* on page 4-14.

Logging On to the Standalone Server

Once Smart Scan Server has restarted, log on using the CLI or Web console.

- To log on to the CLI console, type the administrator user name (`admin`) and password. Use the `admin` account to log on to the CLI shell if you need to perform additional configuration, troubleshooting, or housekeeping tasks.
- To log on to the Web console, open a Web browser and type the URL indicated on the initial CLI banner. Log on to the Web console to perform post installation tasks, such as configuring proxy settings.

FIGURE 3-12. Log on screen



Note: Client connection addresses are used for configuring the OfficeScan Server Smart Scan Server list as a part of the smart scan solution.

For information on managing the server's settings, see *Managing the Standalone Smart Scan Server* on page 4-8.

Installing the Integrated Smart Scan Server

The integrated Smart Scan Server installs with the OfficeScan server. For installation 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 scan:

- Antivirus
- Web Reputation and Anti-spyware

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

Client Connection Protocols

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

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

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

OFFICESCAN WEB SERVER SETTINGS	OFFICESCAN SERVER SSL PORT	INTEGRATED SMART SCAN 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

TABLE 3-3. SSL port numbers for the OfficeScan server and integrated Smart Scan Server (Continued)

OFFICESCAN WEB SERVER SETTINGS	OFFICESCAN SERVER SSL PORT	INTEGRATED SMART SCAN SERVER SSL PORT
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

Integrated Smart Scan Server Reactivation

If you did not install the integrated Smart Scan Server during OfficeScan server installation but now want to use it in your smart scan environment, reactivate the server by performing the following steps.

To reactivate the integrated Smart Scan 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,C:\Program Files\Trend
Micro\OfficeScan\PCCSRV\WSS\isapi,,5
[WSS_WEB_SERVER]
ServerPort=8082
IIS_VhostName=Smart Scan 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,C:\Program Files\Trend Micro\OfficeScan\PCCSRV\WSS\isapi,,<value>

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

- If using Apache Web server:

```
[WSS_VIRDIR_INFO]
ROOT=/tmcss,C:\Program Files\Trend
Micro\OfficeScan\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 Scan 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 Scan Server**.
   e. On the screen that displays, click **Test Connection**. Connection with the integrated server should be successful.

Configuring External Proxy Settings

Clients can use the proxy settings configured in Internet Explorer to connect to the Trend Micro Global Smart Scan Server. 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**.

Configuring Internal Proxy Settings

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

OfficeScan Server Computer

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

Local Smart Scan Servers

Local Smart Scan Servers include all standalone Smart Scan Servers and the integrated Smart Scan Server of other OfficeScan servers. Clients connect to the servers to send scan 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**.

Configuring the Smart Scan Server List

Add the Smart Scan Servers you have set up to the Smart Scan Server list. Clients refer to the list to determine which Smart Scan 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 Scan Servers, assign a standalone Smart Scan 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 scan queries.

To configure the Smart Scan Server list:

PATH: SMART SCAN > SCAN 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 SCAN > SCAN SOURCE > INTERNAL CLIENTS

1. Click the **standard list** link.
2. In the screen that opens, click **Add** and specify the Smart Scan Server's address (in URL format).

To obtain the Smart Scan Server address:

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

Tip: Because the integrated Smart Scan 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 Scan Server as the primary scan source and the integrated server as a backup source.

---

3. Click **Test Connection** to verify if connection to the server can be established. Click **Save** when the test connection is successful.
4. Click the link under **Smart Scan Server Address** to modify the server's address.
5. To open the console of a local Smart Scan Server, click **Launch console**.
   - For the integrated Smart Scan Server, the server's configuration screen displays.
   - For standalone Smart Scan Servers and the integrated Smart Scan Server of another OfficeScan server, the console logon screen displays.
6. To delete an entry, select the check box for the server and click **Delete**.
7. To export the list to a .dat file, click **Export** and then click **Save**.
8. 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.
9. 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.
10. 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 SCAN > SCAN SOURCE > INTERNAL CLIENTS

1. Click **Add**.
2. In the screen that opens, specify the following:
   - IP address range
   - Proxy settings clients will use to connect to the local Smart Scan Servers
3. Specify the Smart Scan Server's address (in URL format).

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

   Tip: Because the integrated Smart Scan 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 Scan Server as the primary scan source and the integrated server as a backup source.

4. Click **Test Connection** to verify if connection to the server can be established. Click **Save** when the test connection is successful.
5. To open the console of a local Smart Scan Server, click **Launch console**.
   - For the integrated Smart Scan Server, the server's configuration screen displays.
   - For standalone Smart Scan Servers and the integrated Smart Scan Server of another OfficeScan server, the console logon screen displays.
6. To delete an entry, click the icon under **Delete**.
7. 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.

8. Click **Save**.
9. Back in the Smart Scan Source screen, select whether to refer to the standard list if the client is unable to connect to any server on the custom list.
10. To modify an IP address range and its corresponding custom list, click the link under **IP Range**.
11. To export the custom lists to a .dat file, click **Export** and then click **Save**.
12. 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.

Configuring Computer Location Settings

OfficeScan includes an awareness location function that identifies the client computer's location and determines whether the client connects to the global or a local Smart Scan Server. This ensures that clients remain protected regardless of their location.

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 client's location is internal and the client will connect to a local Smart Scan Server. Otherwise, the computer's location is external and the client will connect to the Global Smart Scan Server.

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 3-34 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

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 connects to local Smart Scan Servers.

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.
- 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 Smart Scan Clients and Servers

Topics in this chapter:

Managing Smart Scan Clients

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

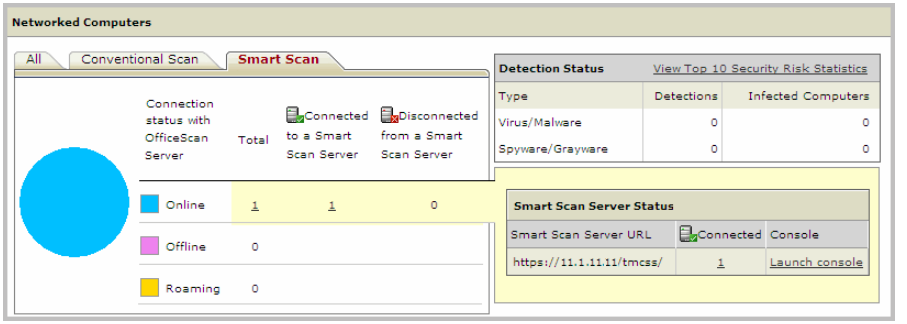
Client Information

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 Summary screen



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

---

Note: Only online clients can report their connection status with Smart Scan Servers.

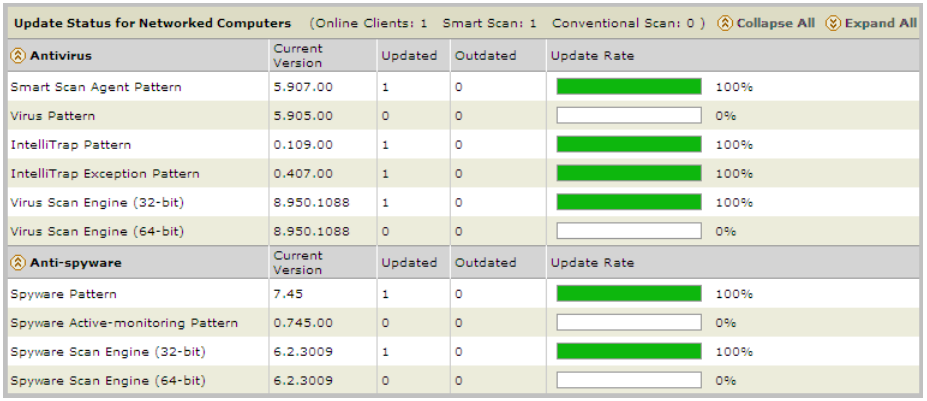
If clients are disconnected from a Smart Scan Server, restore the connection by performing the steps in *A Client Cannot Connect to a Smart Scan Server* on page 5-3.

- The number of detected security risks
- The computers where the security risks were detected
- A list of Smart Scan Servers

- The number of clients connected to each Smart Scan Server. Clicking the number opens the client tree where you can manage client settings.
- For each Smart Scan Server, a link that launches the server's console
- A **More** link (if you have clients connecting to more than two Smart Scan Servers) that opens a screen where you can:
  - View all the local Smart Scan 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.

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



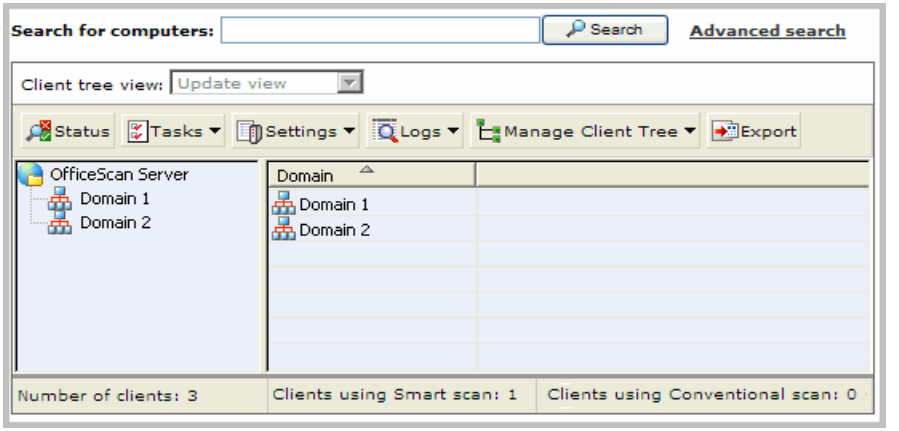
Update Status for Networked Computers (Online Clients: 1 Smart Scan: 1 Conventional Scan: 0) Collapse All Expand All

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%

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 *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 Scan Server is available for a client
- The URL of the Smart Scan 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 a smart scan client's connection status with the OfficeScan server and Smart Scan Server (local or global).

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

- Real-time Scan is disabled.
- Real-time Scan service stops. 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.
- Smart scan client is not connected to any Smart Scan 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
	The client can connect to a Smart Scan Server. All services work properly.
	The client can connect to a Smart Scan Server. Real-time Scan is disabled.
	The client can connect to a Smart Scan Server. Real-time Scan Service was stopped.
	The client cannot connect to a Smart Scan Server. Real-time Scan is enabled.
	The client cannot connect to a Smart Scan Server. Real-time Scan is disabled.
	The client cannot connect to a Smart Scan Server. 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
	The client can connect to a Smart Scan Server. Real-time Scan is enabled.
	The client can connect to a Smart Scan Server. Real-time Scan is disabled.
	The client can connect to a Smart Scan Server. Real-time Scan Service was stopped.
	The client cannot connect to a Smart Scan Server.
	The client cannot connect to a Smart Scan Server. Real-time Scan is disabled.
	The client cannot connect to a Smart Scan Server. Real-time Scan Service was stopped.

Roaming Clients

Roaming clients cannot update components from, nor send logs to, the OfficeScan server. The OfficeScan server also cannot manage roaming clients, including initiating tasks and deploying client settings. 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 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 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, navigate 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
	The client can connect to a Smart Scan Server. Real-time Scan is enabled.
	The client can connect to a Smart Scan Server. Real-time Scan is disabled.
	The client can connect to a Smart Scan Server. Real-time Scan Service was stopped.
	The client cannot connect to a Smart Scan Server. Real-time Scan is disabled.
	The client cannot connect to a Smart Scan Server. Real-time Scan is disabled.
	The client cannot connect to a Smart Scan Server. Real-time Scan Service was stopped.

Managing the Standalone Smart Scan Server

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

Using the Product Console

The product console consists of the following elements:

- **Main menu**—Provides links to the Summary, Update, and Administration screens.
- **Work area**—View summary information and component status, configure settings, update components, and perform administrative tasks.

FIGURE 4-4. Product console

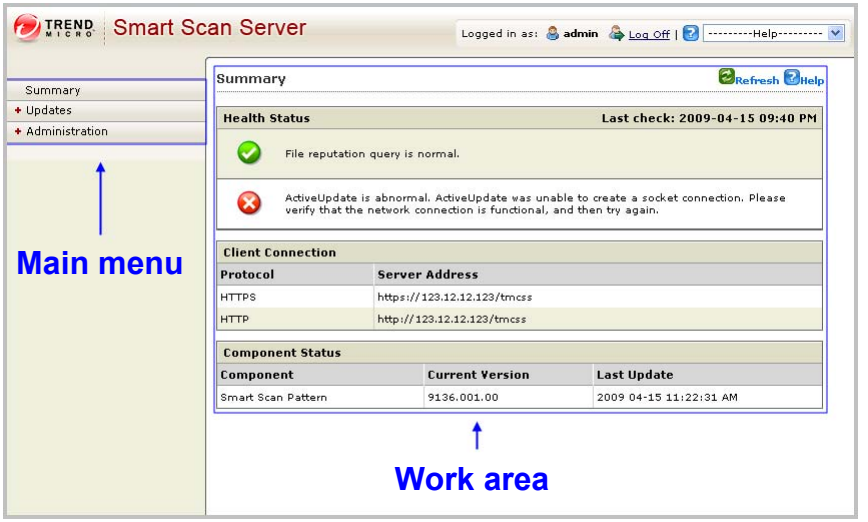


TABLE 4-4. Contents of Smart Scan Server Main Menu

MAIN MENU	
Summary	Displays the Health Status, Client Connection, and Component Status.
Updates	Provides options for configuring scheduled updates, proxy server settings, and manual program updates.
Administration	Provides options to configure SNMP service and collect diagnostic information for troubleshooting.

Accessing the Product Console

Upon opening the Web console, the initial screen displays the status summary for Smart Scan Server. To access the Web console:

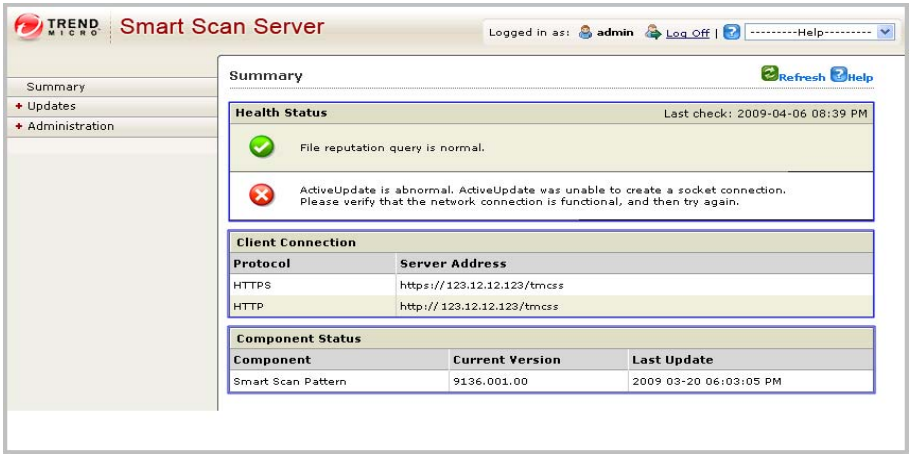
1. Open a Web browser and type the URL indicated on the initial CLI banner.
2. Type `admin` for the user name and the password in the corresponding fields.
3. Click **Log on**.

Using the Summary Screen

The Summary screen displays the **Health Status**, **Client Connection**, and **Component Status**.

Smart Scan Server supports both HTTP and HTTPS protocols for client connection purposes. HTTPS provides a more secure connection while HTTP uses less bandwidth.

FIGURE 4-5. Summary Screen



Note: Client connection addresses are used for configuring the Smart Scan Server list on the OfficeScan Web console as a part of the smart scan solution.

Updating Components

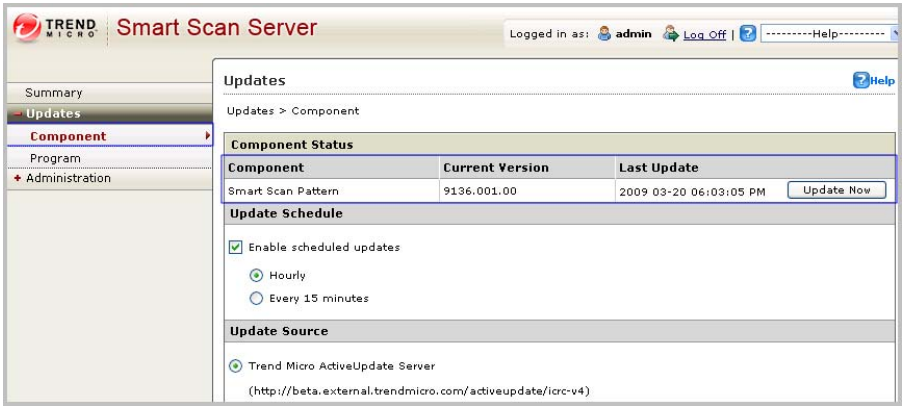
The effectiveness of Smart Scan Server depends upon using the latest pattern files. Trend Micro releases new versions of the *Smart Scan Pattern* files hourly.

Tip: Trend Micro recommends updating components immediately after installation.

Configuring Manual Updates

Smart Scan Server can perform manual updates for the *Smart Scan Pattern* file.

FIGURE 4-6. Configuring manual updates



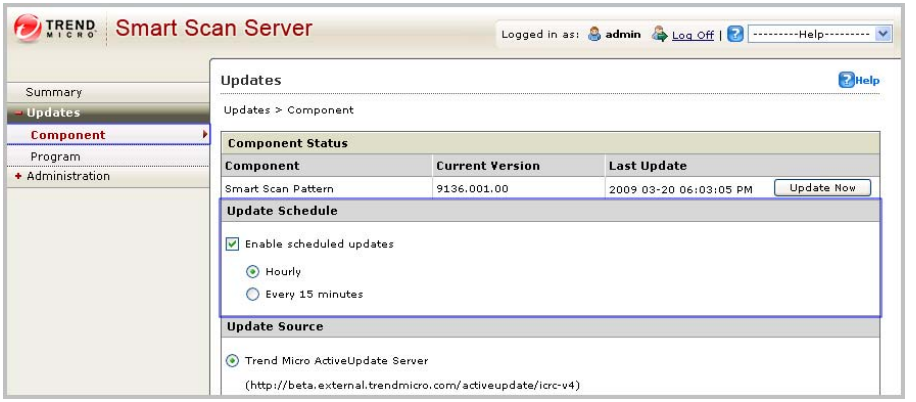
To configure manual updates:

1. Log on to the Web console.
2. Click **Updates** from the main menu. A drop down menu appears.
3. Click **Component** from the drop down menu. The Component screen appears.
4. Click **Update Now**.

Configuring Scheduled Updates

Smart Scan Server can perform scheduled updates for the *Smart Scan Pattern* file.

FIGURE 4-7. Configuring scheduled updates



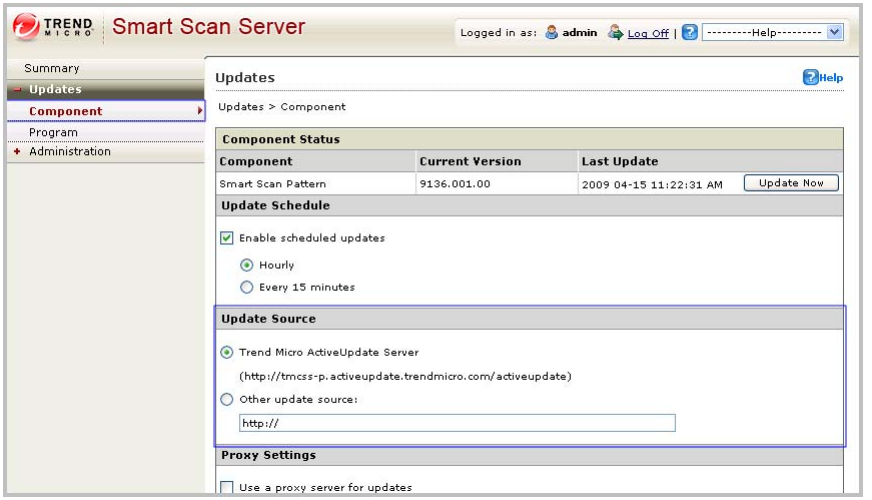
To configure scheduled updates:

1. Log on to the Web console.
2. Click **Updates** from the main menu. A drop down menu appears.
3. Click **Component** from the drop down menu. The Component screen appears.
4. Select **Enable scheduled updates**.
5. Select either hourly or 15 minute updates.
6. Click **Save**.

Configuring an Update Source

Use this screen to specify the update source. The default update source is Trend Micro ActiveUpdate Server.

FIGURE 4-8. Configuring an update source



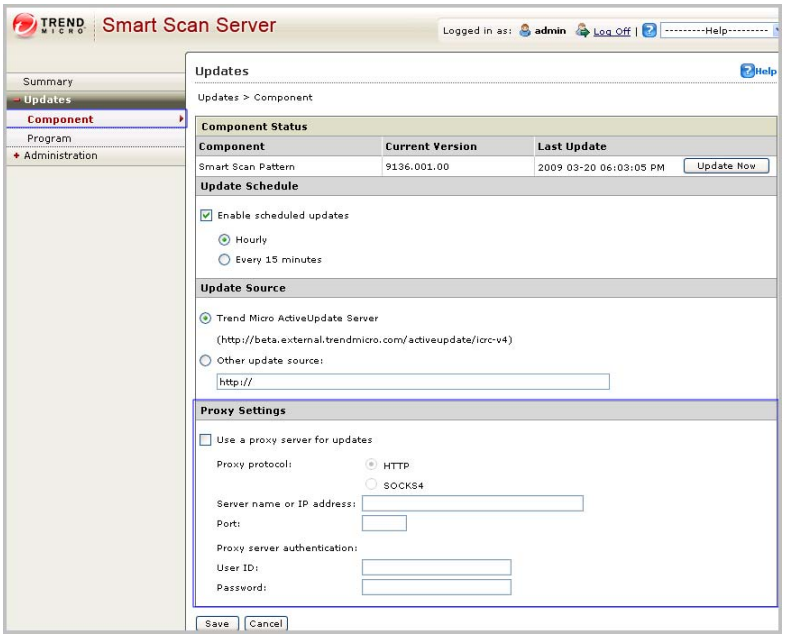
To configure an update source:

1. Log on to the Web console.
2. Click **Updates** from the main menu. A drop down menu appears.
3. Click **Component** from the drop down menu. The Component screen appears.
4. Select **Trend Micro ActiveUpdate Server** or select **Other update source** and type a URL.
5. Click **Save**.

Configuring Proxy Settings

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

FIGURE 4-9. Configuring proxy settings



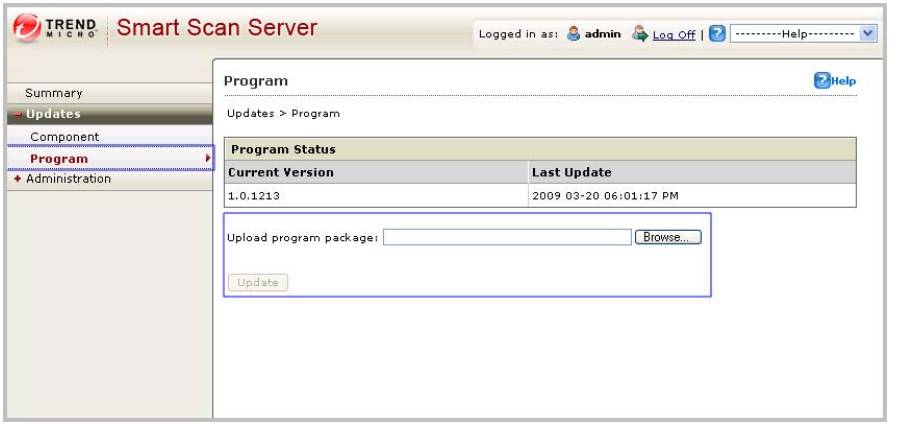
To configure proxy settings:

1. Log on to the Web console.
2. Click **Updates** from the main menu. A drop down menu appears.
3. Click **Component** from the drop down menu. The Component screen appears.
4. Select the **Use a proxy server for updates** check box.
5. Select **HTTP** or **SOCKS4** for the **Proxy protocol**.
6. Type the server name or IP address.
7. Type the port number.
8. If your proxy server requires credentials, type the **User ID** and **Password**.
9. Click **Save**.

Updating the Program

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

FIGURE 4-10. Updating the program



To update the program:

1. Log on to the Web console.
2. Click **Updates** from the main menu. A drop down menu appears.
3. Click **Program** from the drop down menu. The Program screen appears.
4. Click **Browse**... to locate the program file.
5. Locate the file and click **Open**.
6. Click **Update**.

Administrative Tasks

Administrative tasks allow you to configure SNMP Service and download diagnostic information.

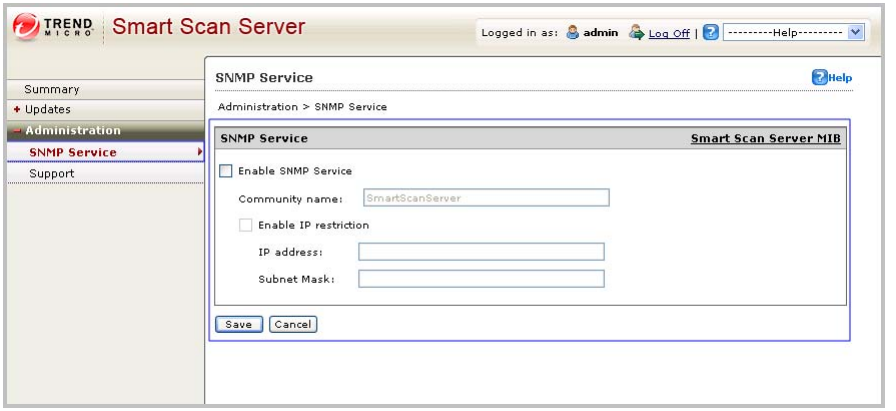
Using SNMP Service

Smart Scan Servers supports SNMP to provide further flexibility in monitoring the product. Configure settings and download the MIB file from the Web console.

Configuring SNMP Service

Configure SNMP Service to monitor Smart Scan Server using SNMP notifications.

FIGURE 4-11. SNMP Service



To configure SNMP Service:

1. Log on to the Web console.
2. Click **Administration** from the main menu. A drop down menu appears.
3. Click **SNMP Service** from the drop down menu. The SNMP Service screen appears.
4. Select the **Enable SNMP Service** check box.
5. Specify a **Community name**.
6. To enable IP address restriction, click the **Enable IP restriction** check box. Classless Inter-Domain Routing (CIDR) is not supported for IP restriction.
   a. Specify an IP address.
   b. Specify a subnet mask.
7. Click **Save**.

Downloading the MIB File

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

To download the MIB file:

1. Log on to the Web console.
2. Click **Administration** from the main menu. A drop down menu appears.
3. Click **SNMP Service** from the drop down menu. The SNMP Service screen appears.
4. Click **Smart Scan Server MIB** to download the MIB file. A confirmation prompt displays.
5. Click **Save**. The **Save As** screen displays.
6. Specify the save location.
7. Click **Save**.

Downloading Diagnostic Information

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

FIGURE 4-12. Downloading Diagnostic Information

To download diagnostic information:

1. Log on to the Web console.
2. Click **Administration** from the main menu. A drop down menu appears.
3. Click **Support** from the drop down menu. The Support screen appears.
4. Click **Start**. The download progress screen appears.
5. Click **Save** when the prompt for the downloaded file appears.
6. Specify the location and file name.
7. Click **Save**.

Changing the Product Console Password

The product console password is the primary means to protect Smart Scan 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). The CLI allows you to change the admin account passwords. Use the "configure password" command from the CLI to make changes.

Tip: To design a safe 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 both 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 Scan Server

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

Updating Components

The Smart Scan Server downloads the Smart Scan Pattern. Clients verify potential threats against the pattern by sending scan queries to the Smart Scan Server. Clients do not download the Smart Scan Pattern.

Note: The other pattern used in the smart scan 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 Scan 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 Scan 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 SCAN > INTEGRATED SERVER

1. Select to use the Integrated Smart Scan Server. If you do not select the check box:
   - The Trend Micro Smart Scan Server service (iCRCServfice.exe) stops.
   - The integrated server stops updating components from the ActiveUpdate server.
   - Clients will not be able to send scan queries to the integrated server.
2. Use the information under **Server Address** when configuring the Smart Scan Server list. For details about the list, see *Configuring the Smart Scan Server List* on page 3-29.

   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.

Note: 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 Scan 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. To update the pattern automatically, enable scheduled updates and configure the update schedule.
5. Select the location from where you want to download component updates.

   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 4-21 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.
6. Click **Save**.

Proxy for Server Update

You can configure the integrated Smart Scan 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

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 Scan Server

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

   For details, see *Configuring Computer Location Settings* on page 3-32.
2. Check if the Smart Scan Server address on the standard or custom list of scan servers is correct.

   For details, see *Configuring the Smart Scan Server List* on page 3-29.
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 Scan 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 Scan Server.
   - If LocationProfile=2, the client is not connected to the network and should connect to the Global Smart Scan 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 Scan Servers (local and global).

   For details, see *Configuring External Proxy Settings* on page 3-27 and *Configuring Internal Proxy Settings* on page 3-28.

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
- VMWare platform and version

- Exact text of the error message, if any
- Steps to reproduce the problem
- Collect Diagnostic Information. See *Downloading Diagnostic Information* on page 4-18.

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

Smart Scan Deployment Tasks

This section includes detailed information and procedures about smart scan deployment tasks.

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 server information. Specify this information on the OfficeScan 8.x/7.x 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.

Upgrading Clients by Moving Them to an OfficeScan 10 Server

One of the ways you can upgrade clients is by moving them to an OfficeScan 10 server.

To move clients to an OfficeScan 10 server:

For OfficeScan 8.x:

1. On the Web console, navigate to **Updates > Summary**.
2. Click **Cancel Notification**. This function clears the server notification queue, which will prevent problems moving clients to the OfficeScan 10 server.

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

3. Navigate to **Networked Computers > Client Management**.
4. From the client tree, select the clients you want to upgrade. Stagger the upgrade either by selecting a domain or specific clients from 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.

5. Click **Manage Client Tree > Move Client**.
6. Specify the OfficeScan 10 server computer name/IP address and server listening port under **Move selected client(s) online to another OfficeScan Server**.
7. Click **Move**.

For OfficeScan 7.x:

1. On the Web console, click **Clients** on the main menu.
2. From the client tree, select the clients you want to upgrade. Stagger the upgrade either by selecting a domain or specific clients from 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 **Move**.
4. Specify the OfficeScan 10 server computer name/IP address and server listening port under **Move selected client(s) online to another OfficeScan Server**.
5. Click **Move**.

Upgrade Results

- Online clients start to move and upgrade.
- Offline clients move and upgrade when they become online. The OfficeScan 8.x/7.x server continues to manage these clients.
- Roaming clients move and upgrade when they become online or, if the client has scheduled update privileges, when scheduled update runs.

Note: You can uninstall the OfficeScan 7.x or 8.x 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. Do this if you have a large number of clients.

Perform the following tasks on the OfficeScan 10 Web console:

To manually upgrade clients after the OfficeScan server upgrades:

1. Navigate to **Networked Computers > Client Management**.
2. On the client tree, select the clients you want to upgrade. Stagger the upgrade either by selecting a domain or specific clients from 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)

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 2000, 2003, and XP Professional logs on to a server whose login script you modified using Login Script Setup (AutoPcc.exe).

- Schedule 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 2000, 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 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**.
   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 Clients**.
6. Navigate to **Updates > Networked Computers > Automatic Update**.
7. Check 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).

   a. Enable these settings if you disabled the setting in step 4.
   b. Disable these settings if you enabled the setting in step 4.

8. Click **Save**.

For OfficeScan 7.x:

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. Check 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.

   a. Enable these settings if you disabled the setting in step 4.
   b. Disable these settings if you enabled the setting in step 4.
8. Click **Save**.

Managing 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 simultaneously configure, manage, and apply the same configuration to all domain members.

OfficeScan 10/8.x Domains

To add a domain:

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.

To move a client:

PATH: NETWORKED COMPUTERS > CLIENT MANAGEMENT > MANAGE CLIENT TREE > MOVE CLIENT

1. Select whether to move clients to another domain or OfficeScan server.
   a. To move clients to another domain, select **Move selected client(s) to another domain**, choose the domain from the drop-down list, and decide whether or not to apply the settings of the new domain to the clients.

   Tip: Alternatively, drag and drop the client to another domain in the client tree.

   b. To move clients to another OfficeScan server, specify the server name and HTTP port number under **Move selected client(s) to another OfficeScan Server**.
2. Click **Move**.

OfficeScan 7.x Domains

To move a client:

1. Click **Clients** on the main menu.
2. On the screen that displays, select **Move selected client(s) to another domain** and then select the domain.
3. Moving clients to a different domain may change settings for the client. To preserve the existing client settings, disable **Apply settings of new domain to selected clients**.
4. Click **OK**.

Appendix B

Command Line Interface (CLI) Commands

This section describes the Command Line Interface (CLI) commands that you can use in the standalone Smart Scan Server to perform monitoring, debugging, troubleshooting, and configuration tasks.

List of Commands

This section describes the Command Line Interface (CLI) commands that you can use in the standalone Smart Scan Server 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 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]

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

COMMAND	SYNTAX	DESCRIPTION
configure ip static	configure ip static <ip> <mask> <gateway> [vlan]	Configure the default Ethernet interface to use the static IP configuration
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 Scan 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

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

COMMAND	SYNTAX	DESCRIPTION
configure timezone America Caracas	configure timezone America Caracas	Configure timezone to America/Caracas location
configure timezone America Chicago	configure timezone America Chicago	Configure timezone to America/Chicago location
configure timezone America Chihuahua	configure timezone America Chihuahua	Configure timezone to America/Chihuahua location
configure timezone America Denver	configure timezone America Denver	Configure timezone to America/Denver location
configure timezone America Godthab	configure timezone America Godthab	Configure timezone to America/Godthab location
configure timezone America Lima	configure timezone America Lima	Configure timezone to America/Lima location
configure timezone America Los_Angeles	configure timezone America Los_Angeles	Configure timezone to America/Los_Angeles location
configure timezone America Mexico_City	configure timezone America Mexico_City	Configure timezone to America/Mexico_City location
configure timezone America New_York	configure timezone America New_York	Configure timezone to America/New_York location
configure timezone America Noronha	configure timezone America Noronha	Configure timezone to America/Noronha
configure timezone America Phoenix	configure timezone America Phoenix	Configure timezone to America/Phoenix

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

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

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

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

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

COMMAND	SYNTAX	DESCRIPTION
configure timezone Asia Taipei	configure timezone Asia Taipei	Configure timezone to Asia/Taipei location
configure timezone Asia Tehran	configure timezone Asia Tehran	Configure timezone to Asia/Tehran location
configure timezone Asia Tokyo	configure timezone Asia Tokyo	Configure timezone to Asia/Tokyo location
configure timezone Asia Yakutsk	configure timezone Asia Yakutsk	Configure timezone to Asia/Yakutsk location
configure timezone Atlantic Azores	configure timezone Atlantic Azores	Configure timezone to Atlantic/
configure timezone Australia Adelaide	configure timezone 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/

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

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

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

COMMAND	SYNTAX	DESCRIPTION
configure timezone Pacific Honolulu	configure timezone Pacific Honolulu	Configure timezone to Pacific/Honolulu location
configure timezone Pacific Kwajalein	configure timezone Pacific Kwajalein	Configure timezone to Pacific/Kwajalein location
configure timezone Pacific Midway	configure timezone Pacific Midway	Configure timezone to Pacific/Midway location
configure timezone US Alaska	configure timezone US Alaska	Configure timezone to US/Alaska location
configure timezone US Arizona	configure timezone US Arizona	Configure timezone to US/Arizona location
configure timezone US Central	configure timezone US Central	Configure timezone to US/Central location
configure timezone US East-Indiana	configure timezone US East-Indiana	Configure timezone to US/East-Indiana location
configure timezone US Eastern	configure timezone US Eastern	Configure timezone to US/Eastern location
configure timezone US Hawaii	configure timezone US Hawaii	Configure timezone to US/Hawaii location
configure timezone US Mountain	configure timezone US Mountain	Configure timezone to US/Mountain location
configure timezone US Pacific	configure timezone US Pacific	Configure timezone to US/Pacific location
disable ssh	disable ssh	Disable the sshd daemon
enable	enable	Enable administrative commands
enable ssh	enable ssh	Enable the sshd daemon

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

COMMAND	SYNTAX	DESCRIPTION
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
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

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

COMMAND	SYNTAX	DESCRIPTION
show url management	show url management	Display Web console URL
show url scanservice	show url scanservice	Display client connection addresses
shutdown	shutdown [time]	Shut down this machine after a specified delay or immediately *time* UNIT Time in minutes to shutdown this machine [0]

Index

V

W